

IJCSIS Vol. 14 No. 4, April 2016 Part I
ISSN 1947-5500

International Journal of Computer Science & Information Security

© IJCSIS PUBLICATION 2016
Pennsylvania, USA

Indexed and technically co-sponsored by :



Please consider to contribute to and/or forward to the appropriate groups the following opportunity to submit and publish original scientific results.

CALL FOR PAPERS

International Journal of Computer Science and Information Security (IJCSIS) January-December 2016 Issues

The topics suggested by this issue can be discussed in term of concepts, surveys, state of the art, research, standards, implementations, running experiments, applications, and industrial case studies. Authors are invited to submit complete unpublished papers, which are not under review in any other conference or journal in the following, but not limited to, topic areas.

See authors guide for manuscript preparation and submission guidelines.

Indexed by Google Scholar, DBLP, CiteSeerX, Directory for Open Access Journal (DOAJ), Bielefeld Academic Search Engine (BASE), SCIRUS, Scopus Database, Cornell University Library, ScientificCommons, ProQuest, EBSCO and more.

Deadline: see web site

Notification: see web site

Revision: see web site

Publication: see web site

Context-aware systems

Networking technologies

Security in network, systems, and applications

Evolutionary computation

Industrial systems

Evolutionary computation

Autonomic and autonomous systems

Bio-technologies

Knowledge data systems

Mobile and distance education

Intelligent techniques, logics and systems

Knowledge processing

Information technologies

Internet and web technologies

Digital information processing

Cognitive science and knowledge

Agent-based systems

Mobility and multimedia systems

Systems performance

Networking and telecommunications

Software development and deployment

Knowledge virtualization

Systems and networks on the chip

Knowledge for global defense

Information Systems [IS]

IPv6 Today - Technology and deployment

Modeling

Software Engineering

Optimization

Complexity

Natural Language Processing

Speech Synthesis

Data Mining

For more topics, please see web site <https://sites.google.com/site/ijcsis/>

arXiv.org Google scholar

SCIRUS
search engine for science

ScientificCommons

Scribd

.docstoc
find and share professional documents

BASE
Bielefeld Academic Search Engine

CiteSeerX beta

uni-trier.de
Computer Science
Bibliography

DOAJ
DIRECTORY OF
OPEN ACCESS
JOURNALS

EBSCO
HOST

ProQuest

Editorial Message from Editorial Board

It is our great pleasure to present the April 2016 issue (Volume 14 Number 4) of the International Journal of Computer Science and Information Security (IJCSIS). High quality survey and review articles are proposed from experts in the field, promoting insight and understanding of the state of the art, and trends in computer science and technology. It especially provides a platform for high-caliber researchers, practitioners and PhD/Doctoral graduates to publish completed work and latest development in active research areas. According to Google Scholar, up to now papers published in IJCSIS have been cited over 5908 times and the number is quickly increasing. This statistics shows that IJCSIS has established the first step to be an international and prestigious journal in the field of Computer Science and Information Security. There have been many improvements to the processing of papers; we have also witnessed a significant growth in interest through a higher number of submissions as well as through the breadth and quality of those submissions. IJCSIS is indexed in major academic/scientific databases and repositories: Google Scholar, Thomson Reuters, ArXiv, CiteSeerX, Cornell's University Library, Ei Compendex, ISI Scopus, DBLP, DOAJ, ProQuest, ResearchGate, Academia.edu and EBSCO among others.

On behalf of IJCSIS community and the sponsors, we congratulate the authors and thank the reviewers for their outstanding efforts to review and recommend high quality papers for publication. In particular, we would like to thank the international academia and researchers for continued support by citing papers published in IJCSIS. Without their sustained and unselfish commitments, IJCSIS would not have achieved its current premier status.

"We support researchers to succeed by providing high visibility & impact value, prestige and excellence in research publication." For further questions or other suggestions please do not hesitate to contact us at ijcsiseditor@gmail.com.

A complete list of journals can be found at:

<http://sites.google.com/site/ijcsis/>

IJCSIS Vol. 14, No. 4, April 2016 Edition

ISSN 1947-5500 © IJCSIS, USA.

Journal Indexed by (among others):



Open Access This Journal is distributed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source.



Bibliographic Information

ISSN: 1947-5500

Monthly publication (Regular Special Issues)

Commenced Publication since May 2009

Editorial / Paper Submissions:

IJCSIS Managing Editor

[\(ijcsiseditor@gmail.com\)](mailto:ijcsiseditor@gmail.com)

Pennsylvania, USA

Tel: +1 412 390 5159

IJCSIS EDITORIAL BOARD

Editorial Board Members	Guest Editors / Associate Editors
Dr. Shimon K. Modi [Profile] Director of Research BSPA Labs, Purdue University, USA	Dr Riktesh Srivastava [Profile] Associate Professor, Information Systems, Skyline University College, Sharjah, PO 1797, UAE
Professor Ying Yang , PhD. [Profile] Computer Science Department, Yale University, USA	Dr. Jianguo Ding [Profile] Norwegian University of Science and Technology (NTNU), Norway
Professor Hamid Reza Naji , PhD. [Profile] Department of Computer Engineering, Shahid Beheshti University, Tehran, Iran	Dr. Naseer Alquraishi [Profile] University of Wasit, Iraq
Professor Yong Li , PhD. [Profile] School of Electronic and Information Engineering, Beijing Jiaotong University, P. R. China	Dr. Kai Cong [Profile] Intel Corporation, & Computer Science Department, Portland State University, USA
Professor Mokhtar Beldjehem , PhD. [Profile] Sainte-Anne University, Halifax, NS, Canada	Dr. Omar A. Alzubi [Profile] Prince Abdullah Bin Ghazi Faculty of Information Technology Al-Balqa Applied University (BAU), Jordan
Professor Yousef Farhaoui , PhD. Department of Computer Science, Moulay Ismail University, Morocco	Dr. Jorge A. Ruiz-Vanoye [Profile] Universidad Autónoma del Estado de Morelos, Mexico
Dr. Alex Pappachen James [Profile] Queensland Micro-nanotechnology center, Griffith University, Australia	Prof. Ning Xu , Wuhan University of Technology, China
Professor Sanjay Jasola [Profile] Dean, School of Information and Communication Technology, Gautam Buddha University	Dr. Bilal Alatas [Profile] Department of Software Engineering, Firat University, Turkey
Dr. Siddhivinayak Kulkarni [Profile] University of Ballarat, Ballarat, Victoria, Australia	Dr. Ioannis V. Koskosas , University of Western Macedonia, Greece
Dr. Reza Ebrahimi Atani [Profile] University of Guilan, Iran	Dr Venu Kuthadi [Profile] University of Johannesburg, Johannesburg, RSA
Dr. Umar Ruhi [Profile] University of Ottawa, Canada	Dr. Zhihan Lv [Profile] Chinese Academy of Science, China
Dr. Vahid Esmaelzadeh [Profile] Iran University of Science and Technology	Prof. Ghulam Qasim [Profile] University of Engineering and Technology, Peshawar, Pakistan
Dr. Jiliang Zhang [Profile] Northeastern University, China	Prof. Dr. Maqbool Uddin Shaikh [Profile] Preston University, Islamabad, Pakistan
Dr. Jacek M. Czerniak [Profile] Casimir the Great University in Bydgoszcz, Poland	Dr. Musa PEKER [Profile] Faculty of Technology, Mugla Sitki Kocman University, Turkey
	Dr. Wencan Luo [Profile] University of Pittsburgh, US

TABLE OF CONTENTS

1. PaperID 31031698: Flexible Hardware Implementation of Hyperelliptic Curves Cryptosystem (pp. 1-7)

*Anissa Sghaier #, Chiraz Massoud #, Medien Zeghid *, Mohsen Machhout #*

Faculty of Sciences, University of Monastir, E&E Lab Avenue of the environment 5019 Monastir

** Higher Institute of Applied Sciences and Technology Taffala City, 4003 Sousse Tunisie*

Abstract — Due to the resolution of key distribution problem, asymmetric scheme become the most popular cryptographic technique compared to symmetric scheme. One of the well-known asymmetric encryption algorithms are (Hyper)Elliptic Curve Cryptosystem (ECC and HECC). They provide equal security levels compared with the RSA algorithm with shorter operand size. Although, the HECC outperform the ECC due to its shorter operand size. The objective of this paper is to present an efficient hardware architecture using Cantor's method, to implement a new way of explicit formula over genus curve 2, and analyze the performance of the two implementations. HECC cryptosystem was implemented over GF(283) on XC5V240 FPGA, it takes about 5086 slices, and it runs at 175 MHz in 0.287 ms.

Keywords: ECC, HECC, hardware implementation, Cantor's method, explicit formula

2. PaperID 310316100: Phishing Identification Using a Novel Non-Rule Neuro-Fuzzy Model (pp. 8-14)

Luong Anh Tuan Nguyen, Faculty of Information Technology, Ho Chi Minh City University of Transport, Ho Chi Minh City, Vietnam

Huu Khuong Nguyen, Faculty of Information Technology, Ho Chi Minh City University of Transport, Ho Chi Minh City, Vietnam

Abstract — This paper presents a novel approach to overcome the difficulty and complexity in identifying phishing sites. Neural networks and fuzzy systems can be combined to join its advantages and to cure its individual illness. This paper proposed a new neuro-fuzzy model without using rule sets for phishing identification. Specifically, the proposed technique calculates the value of heuristics from membership functions. Then, the weights are trained by neural network. The proposed technique is evaluated with the datasets of 22,000 phishing sites and 10,000 legitimate sites. The results show that the proposed technique can identify with an accuracy identification rate of above 99%.

Keywords — Phishing; Fuzzy; Neural Network; Neuro-Fuzzy

3. PaperID 31031614: A Predictable Markov Based Cache Replacement Scheme in Mobile Environments (pp. 15-26)

Ahmed. A. A. Gad-ElRab, Faculty of Science, Al-Azhar University, Cairo, Egypt

Kamal A. ElDahshan, Faculty of Science, Al-Azhar University, Cairo, Egypt

Ahmed Sobhi, (PhD Student) Faculty of Science, Al-Azhar University, Cairo, Egypt

Abstract — Mobile Location-dependent services are popular services that the mobile environments support. Data caching is an effective technique that plays an important role in improving these services. In mobile environments, due to the limited cache size of mobile devices, the cache replacement which is finding a suitable subset of items for eviction from cache becomes important. Most of the existing cache replacement schemes use the cost functions in the replacement operation. In this paper we propose a Predictable Markov based Cache Replacement (PMCR) scheme for Mobile Environments. The proposed scheme uses a markov model with cost function in the replacement operation. The key idea of the markov model is the prediction of future client locations by giving us the weight of visiting each location whose data is cached. Simulation results show that our approach improves the system performance compared to the existing schemes.

Keywords - Mobile Location-dependent services; Data dissemination; Cache replacement; Predicted region; Markov model; PMCR.

4. PaperID 31031619: Developing an Intelligent System for Crowd Density Estimation (pp. 27-31)

Dr. Ali Salem Ali Bin-Sama, Dr. Salem Saleh Ahmed Alamri

Department of Engineering Geology, Oil & Minerals Faculty, Aden University, Aden, Yemen

Abstract — Crowd density estimation models are important for monitoring people behaviors in a crowd. In this paper a development of an intelligent system is introduced to achieve the goal of density estimation. Mainly, the proposed system consist of Gabor features texture pattern extraction and convolutional neural network for pattern classification. To assess the performance of the developed, a number of public benchmark images are used such as LIBRARY Dataset, QUT Dataset, and Fudan Pedestrian Dataset.

Keyword: Crowd Density Estimation, Gabor filters, Convolutional neural network, Texture Image.

5. PaperID 31031641: A Security Scheme for Providing AIC Triad in Mobile Cloud Computing (pp. 32-36)

Isra Sitan Al-Qasrawi

Department of Information Technology, Al-balqa' Applied University, AL-Huson University College, Irbid, Jordan

Abstract — As mobile devices like smart phones and tablets continue to grow, the requirement of cloud computing in mobile devices continue to grow too, and becomes an important service to provide users the ability to manage files and data remotely, which gave birth of Mobile Cloud Computing (MCC). As a result, new web-based threats and attacks will continue to increase in number. The most important issues must be covered to provide users reliable and secure services of mobile cloud computing are: Availability, Integrity, and Confidentiality. In this paper, (i) the concepts of cloud computing and mobile computing are discussed, the challenges that face each one of them, the meaning of mobile cloud computing, the challenges of MCC. (ii) Different mechanisms to store data in secure manner are explored. (iii) Propose a new scheme to secure the data storage in Mobile Cloud Computing without exposing the data content to the cloud service providers to protect mobile users' privacy. This scheme provides the security AIC triad concepts (Availability, Integrity, and Confidentiality) for data by applying a number of operations.

Keywords - cloud computing; mobile computing; mobile cloud computing; security; data storage; mobile user.

6. PaperID 31031668: SimCT: A Measure of Semantic Similarity Adapted to Hierarchies of Concepts (pp. 37-44)

Coulibaly Kpinna Tiekoura, National Polytechnic Institute, Department of Mathematics and Computer Science, Abidjan, Ivory Coast

Brou Konan Marcellin, National polytechnic Institute, Department of Mathematics and Computers Science, Yamoussoukro, Ivory Coast

Achiepo Odilon, National polytechnic Institute, Abidjan, Ivory Coast

Babri Michel, National Polytechnic Institute, Abidjan, Ivory Coast

Aka Boko, University of Nangui Abrogoua, Abidjan, Ivory Coast

Abstract — The Calculating of the similarity between data is a key problem in several disciplines such as machine learning, information retrieval (IR) and data analysis. In some areas such as social resilience, the similarity measures can be used to find the similarities between traumatized individuals or resilience's dimensions. In this paper, we propose a measure of semantic similarity used in many applications including clustering and information retrieval. It relies on a knowledge base represented as a hierarchy of concepts (ontology, graph, taxonomy). Its uniqueness with respect to previous proposals is the difference between the indices of similarity that it establishes between brothers concepts located at the same hierarchical level and having the same direct ancestor. In addition, our semantic similarity

measure provides better modularity in clustering compared with Wu and Palmer's similarity measure and Proxygenea 3.

Keywords - clustering, hierarchical tree, resilience, semantic similarity measure.

7. PaperID 31031672: An Algorithm (COLMSTD) for Detection of Defects on Rail and Profile Surfaces (pp. 45-50)

*İlhami Muharrem Orak, Faculty of Engineering, Karabük University, Karabük, Turkey (78000)
Ahmet Çelik, Tavşanlı Vocational School, Dumlupınar University, Kütahya, Turkey*

Abstract — Rail or profile products are used in many fields today. The rolling process is the most important production phase of the rail and the profile product. However, undesirable defects in the surface of the product during the rolling process can occur. Identifying these defects quickly by an intelligent system using image processing algorithms will provide a major contribution in terms of time and labor. For the detection of the regions, objects and shapes on the image, several algorithms were used. In this study, we introduce a Standard Deviation based algorithm (COLMSTD) by using the pixel color values. In order to evaluate the performance of the algorithm, the result of the COLMSTD algorithm is compared with the results of Hough Transform, MSER, DFT, Watershed, Blob Detection algorithms. In this study, it was seen that each algorithm has different capability in some extend to identify the surface defects in rail or profile. However, COLMSTD algorithm achieve more accurate and successful results than the other algorithms.

Keywords - Computer vision; Image processing; Manufacturing systems; Defect detection; Hot rolling; Rail; Profile.

8. PaperID 310316121: Investigating the Opportunities of Using Mobile Learning by Young Children in Bulgaria (pp. 51-55)

*Radoslava Kraleva #, Aleksandar Stoimenovski #, Dafina Kostadinova *, Velin Kralev #
Department of Informatics, South West University "Neofit Rilski", Blagoevgrad, Bulgaria
* Department of Germanic and Romance Studies, South West University "Neofit Rilski", Blagoevgrad, Bulgaria*

Abstract — This paper provides an analysis of literature related to the use of mobile devices in teaching young children. For this purpose, the most popular mobile operating systems in Bulgaria are considered and the functionality of the existing mobile applications with Bulgarian interface is discussed. The results of a survey of parents' views regarding the mobile devices as a learning tool are presented and the ensuing conclusions are provided.

Keywords – Mobile learning, Mobile learning application, Analysis of the parents' opinion

9. PaperID 31031638: Conducting Multi-class Security Metrics from Enterprise Architect Class Diagram (pp. 56-61)

*Osamah S. Mohammed, Dept. of Software Engineering, College of Computer Sc. & Math, University of Mosul.
Mosul, Iraq.*

*Dujan B. Taha, Dept. of Software Engineering, College of Computer Sc. & Math, University of Mosul.
Mosul, Iraq*

Abstract — Developers often neglect security until the end of developing the software just after coding, and any change in the code with respect to security may lead to change in the software code, this consumes time and cost depending on the software size. Applying security on a software late in its SDLC may result in many security flaws, some of them can involve serious architectural issues. Applying security metrics on design phase can reveal the security level and fix vulnerabilities of a software earlier in the project. In this work, security metrics has been discussed, and conducting these metrics from Enterprise Architect class diagram using a proposed CASE tool.

Keywords - Software Engineering; Security metrics; Enterprise architect; Class diagram; SDLC; Design phase

10. PaperID 31031639: Data Traffic Optimization in Different Backoff Algorithms for IEEE 802.15.4/Zigbee Networks (pp. 62-66)

Muneer Bani Yassein, Maged Refat Fakirah

Faculty of Computer and Information Technology, Jordan University of Science and Technology, Irbid, Jordan

Qusai Abuein, Mohammed Shatnawi, Laith Bani Yaseen

Jordan University of Science and Technology Irbid, Jordan

Abstract — Zigbee/IEEE 802.15.4 is a short range wireless communication standard designed for home monitoring, health care, and industrial applications. In this paper, the impact of data traffic load and two data traffic types, namely, Constant Bit Rate (CBR) and Variable Bit Rate (VBR) are studied by considering Binary Exponential Backoff Algorithm (BEB), Linear Backoff Algorithm and Fibonacci Backoff Algorithm (FIB). The efficiency of these algorithms is extensively evaluated by modifying the number of CBR or VBR packets sent from the nodes to the PAN coordinator. The obtained results demonstrate that using the VBR data traffic increases the throughput and decreases the end to end delay, while adopting the CBR data traffic decreases the total energy consumption of a small scale network.

Keywords—IEEE 802.15.4/ZigBee; backoff ; BEB; Linear; FIB; data traffic load; VBR; CBR

11. PaperID 31031653: A Novel Polygon Cipher Technique using Hybrid Key Scheme (pp. 67-71)

Shadi R. Masadeh, Faculty of Information Technology, Isra University, Amman, Jordan

Hamza A. A. Al_Sewadi, King Hussein Faculty of Computing, Prince Sumaya for Technology, Amman, Jordan

Abstract — Due to the narrow key space and frequency analysis weakness, classical cipher techniques are not suitable for most today's information communication. On the other hand, modern standardized ciphers are far more secure and widely used for such communication. However, they are so complicated in implementation and may not be suitable for less sophisticated applications. This paper suggests a novel symmetric cipher method based on polygon scheme that shows superior security as compared with classical methods by having wide key space and strength against frequency analysis attack and yet it is simpler than modern ciphers.

Keywords- information security, encryption/decryption, secret key, symmetric cryptography, asymmetric key implementation.

12. PaperID 31031659: An Efficient Method to Diagnose the Treatment of Breast Cancer using Multi-Classifiers (pp. 72-80)

J. Umamaheswari, Computer Science dept. Majmaah University, Al- Majmaah, Saudi Arabia

Jabeen Sultana, Ruhi Fatima, Computer Science dept. Majmaah University, Al- Majmaah, Saudi Arabia

Abstract — Knowledge discovery in the form of rule extraction proposed to extract rules from classification datasets by giving data set to Decision Trees (DT), NBTREE, KNN and 10-fold Cross Validation performed, resulting the tree or a model from which rules are extracted and measured on different parameters taken from root node to leaf node.

Keywords - Transparent; Opaque; Knowledge discovery; rule extraction

13. PaperID 31031607: A Study on Optimizing the Efficiency of Location Aided Routing (LAR) Protocol (pp. 81-86)

Priyanka Kehar, Department of Computer Science, Lovely Professional University, Punjab, India

Pushpendra Kumar Pateriya, Lovely Faculty of Technology and Sciences, Lovely Professional University, Phagwara, India

Abstract -The improvised network is an arrangement less network consisting of portable nodes. VANETs is the recently developed technique to achieve traffic safety and efficiency through inter vehicle communication, where routing protocol plays a vital role. Inefficient path establishment and network congestion both bring the severe degradation in network throughput and performance. Routing throughput and enactment is largely reliant on the stability and availability of the wireless link which makes it a very pivotal factor, that can't be ignored in order to obtain proper performance and throughput measurement in vehicular improvised network. As vehicle nodes have higher mobility due to which some prediction based techniques were proposed in previous times for path establishment. Among the proposed prediction based techniques, location aided routing protocol influence real time vehicular information to generate path between source and destination, with high possibility of network connectivity among them. The main feature of optimized LAR is: minimize the delay, minimize the fuel consumption, and maximize the throughput.

Keywords - *Road Side Unit (RSU); Location Aided Protocol (LAR); Internet Service Provider (ISP); Intelligent Transport Service (ITS).*

14. PaperID 31031611: Analyzing and Processing Data Faster Based on Balanced Partitioning (pp. 87-92)

*Annie P. Kurian, Dept. of Computer Science & Engg., Velammal Engg. College, Chennai, India
Prof. Dr. V. Jeyabalara, Dept. of Computer Science & Engg., Velammal Engg. College, Chennai, India*

Abstract — Big data has become a well-known buzzword to the public at large which handles enormous amount of data i.e., in terabyte to zeta byte. Processing and analyzing such huge amount of data is not possible with traditional and conventional environments. The existing system approaches for range partition queries are deficient to rapidly provide definite results in big data. In this paper, we propose a agile approach to range- aggregate queries in big data documents/table using balanced partitioning. This approach first divides the big data into independent partition with balanced partitioning, and then it generates a local estimation sketch for each partition. When a RA-query request arrives, the system quickly fetches and obtains the result directly by compiling local estimation from all partitions. The balanced partitioning avoids the overall scan of the data in order to provide the result. Big data ecosystem like HIVE and Impala is used to handle the structured data and uses the balanced partitioning to provide fast and accurate output. Partitioning provides maintenance, availability and improvised query performance to the users. It reduces the time complexity, i.e., O(1) time complexity for data updates. The overall performance of the dataset produced would be efficient, fault-tolerant, accurate and fast.

Keywords – *range aggregate, big data, HIVE, Impala, partition, map reduce, HDFS.*

15. PaperID 31031613: ICT Convergence in Internet of Things – The Birth of Smart Factories (pp. 93)

*Mahmood Adnan, Hushairi Zen
Faculty of Engineering, Universiti Malaysia Sarawak*

Abstract – Over the past decade, most factories across developed parts of the world employ a varying amount of the manufacturing technologies including autonomous robots, RFID (radio frequency identification) technology, NCs (numerically controlled machines), wireless sensor networks embedded with specialized computerized softwares for sophisticated product designs, engineering analysis, and remote control of machinery, etc. The ultimate aim of these all dramatic developments in manufacturing sector is thus to achieve aspects such as shorter innovation / product life cycles and raising overall productivity via efficiently handling complex interactions among the various stages (functions, departments) of a production line. The notion, Factory of the Future, is an unpredictable heaven of efficaciousness, wherein, issues such as the flaws and downtime would be issues of the long forgotten age. This technical note thus provides an overview of this awesome revolution waiting to be soon realized in the manufacturing sector.

Index Terms – Smart Factories, Fourth Industrial Revolution, Internet of Things, Ubiquitous Computing.

16. PaperID 31031626: IEEE 802.11ac vs IEEE 802.11n: Throughput Comparison in Multiple Indoor Environments (pp. 94-101)

Zawar Shah (a), Ashutosh A Kolhe (a), Omer Mohsin Mubarak (b)

(a) Whitireia Community Polytechnic, Auckland, New Zealand.

(b) Iqra University, Islamabad, Pakistan

Abstract — IEEE 802.11ac is a fifth generation WiFi standard that has many advanced features than the current widely used IEEE 802.11n. In this paper, we perform experiments in two real indoor environments (that possess interference and have different multipath characteristics) to quantify the gain in average throughput provided by IEEE 802.11ac compared to IEEE 802.11n. Our experimental results show that in an environment with less multipath effect, IEEE 802.11ac provides 51% and 126% gain compared to IEEE 802.11n at a distance of 5m and 18.5m from the wireless router, respectively. Similarly, in an environment with high multipath effect, IEEE 802.11ac provides gain of 21% and 32% compared to IEEE 802.11n at a distance of 1m and 18.5m from the wireless router, respectively. We conclude that IEEE 802.11ac can effectively handle interference caused by other IEEE 802.11n (5GHz) sources and provides higher throughput than IEEE 802.11n.

Keywords: IEEE 802.11ac, IEEE 802.11n, Throughput, MIMO.

17. PaperID 31031651: Implementing Navigational Aspect of Specific Testing Process Model (pp. 102-111)

Garima Singh, Dept. of Computer Science and Engineering, JECRC University, Jaipur, Rajasthan, India

Manju Kaushik, Associate Professor, Dept. of Computer Science and Engineering, JECRC University, Jaipur, Rajasthan, India

Abstract - Navigational modeling of web application and testing the navigational aspect of the web application is as important as the content displayed and security of application to maintain the quality and user satisfaction. Test paths are generated through the navigation model which is derived from the activity diagram. The objective of this paper is to implement navigational aspect of web application through a model.

Keywords - Specific Testing Process Model, Web application modelling, web application navigational testing

18. PaperID 31031667: Comparative Analysis of LEACH and V-LEACH Protocols in Wireless Sensor Networks (pp. 112-119)

*Layla Aziz (*1), Said Raghay (1), Abdellah Jamali (2), and Hanane Aznaoui (1)*

(1) Laboratory(LAMAI), Cadi Ayyad University, Marrakech, Morocco

(2) Laboratory (RI2M), Hassan 1st University , Berrchid, Morocco

Abstract — In the past few years, the research community is strongly attracted to wireless sensor networks (WSNs). Sensor node is generally driven by an irreplaceable battery which limits its energy supply. A number of new methods and strategies have been proposed to reduce energy consumption in WSNs. LEACH (Low Energy Adaptive Clustering Hierarchy) protocol is a well-known approach using the Clustering mechanism to minimize the energy consumption and improve the lifetime of WSN . In this work, we describe various clustering algorithms and a comparative analysis of LEACH protocol with its improved version V-LEACH using NS2 simulator.

Index Terms— CLUSTERING, LEACH, NS2, V-LEACH, WSN

19. PaperID 31031670: Slow Wave-IDC Loaded High Bandwidth Microstrip Antenna Operates For Multi Band Applications (pp. 120-125)

Brajlata Chauhan, Uttarakhand Technical University, Dehradun UK, India

Sandip Vijay, Deptt. of Electronics & Communication Engg. ICFAI Univ. Dehradun UK, India

S C Gupta, Department of Electronics & Communication Engineering, DIT Dehradun UK, India

Abstract — A slow wave structure as inter-digital capacitor (IDC) is incorporated in micro-strip patch to obtain Miniaturized and high band width antenna specially for WLAN, X & Ku –bands. The antennas are loaded with IDC to slow down the guided wave to increase Gain - Bandwidth product. The simulated antennas offered gain of 6.47dB, directivity of 6.47dB and radiated power of 0.001066 watt (antenna2). This paper presents increased bandwidth to 55.33% by inserting a slot on the above patch offered nominal change in gain of 5.8852 and the loaded slot antenna produce directivity of 7.38832dB and radiated power of 0.0299368 watt (antenna 3) in the range of VSWR is less than 1.5.

Keywords- Slow wave structure; inter-digital capacitor (IDC); Gain band width product; multi band micro-strip patch antenna; rectangular slot; equivalent circuit.

20. PaperID 31031673: An Efficient Anti-noise Fast FCM Clustering for Glioblastoma Multiforme Tumor Segmentation (pp. 126-133)

B. Srinivasa Rao, ANUCET, Acharya Nagarjuna University, Guntur-522510, Andhra Pradesh, India.

Dr. E. Sreenivas Reddy, Professor, ANUCET, ANUCET, Acharya Nagarjuna University, Guntur-522510, Andhra Pradesh, India

Abstract -- Image segmentation plays an important role in medical image processing. Magnetic Resonance Imaging (MRI) is primary diagnostic technique to do image segmentation. Clustering is an unsupervised learning method of segmentation. The conventional FCM algorithm is sensitive to noise, suffers from the computation time overhead and is very sensitive to cluster center initialization. In order to overcome this problem, a new method called Anti-Noise Fast Fuzzy C-Means (AN-FFCM) clustering algorithm for segmentation of Glioblastoma Multiforme tumor segmentation is proposed. The proposed algorithm is able to minimize the effects of impulse noise by incorporating noise detection stage to the clustering algorithm during the segmentation process without degrading the fine details of the image. This method also improves the performance of the FCM algorithm by finding the initial cluster centroids based on histogram analysis, reducing the number of iterations for segmentation of noisy images. The advantages of the proposed method are: (1) Minimizes the effect of impulse noise during segmentation, (2) Minimum number of iterations to segment the image. The performance of the proposed method is tested on BRATS data set. Experimental results show that the proposed algorithms are superior in preserving image details and segmentation accuracy while maintaining a low computational complexity.

Index Terms: Glioblastoma Multiforme(GBM), image segmentation, Histogram, salt-and-pepper noise, Fuzzy c-means, Medical Image processing.

21. PaperID 31031679: Ear Classifying in Profile images Based on Curves and Shape (pp. 134-137)

Mohammad Mahmoudi, Department of Computer Science and Engineering, Khoy branch, Islamic Azad University Khoy, Iran

Ali Habiboghi, Department of Computer Science and Engineering, Khoy branch, Islamic Azad University Khoy, Iran

Abstract — In this research we are going to classify ears based on their appearance. For this aim, region of ear in profile image should be extracted. Then by using margins surrounding around the ear and the center of ear would be obtained by the proposed method. Finally by determining appropriate threshold the ears were classified based on their shapes. The database used in this article is CVL. Simulating and classifying of this article have acceptable accuracy 83.6%.

Keywords -- Classification, Ear Recognition; Image Processing; Profile Images

22. PaperID 31031685: Color Coding Based Detection and Prevention Mechanism for Wormhole Attack in MANET (pp. 138-144)

*Harsh Bansal, Lovely Professional University, Phagwara, Punjab, India
Gurpreet Singh, Lovely Professional University, Phagwara, Punjab, India*

Abstract — MANET is infrastructure-less, lacks centralized monitoring and has dynamic changing network topology. The high usage of MANET demands more security and confidentiality and integrity of the data communicated through network. Security has turned out to be a major concern so as to provide non-endangered communication between mobile nodes in an unfriendly environment of MANET, which poses a number of trivial challenges to security design. The wormhole attack is one of the most threatening and hazardous attacks. In this paper we have classified the well-known countermeasures against wormhole attack in the network according to detection and prevention techniques based on hop counts and delay, protocol modification, trust and reputation. The projected technique to be used for detection of wormhole attack using trust based mechanism, neighbor monitoring concept and credits based mechanism will help to detect and isolate the malicious nodes hence enabling the formation of trusted network.

Keywords— MANET, Intrusion Detection, Wormhole Attack, Secure Routing, Network Security.

23. PaperID 31031687: Pragmatic Analysis Based Document Summarization (pp. 145-149)

*Ms. Bhakti A. Mukhedkar #, Mrs. D. Y. Sakhare #, Mr. Raj Kumar **
Department of Electronics Engineering, MIT Academy of Engineering, Alandi, Pune, India
** Scientist DRDO, Pune.*

Abstract - Automatic Text summarization is the process of reducing a text document to create a summary that relates only important points of the original document. Now a day's huge information available so there is interest in automatic Text summarization. It's very hard for human being to manually summarize large documents of text. Hence we use Text Summarization techniques. Basically Text Summarization Techniques classified in two types 1. Abstraction 2. Extraction. In this Paper We Proposed Abstraction Type of Text Summarizations by using pragmatic analysis. This Summary being generated by Matlab and serially transmitted to PIC microcontroller and displayed on LCD.

Index Terms— POS Tagging, Text Summarization by pragmatic analysis.

24. PaperID 31031695: Mobility Aware Fault Tolerant Multipath Multicast Routing Protocol for MANET (pp. 150-158)

*Channabasayya Mathad, Dept. of Electronics & Communication Engg, Kalpataru Institute of Technology, Tiptur Karnataka, India.
Paramesha, Dept. of Electronics & Communication Engg, Govt Engineering College, Hassan Karnataka, India.
D Srinivasa Rao, Dept. of Electronics & Communication Engg, Jawaharlal Nehru Technological University, Hyderabad Telangana, India*

Abstract — In MANETs, due to the constant mobility of the nodes, the topology is ever changing. Hence, the selection of paths is crucial. So, it is always efficient to select more than one route to the destination, so that even if one path fails, there is always high possibility for the data to reach the destination. In MANETs, since the nodes keep on joining and leaving the network randomly, selecting paths that are less susceptible to turn out faulty is important. Since several disjoint paths are possible, multicasting is economical in MANETs. In this proposed scheme a multipath, multicast routing protocol which works efficiently by selecting route with higher lifetime and it also recovers the lost packets.

Keywords - Multipath, Multicast, Fault Tolerent, LinkLife Time, Hop Count.

25. PaperID 31031697: Fully Homomorphic Encryption: State of Art and Comparison (pp. 159-167)

Ahmed EL-YAHYOUI, Mohamed Dafir ELKETTANI

Information Security Research Team, CEDOC ST2I ENSIAS, Mohammed V University in Rabat, Rabat, Morocco

Abstract - Fully homomorphic encryption (FHE) is an alternative of cryptography that allows evaluating arbitrary functions on encrypted data without the need for decryption of ciphertexts. In this article we present the state of the art of fully homomorphic encryption schemes. In particular we present a classification of several existent FHE schemes followed by a comparison of performances and complexity of these cryptosystems. Finally we will give different possible axes of research in the conclusion.

Keywords: *cryptosystem, fully homomorphic, cloud, bootstrappability, modulus reduction, key changing.*

26. PaperID 310316106: Autoregressive Model Based Segmentation of Overlapped Region (pp. 168-174)

Vidyadevi G Biradar, Department of ISE, NMIT, Bangalore, India

H Sarojadevi, Department of CSE, NMAMIT, Bangalore, India

H C Nagaraj, Department of ECE, NMIT, Bangalore, India

Abstract — Overlapped fingerprints occur due to multiple impressions of fingerprints on the same object at same place. This is natural in uncontrolled environments, or they are the residual fingerprints left over on fingerprints scanner. Overlapped fingerprints need to be separated into individual fingerprints for recognition. Separation of overlapped fingerprints involves steps, segmentation of image regions, feature extraction and classification. State of the art algorithms for separation of overlapped fingerprints adopts region wise processing approach to feature extraction. Therefore segmentation of overlapped region is an essential step for robust feature extraction. This paper presents a new algorithm for segmentation of overlapped region using time series two dimensional Autoregressive (2D AR) model. AR model parameters are estimated using Least Squares (LS) method which ensures minimum mean square error. The performance of the algorithm is evaluated using a standard database of 100 overlapped fingerprints images. The results are compared with ground truth results and are found satisfactory. Segmentation accuracy achieved is between 80% to 90%.

Keywords- *Segmentation, AR model, overlapped fingerprints, texture, separation.*

27. PaperID 310316107: A Hybrid Hashing Security Algorithm for Data Storage on Cloud Computing (pp. 175-181)

Noha MM. AbdElnapi, Computer science department, Nahda University, Beni Suef, Egypt

Fatma A. Omara, Computer science department, Cairo University, Cairo, Egypt

Nahla F. Omran, Mathematics department, South Valley University, Qena, Egypt

Abstract — In today's modern IT everything is possible on the web by cloud computing, it allows us to create, configure, use and customize the applications, services, and storage online. The Cloud Computing is a kind of Internet-based computing, where shared data, information and resources are provided with computers and other devices on-demand. The Cloud Computing offers several advantages to the organizations such as scalability, low cost, and flexibility. In spite of these advantages, there is a major problem of cloud computing, which is the security of cloud storage. There are a lot of mechanisms that is used to realize the security of data in the cloud storage. Cryptography is the most used mechanism. The science of designing ciphers, block ciphers, stream ciphers and hash functions is called cryptography. Cryptographic techniques in the cloud must enable security services such as authorization, availability, confidentiality, integrity, and non-repudiation. To ensure these services of security, we propose an effective mechanism with a significant feature of the data. This paper is to show how to improve the security of the Cloud storage using the implementation of a hybrid encryption algorithm and hash functions. It proposes the implementation of two algorithms, Rivest-Shamir-Adleman (RSA) and Advanced Encryption Standard (AES) with a

secure hashing algorithm (SHA256) by using Netbeans IDE 8.0.2, JDK 1.7 tool and EyeOS2.5 as a cloud platform on ubuntu14.04.

Keywords— *Cloud Computing, Security, Advanced Encryption Standard (AES), Rivest-Shamir-Adleman (RSA), Hybrid Algorithm, Hash functions, Secure Hash Algorithm (SHA256), Encryption, Cryptography, availability, confidentiality, integrity, authorization, and non-repudiation.*

28. PaperID 310316108: 8-neighborhood Variant for a Better Container Code Extraction and Recognition (pp. 182-186)

Wassim Al-Khawand, School of Engineering, Sciences and Technologies - University of Genoa, Italy

Seifedine Kadry, School of Engineering – American University of the Middle East, Kuwait

Riccardo Bozzo, Dept. of Electrical, Electronic, Telecommunications Engineering and Naval Architecture - University of Genoa, Italy

Khaled Smaili, Faculty of Sciences – Lebanese University, Lebanon

Abstract — In this paper, we will present a new variant of the 8-neighborhood connectivity; our approach remedies the segmentation problem related to scratched container code digits. Our approach is highly suitable for real-time automatic container code recognition applications because it treats many special cases, its average response time is equal to 21 milliseconds, and it improves the container code extraction and recognition by 0.89%; due to our contribution in enhancing the segmentation phase, the container code extraction accuracy reached 98.7%.

Keywords— *binary image, 8-neighborhood connectivity, segmentation, Container code.*

29. PaperID 310316114: Notification System Based on Face Detection and Recognition: A Novel Approach (pp. 187-191)

Ahmed AbdulQader Al-Bakeri, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia

Abdullah Ahmad Basuhail, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia

Abstract — Nowadays, many applications implemented for face detection and recognition are used to achieve different types of projects, whether they are to be used for attendance systems in schools or for the check-in and check-out of employees in an organization. The purpose of this paper is to propose a new notification system using face detection and recognition to notify the house owner of visitors by using the SMTP to send an email containing the names and phone numbers of those visitors. In this system, the camera detects and recognizes the persons in front of the door and then sends their personal information to the host. The theoretical and practical aspects of this system are provided as follows.

Keywords- *Face, Biometric, SMTP, Notification, Face recognition*

30. PaperID 310316120: AndorEstimator: Android based Software Cost Estimation Application (pp. 192-202)

Muhammad Zubair Asghar, Institute of Computing and Information Technology, Gomal University, D.I.Khan, Pakistan

Ammara Habib, Institute of Computing and Information Technology, Gomal University, D.I.Khan, Pakistan

Anam Habib, Institute of Computing and Information Technology, Gomal University, D.I.Khan, Pakistan

Syeda Rabail Zahra, Institute of Computing and Information Technology, Gomal University, D.I.Khan, Pakistan

Sadia Ismail, Institute of Computing and Information Technology, Gomal University, D.I.Khan, Pakistan

Abstract — The main aim of the proposed system is to assist the software development team to estimate the cost, effort and maintenance of the project under development. Android-based platform, namely MIT App Inventor is used for

the development of application, which contains visual block programming language. The current study has following uniqueness of (1) Accuracy of results, (2) user friendly environment (3) no such application is available on android platform to the best of our knowledge. Questionnaire regarding CoCoMo model is developed and circulated by using objective qualitative method. Findings: The estimation module of our application is quite important with respect to facilitating the students of software engineering for performing CoCoMo-based cost estimation easily, and enabling the software developers for performing software cost estimation easily. The cost estimator based on CoCoMo model is developed on android platform however, to the best of our knowledge no such application is available. This system can be used by business and educational stakeholders, such as students, software developers, and business organizations.

Keywords — *CoCoMo model; App Inventor; Cost estimation; Android*

31. PaperID 310316129: Survey of Keystroke Dynamics as a Biometric for Static Authentication (pp. 203-207)

Pranit Shinde, Dept. of Computer Engineering, Fr. Conceicao Rodrigues College of Engineering, Mumbai, India

Saideep Shetty, Dept. of Computer Engineering, Fr. Conceicao Rodrigues College of Engineering, Mumbai, India

Mahendra Mehra, Dept. of Computer Engineering, Fr. Conceicao Rodrigues College of Engineering, Mumbai, India

Abstract — Keystroke Dynamics is the study of a user's typing pattern based on the various timing information obtained when a key is pressed and released. It comes under Behavioral Biometrics and has been a topic of interest for authenticating as well as identifying users based on their typing pattern. There have been numerous studies conducted on Keystroke Dynamics as a Biometrics with different data acquisition methods, user base, feature sets, classification techniques and evaluation strategies. We have done a comprehensive study of the existing research and gave our own inference on the topic. In this paper we discuss where the Keystroke Dynamics research currently stands and what scope it has in the future as a biometric application.

Keywords - *Keystroke Dynamics, Behavioral Biometrics, User Authentication, Identification, Computer Security.*

32. PaperID 310316131: A Novel Supervised Approach to Detection of Shilling Attack in Collaborative Filtering Based Recommendation System (pp. 208-211)

Krupa Patel, Department of Information Technology, CSPIT, CHARUSAT, Anand, India.

Amit Thakkar, Associate Professor, Department of Information Technology, CSPIT, CHARUSAT, Anand, India.

Chandni Shah, Assistant Professor, Department of Information Technology, CSPIT, CHARUSAT, Anand, India.

Kamlesh Makvana, Assistant Professor, Department of Information Technology, CSPIT, CHARUSAT, Anand, India.

Abstract — Collaborative filtering is widely used recommendation algorithm to generate variety of recommendation for target users. With increasing popularity of collaborative filtering recommendation, number of users started to insert fake shilling profiles into the system. Due to shilling attack or profile injection attack, accuracy of collaborative filtering recommendation will reduce. This paper attempts to proposed method to detection of shilling attack in collaborative filtering recommendation system using supervised approach. Our proposed method use statistical parameters RDMA, DigSim and LengthVar to identify shilling attack profiles from genuine profile. These parameters are used to train the model for detection of attacker profiles. Then our proposed method will identify genuine profile those are classified as attacker profiles.

Keywords — *Recommendation System, Collaborative Filtering, Shilling Attack, Profile Injection Attack, Supervised Learning, Statistical parameters.*

33. PaperID 310316140: Privacy Preserving Data Classification using a New Heterogeneous Data Distortion (pp. 212-217)

J. Hyma (†), PVGD Prasad Reddy (††), and A. Damodaram (†††)

† Department of CSE, GIT, GITAM University, Visakhapatnam, INDIA

†† † Department of CS&SE, AU College of Engineering, Andhra University, Visakhapatnam, INDIA

††† Department of CSE, Sri Venkateswara University, Tirupathy, INDIA

Abstract - The new digital technology facilitates us to collect huge amount of data every day. Due to this tremendous growth in size and complexity, two important factors have got the increased attention of all the technology users. One is the complex data analysis that could be done using various data mining methods. The second is privacy concern of the individual towards their data. Privacy Preserving Data Mining (PPDM) is one such process that pays an equal attention towards these two factors. Though there are various techniques in PPDM process, there is no such existing technique that exerts the equal amount of importance on all the roles involved in communication. Our proposed model not only considers the various roles like data owners, data collectors and data users, but also applies the required set of heterogeneous constraints to obtain better privacy protection and better data usability. Heterogeneous constraints used in this work are proposed basing upon the owners willingness to publish the data and existing correlations and privacy analysis carried out by the anonymization framework of the data collector layer.

Keywords: *Privacy preserving data mining (PPDM), Heterogeneous constraints, Privacy preserving data classification.*

34. PaperID 29021627: Evaluating the Effects of Network Size and Nodes Mobility Speed on the Performance of TCP over Mobile Ad-Hoc Networks (pp. 218-227)

O. G. Aju, O. Oriola

Department of Computer Science, Faculty of Science, Adekunle Ajasin University, Akungba-Akoko, Ondo State, Nigeria

Abstract — The purpose for the design of Transmission Control Protocol (TCP) was to provide reliable end-to-end delivery of data over unsecured networks. Although, it is designed to be deployed in the traditional wired networks but recently, there has been an increase in its deployment over the wireless networks such as Mobile Ad-Hoc Networks (MANETs). This paper investigates the performance of various TCP variants in specified network scenarios in Mobile Ad hoc Networks (MANETs) using Reno, New Reno and SACK as case study under the Dynamics Source Routing (DSR) Protocol by observing the effects of some network designs on the performance of TCP variants in MANETs using throughput, delay and retransmission attempts as performance metrics. Application traffics were submitted to MANETs while the network size (number of nodes) and the nodes mobility speed were varied to create network models and the resulting throughput, end-to-end delay and retransmission attempts were observed to determine how the network size and the nodes mobility speed affects the performance of the TCP variants.

Index Terms— *Mobile Ad hoc Network, Transmission Control Protocol, Selective Acknowledgements, File Transfer Protocol, Hypertext Transfer Protocol, Voice over Internet Protocol.*

35. PaperID 29021672: Adaptive Fuzzy Control to Design and Implementation of Traffic Simulation System (pp. 228-246)

Laheeb Mohammed Ibrahim, Software Engineering, Mosul University, Collage of Computer Sc. & Math., Mosul, Iraq

Mohammed A. Aldabbagh, Software Engineering, Mosul University, Collage of Computer Sc. & Math., Mosul, Iraq

Abstract — In this paper a Fuzzy Adaptive Traffic Signal System (FATSS) was designed and implemented to improve optimization and compare fix time traffic light controller. FATSS allows the user to select input parameters and tune rule base to improve optimization and compare fix time traffic light controller. FATSS reducing the average waiting time for vehicles between 2% to 20%, and that indicate the adaptive traffic light controller based on fuzzy logic outperform is better when is compare with other fixed controller FATSS was built using C# language in Microsoft Visual studio 2010 development environment. The simulation is implemented by Simulation for Urban Mobility (SUMO).

36. PaperID 29021695: Secure Cooperative Intrusion Detection System for Mobile Ad-Hoc Network (pp. 247-250)

*Himanshu Kumar, Department of Information Technology, SRM University Kattankulathur Chennai
J. Godwin Ponsam, Asst. Professor, Department of Information Technology, SRM University Kattankulathur, Chennai*

Abstract - The Mobile Ad-Hoc Network does not have any fixed infrastructure so they rely on their neighbors to relay data packets over a network. Intrusion detection system in mobile ad-hoc network can be carried out in a distribution scenario due to absence of fixed infrastructure. This nature of MANET attracts the malicious users. Intrusion Detection System are the techniques to detect the malicious node. The objective of this project is to propose an Energy efficient system based on a cooperative IDS scheme to deal with intrusions in clustered mobile ad-hoc networks. We are analyzing the Energy Consumption of MANET by using present Protocols in terms of Packet dropping detection ratio, Mobility stability and Transmission Power Control etc.

Keywords: *Ad-hoc Network, IDS, Energy Consumption, MANET, Wireless Network*

37. PaperID 310316119: Ensuring Interoperability among Heterogeneous Devices through IoT Middleware (pp. 251-255)

*Muhammad Ahsan, M. Ramzan Talib, M. Umer Sarwar, M. Irfan Khan, M. Bilal Sarwar
Department of Computer Science, Government College University Faisalabad, Pakistan*

Abstract — Internet of Things provides truly ubiquitous and smart environment. The multilayer distributed architecture with a variety of different components together with end devices, applications and the association with its framework poses challenge. Internet of Things middleware actions as a joining link between the heterogeneous areas that communicate across heterogeneous edges. In this work, we study the interoperability issue between heterogeneous devices. We presented guidelines to handle the interoperability issue in Internet of Things. Furthermore, we have proposed architectural framework for Home Area Network.

Keywords - *Interoperability, Internet of things, Middleware, Heterogeneous devices*

38. PaperID 31031699: SQL Injection Attack Detection & Prevention over Cloud Services (pp. 256-261)

*Niharika Singh, Ajay Jangra, Upasana Lakhina, Rajat Sharma
Department of Computer Science and Engineering, University Institute of Engineering and Technology,
Kurukshetra University, Kurukshetra, India*

Abstract — Web servers which provide customer services are usually connected to highly sensitive information contained backend databases. The incrementing bar of deploying such web applications initiated in ranging the corresponding bar of number of attacks that target such applications. SQL Injection Attacks come about when data provided by external user are directly included in SQL query but is not properly validated. The paper proposes a novel detection & a prevention mechanism of SQL Injection Attacks using three-tier system. As the methodology is concerned over static, dynamic & runtime detection and prevention mechanism which also filters out the malicious queries and inspires the system to be well prepared for the secure working environment, regardless of being concerned over the database server only. The cloud proposes the services like SaaS, IaaS, PaaS, DaaS, EaaS. As previous solutions are achieved for the database queries for DaaS service only, but this paper enhances the scope of other services as well. It adapts to maintain security of the whole system even when it is for any of the cloud platforms. The solution includes detection & filtration that reduces attacks to 80% in comparison to other algorithms.

Keywords — *Cloud computing; Cloud Security; Architecture, design; Cloud services; Deployment models; SQL Injections;*

39. PaperID 310316125: Survey on Issues in Wireless Sensor Networks: Attacks and Countermeasures (pp. 262-269)

*Rangstone Paul Kurbah, Bobby Sharma
Assam Don Bosco University, Guwahati, Assa*

Abstract — Wireless Sensor Networks have become popular day by day. They find their applications in numerous areas. These networks, however, have some constraints like the physical size (that they must be compact), energy (that minimum energy must suffice them for long hours), memory space (that they should effectively work with just minimum memory space installed on them), and above all that their construction cost must be minimum. Due to these constraints they face some security issues. Securing the data that flows through these networks must be of paramount importance and the security issues that are faced by these networks must be addressed in order to enhance their reliability and usage. This paper focuses on the security aspects of Wireless Sensor Networks. It presents the general characteristics of Wireless Sensor Networks, their constraints, their security goals, the threat models, the different types of attack on WSNs and their defensive measures.

Keywords: Attacks, Defensive Measures, Nodes, Security, Wireless Sensor Network (WSN).

40. PaperID 29021641: Syntactical Knowledge and Sanskrit Memamsa Principle Based Hybrid Approach for Text Summarization (pp. 270-275)

*D. Y. Sakhare (1, 2), Raj Kumar(3)
(1) Bharatividyapeeth Deemed University's College of Engineering, Pune, MS, India
(2) MIT Academy of Engineering, Alandi, Pune, MS, India
(3) DIAT, Khadakwasala Pune, MS, India*

Abstract - The proposed approach works towards integrating syntactic knowledge and sentence fusion for abstractive multi-document summarization system. A fuzzy logic system, based on the “Paninian” Parts of Speech Tagging, is used to extract the syntactical knowledge-based informative words from English the documents. The sentences containing the informative words are selected for the further processing of abstractive summary generation. The sentence formation for the abstractive summarization is done using a neural network with features based on the Memamsa principles of the Sanskrit language. The features, such as “Upakram-Upsanhar,” “Abhyas,” “Apurvata,” “Phalam,” “Sthan,” “Prakaran” and “Samakhya” are used to form meaningful sentences. These features and the target summary of each document are given as input to train the neural network. The neural network trains the system based on the target summary of a set of documents with the same information to generate an abstractive summary for a new cluster of documents. The system performance is measured on a real data set and the DUC 2002 data set using ROUGE-1 and ROUGE-2 scores and the F-measure. The proposed Fuzzy- NN approach performs better than the existing techniques.

Keywords: Text summarization, Informative Word, Sentence Formation, Memamsa principles, Fuzzy NN, ROUGE

41. PaperID 31031602: The Smartcane for Blind People an Electronically Smart Stick to Aid Mobility (pp. 276-285)

*M. Asad Hussain, M. Ghazanfar Ullah, Atif Fareed, Basit Sohail
Department of Electrical Engineering, Usman Institute of Technology – Pakistan*

Abstract — This paper is focused about the development of a — Micro-controller based Smart White Cane || A.K.A. —The Smartcane || and its comparison, based on performance and usability, with other existing models. Our main contribution is to enhance the capabilities of existing models of micro-controller based white stick for blind persons, due to their practical limitations. The developed project serves the best solution to overcome the difficulties of blind people, so that they can easily mobilize themselves, be a more successful part of society. The developed

project facilitates blind persons in a manner that they can handle any obstacle, wet material, uneven surface, etc. Our main objective was to reduce the size of the presented model by integrating the circuits and making it a compact and portable stick for users. Also, we emphasize on the range of the modules and sensors to increase the efficiency and usability of the prototype model. The system accompanied a portable unit that can easily be carried and operated by a visually impaired user. It could easily be incorporated into a walking cane. The salient features of the developed prototype are ultrasonic sensor for obstacle detection, water probe for mud and water detection, I.R. for ditch detection, G.P.S, G.S.M. module, signal-to-speech module, speaker or headset, and portability (size and power). The experimental results shows that the developed prototype is much more efficient and usable in varying situations for a blind person as compared to the ordinary white sticks while affordable and cost effective at the same time.

Keywords – Blind, Mobility Aid, Smartcane, Microcontroller, GPS, GSM, Ultrasonic senor, IR sensor.

42. PaperID 31031612: E-Commerce Framework Based on Evaluation of Data Mining and Cloud Computing (pp. 286-295)

*Mohd Muntjir, College of Computers and Information Technology, Taif University, Taif, Saudi Arabia
Ahmad Tasnim Siddiqui, College of Computers and Information Technology, Taif University, Taif, Saudi Arabia*

Abstract - This paper is a description about the application of e-commerce and data mining with cloud Computing. It emphasizes how data mining is used for e-commerce in combination of cloud computing systems. Data Mining is a process of separating possibly useful information from available raw data. It's also describing that How SaaS is very useful in cloud computing. The combination of data mining techniques into normal day-to-day actions has become common part. Businesses and advertising have become more active through the use of data mining functionalities to deduct the overall costs. Data mining operations can develop much more demographic information respecting customers that was basically not known or hidden in the desired data. It has basically seen enhancements in data mining techniques proposed to such activities as identifying criminal activities, fraud detection, suspects, and indication of potential terrorists. On the whole, data mining systems that have been designed and developed to data for grids, clusters, and distributed clusters have considered that the processors are the limited resource, and hence distributed. When processors become accessible, the data is transferred to the processors.

Keywords: Data Mining, e-commerce, cloud computing systems, data mining and cloud computing, (SaaS) Software-as-a-Service.

43. PaperID 31031618: Radial Basis Polynomial Kernel (RBPK): A Generalized Kernel for Support Vector Machine (pp. 296-315)

Ms. Hetal Bhavsar (1), Dr. Amit Ganatra (2)

(1) Assistant Professor, Department of Computer Science & Engineering, The M. S. University of Baroda, Vadodara, India

(2) H. O. D., Computer Engineering Department, Charotar University of Science & Technology, Changa, Dist. Anand, India.

Abstract - Support Vector Machine (SVM) is a novel machine learning method, based on the statistical learning theory and VC (VapnikChervonenkis) dimension concept. It has been successfully applied to numerous classification and pattern recognition problems. Generally, SVM uses the kernel functions, when data is non-linearly separable. The kernel functions map the data from input space to higher dimensional feature space so the data becomes linearly separable. In this, deciding the appropriate kernel function for a given application is the crucial issue. This research proposes a new kernel function named — Radial Basis Polynomial Kernel (RBPK) || which combines the characteristics of the two kernel functions: the Radial Basis Function (RBF) kernel and the Polynomial kernel and proves to be better kernel function in comparison of the two when applied individually. The paper proves and makes sure that RBPK confirms the characteristics of a kernel. It also evaluates the performance of the RBPK using Sequential Minimal Optimization (SMO), one of the well known implementation of SVM, against the existing kernels. The simulation uses various classification validation methods viz. holdout, training vs. training, cross-validation and random sampling methods with different datasets from distinct domains to prove the usefulness of RBPK. Finally, it

concludes that the use of RBPK results into better predictability and generalization capability of SVM and RBPK can become an alternative generalized kernel.

Keywords: Support vector machine; kernel function; sequential minimal optimization; feature space; polynomial kernel; and Radial Basis function

44. PaperID 31031620: MOiD (Multiple Objects incremental DBSCAN) – A paradigm shift in incremental DBSCAN (pp. 316-346)

Neha Soni (1), Dr. Amit Ganatra (2)

(1) Computer Engineering Dept., SVIT, Vasad, Gujarat, India

(2) Faculty of Tech. & Engg., CHARUSAT, Changa, Gujarat, India

Abstract - Mining an unprecedented increasing volume of data is a herculean task. Many mining techniques are available and being proposed every day. Clustering is one of those techniques used to group unlabeled data. Among prevailing proposed methods of clustering, DBSCAN is a density based clustering method widely used for spatial data. The major problems of DBSCAN algorithm are, its time complexity, handling of varied density datasets, parameter settings etc. Incremental version of DBSCAN has also been proposed to work in dynamic environment but the size of increment is restricted to one data object at a time. This paper presents a new flavour of incremental DBSCAN which works for multiple data objects at a time, named MOiD (Multiple Objects incremental DBSCAN). MOiD has been experimented on thirteen publicly available two dimensional and multi-dimensional datasets. The results show that MOiD performs significantly well in terms of clustering speed with a minor variation in accuracy.

Keywords - Incremental Clustering, DBSCAN, Density based clustering, region query, clustering

45. PaperID 31031629: Wavelet based OFDM with ICI Self Cancellation for Underwater Acoustic Communications (pp. 347-352)

Naresh Kumar, Member, IEEE and B. S. Sohi, Sr. Member, IEEE

University Institute of Engineering & Technology (UIET), Panjab University Chandigarh, India

Abstract — There are many research challenges in underwater acoustic communication environment such as large delay spread, ocean waves, motion of transmitter/receiver, Doppler spread etc. OFDM has potential to combat with many such problems, but it is also deteriorated by Inter Carrier Interference and high peak to average power ratio. Conventional OFDM is spectral inefficiency as it uses cyclic prefixing which consumes approximately 20% of available bandwidth. ICI self-cancellation technique performs better for ICI problems. As it transmits redundant data on adjacent subcarriers which makes some subcarriers idle, hence, ICI is reduced at the cost of bandwidth. In this paper, a Wavelet based OFDM with ICI cancellations is proposed to counter the problem of ICI. Use of Wavelets reduces the need for cyclic prefixing thereby making it more spectral efficient and wavelets also help in maintaining orthogonality between subcarriers which further improves its ICI performance. Simulation results show that proposed technique performs better in terms of bit error rate (BER) as compared to conventional OFDM.

Index Terms — OFDM, Wavelets, BER, Self-Cancellations, ICI

46. PaperID 31031632: A Method for Mining Social Media to Discovering Influential Users (pp. 353-365)

Hosniyeh S. Arian (1), Omid R. B. Speily (2)

(1) Department of Computer Engineering and Information Technology, Islamic Azad University, Qazvin, Iran.

(2) Department of Computer Engineering and Information Technology, Urmia University of Technology, Urmia, Iran

Abstract - Influential users who diffuse information and their followers have interest to this information finally they can maximize diffusion in social networks. Influential users have different influence in diversity domain specificity

for instance user may have strong influence in a special topic and another topics have weak influence. So a proposed method presented for identifying influential users based on domain specificity in this paper. This method identified influential users based on domain specificity that features of user's profile and user's actions (e.g. retweet) that influence on diffusion determined by "multiple regression" and user's contents categorized based on keywords by "TF-IDF" and finally influential users identified by "Tree Regression" based on domain specificity in this paper. The detail of this method discussed the fallowing of paper. In order to evaluate the proposed method on Twitter offer application program interface. 420 users selected randomly, they fallow their friends, join to different groups, and generated diversity tweets on Twitter. The main feature, which distinguishes this method from the previously reported methods, is in two key respective. First previous studies have quantified influence in terms of network metrics for instance number of retweet or page rank, our proposed method measured influence in terms of the size Tree Regression. Second the focuses of previous studies were based on the structural of diffusion and feature of content but Influential users have different influence in diversity domain specificity so in our proposed method focused on this feature. Results showed that accuracy of proposed method is 0.69.

Keywords: Social networks, Categorized, Influence, Content, Diffusion, Domain specificity.

47. PaperID 31031642: StudentPIMS: A Smartphone-Based Personal Information Management System for Students (pp. 366-380)

Irfan Ullah (a,b,), Shah Khusro (b), Habib Un Nabi (a), Rafi Ullah (a)*

(a) Department of Computer Science, Shaheed Benazir Bhutto University, Sheringal, 18050, Pakistan

(b) Department of Computer Science, University of Peshawar, Peshawar, 25120, Pakistan

Abstract - Curricular and co-curricular activities are among the major responsibilities that require proper attention from the students in order to achieve different goals and objectives regarding their bright future. Because of the mismanagement of keeping personal information about these activities, most of students are unable to remember these tasks while they are busy in their studies and therefore, fail to perform these activities at the right time. To handle this issue, they adopt several means including SMS drafts, reminders, sticky notes, notebooks, dairies, and laptops etc., which are limited and unable to fully support students because of several problems including their storage, search, and retrieval. With the availability and wide-spread adaptation of Android and Smartphones, researchers and developers started thinking of new and innovative ways of managing personal information of people especially students. Today, several apps are available on Google Play for managing personal information of students. However, the existing solutions have limitations including bulky user interfaces especially when the stored information exceeds a certain limit, usability, privacy, and requiring access to Internet for accessing certain services, which becomes a barrier to students especially to those living in rural areas of developing countries where access to Internet is among the major issues. Keeping in view these limitations, we have designed and developed StudentPIMS - a simple and usable Android app that allows students to easily manage personal information about these activities without suffering from cognitive overload caused by existing solutions. We have compared our solution with the existing solutions using some evaluation metrics as well as conducted a survey research among users of the app. Results show that StudentPIMS outperforms the available solutions especially in terms of usability, privacy, and low resource consumption.

48. PaperID 31031652: Contribution to a proportional sharing out of IaaS resources for service adaptation with users services according its profile in cloud computing (An equity based approach) (pp. 381-395)

KANGA Koffi, Ecole Doctorale Polytechnique de l'Institut Nationale Polytechnique Félix Houphouët Boigny (EDP/INPHB), Côte D'ivoire UMRI 78 Laboratoire de recherche en informatique et télécommunication

GOORE Bi Tra, Institut Nationale Polytechnique Félix Houphouët Boigny (INPHB), Côte D'ivoire, Laboratoire de Mathématiques et des Nouvelles Technologies de l'Information

BABRI Michel, Institut Nationale Polytechnique Félix Houphouët Boigny (EDP/INPHB), Côte D'ivoire, Laboratoire de Mathématiques et des Nouvelles Technologies de l'Information

Abstract - Cloud computing ensures the allowance of resources consumption to the user, by paying for it as he will do for other basic services as water and electricity. In this article we propose an IaaS resource adaptation technique (space

capacity) necessary for the SaaS and PaaS in order to improve their functioning in terms of storage capacity by taking into account users' profile. In that way, a proportionality coefficient has been defined, and used for this adjustment and also by taking into account previous IaaS space occupations proportion for each service of cloud. Our contribution is based on the setting up of an allocation technique supported by an algorithm allowing its achievement. The outcome results of the implementation of the algorithm show that our method allows a propositional sharing out of the resources. Therefore the IaaS space should be adapted to the users' service.

Keywords: Cloud computing, Users profile, resources allocation, IaaS resources adaptation.

49. PaperID 31031654: Enhanced Data Security in Network Environment (pp. 396-405)

Ram Krishna Akuli, Dr. J. Durga Prasad Rao, Dr. Satyendra Kurariya

(1) Scholar CVRU, Bilaspur

(2) Additional Director & HOD (Computer Science Department), Shri Shankaracharya Mahavidyalaya, Junwani, Bhilai

(3) Head, Computer Science Department, Mata Gujari College, Jabalpur

Abstract - This study is based on the development of a new secure protocol for remote calls. The secure protocol design specification and descriptions are analysed comparing them with the existing protocols. The protocol is designed in a simple way with in built security features. Cryptographic modules can be exchanged due to the flexibility of the new approach depending on various issues and security matters. The developed protocol in this study is platform independent. The security levels of the new secure protocol are properly analysed with desired results. Comparisons with other existing technologies like CORBA or the RMI were also addressed. The results show that creation of a secure network protocol universally acceptable. Although all the bugs and security issues were not addressed as they keep evolving on a daily basis.

Keywords: - Cryptographic Protocol, Secure Remote Protocol, Network Security

50. PaperID 31031661: Security Concerns with Open Research Issues of Present Computer Network (pp. 406-432)

Geetanjali Rathee, Hemraj Saini

Department of Computer Science and Engineering, Jaypee University of Information Technology, Wagnagh, Solan-173234, Himachal Pradesh, India

Abstract - Present networks are the mainstay of modern communication. The existence of networks is enriching our society in countless different ways. Now days, wireless mesh network is considered as an auspicious technology for posing self-healing, organizing and configurable capabilities but one of the foremost challenge in the enterprise of these networks is their susceptibility to security assaults (eavesdropping, network layer attacks and denial of service). In order to overcome against these assaults, several security anxieties are proposed but authentication is taken as an important parameter to provide a secure communication. In this chapter, a review is discussed from origin to the current networking technology i.e. WMN. In addition to this, WMN security is concerned with recent applications such as smart grids, intelligent transportation system, multimedia systems etc. further a clear overview of security with respect to each layer is elucidated and finally the chapter is ruined by outlining the future work which is the next step of this research

51. PaperID 31031662: Performance-aware Cloaking Algorithm for Optimizing Anonymous Location-based Services (pp. 433-439)

Dileep Kumar, Department of Information Media, The University of Suwon, Hwaseong-si South Korea

Abstract - The prevailing infrastructure of ubiquitous computing paradigm on the one hand making significant development for integrating technology in the daily life but on the other hand raising concerns for privacy and

confidentiality. As Location based services (LBS) equip users to query information specific to a location with respect to temporal and spatial factors thus LBS in general while Location Anonymizer, core component of privacy preservation models, in particular put under extreme criticism when it comes to location privacy, user confidentiality and quality of service. For example, a mobile or stationary user asking about his/her nearest hospital, hotel or picnic resort has to compromise their exact location information. Here in this paper we are addressing the significance of our proposed index optimized cloaking algorithm for Location Anonymizer with respect to performance, quality and accuracy which can be smoothly integrated into existing location anonymity model for privacy preservation. The main idea is to deploy R-tree based indexing scheme for Location Anonymizer to make best use of available computing resources. In accordance with the proposed approach, next step is to develop an index optimized cloaking algorithm which can cloak spatial region effectively and efficiently on behalf of R-tree based indexing scheme .Finally we will quantify the benefits of our approach using sampled results through experiments that the proposed cloaking algorithm is scalable, efficient and robust to support spatio-temporal queries for location privacy.

52. PaperID 31031671: Encrypting Grayscale Images using S8 S-Boxes Chosen by Logistic Map (pp. 440-444)

Tariq Shah, Ayesha Qureshi

Department of Mathematics, Quaid-i-Azam University, Islamabad, 44000, Pakistan

Abstract - In the present manuscript, we will design an encryption algorithm for grayscale images that is based on S8 S-boxes transformations constructed by the action of symmetric group S8 on AES S-box. Each pixel value of the plain image is transformed GF (2^8) into with a dissimilar S8 S-box chosen by using the logistic map. In this way, there are 40,320 possible choices to transform a single pixel of the plain image. By applying the generalized majority logic criterion, we will establish that the encryption characteristics of this approach are superior to the encoding performed by AES S-box or a single S8 S-box.

Keywords: AES S-box, S-boxes, logistic map, generalized majority logic criterion.

53. PaperID 31031677: A Dynamic Media Access Control Protocol for Controlling Congestion In Wireless Sensor Network By Using Fuzzy Logic System And Learning Automata (pp. 445-460)

Foroogh Karimi, Mansour Esmaeilpour

Department of Computer Engineering, Hamedan Branch, Islamic Azad University, Hamedan, Iran

Abstract - One of the existing layers in the reference model whose designing is of particular complication is the control layer of access to MAC media, it's proper designing causes to reduce interference and consequently to reduce energy consuming and to increase the network efficiency. In the recommended method, our focus is on the networks being multi-channel in order to distribute the network current through the different channels. In the first step of the research, we have used a layering structure for a better management of the network so that we could prevent congestion via the network management. This management is performed through using Fuzzy logic system logic system. The output of our Fuzzy logic system is the election of the best and most appropriate choice in order to continue route finding. But if a congestion of one incident takes place, we possess learning automata for assigning the channel searchingly for balancing the channel current. Using the resemblance maker of NS2, the results of the resemblance-making maintain that the recommended method has improved more greatly than the two basic protocols and could achieve the quality parameters of route finding services.

Keyword: Wireless sensor networks, Congestion control, Multichannel, Fuzzy logic system, Learning Automata

54. PaperID 310316103: Presenting a Model to Meet the Pathology Component in the Implementation of Beyond Component Processes in Distributed Integrated Information Systems (pp. 461-470)

Masoud Rafighi, Yaghoub Farjami

Department of Computer Engineering and Information Technology, University of Qom, Qom, Iran

Abstract - making all the applications in an enterprise work in an integrated manner, so as to provide unified and consistent data and functionality, is a difficult task because it involves integrating applications of various kinds, such as custom-built applications (C++/C#, Java/J2EE), packaged applications (CRM or ERP applications), and legacy applications (mainframe CICS or IMS). Furthermore, these applications may be dispersed geographically and run on various platforms. In addition, there may be a need for integrating applications that are outside the enterprise. According to the problems of adding application to organization and keep integration between them, in this paper, we studied the ways of integration between systems of organization. Then consider the Problems of models and emphasize on crucial need to create an ideal model for optimal architecture which meets the needs of the organization for flexibility, extensibility and integration of systems. Finally proposed a model which in addition doing comprehensive processes between the components easily in distributed systems, it does not have the problems of previous models. Since components are vulnerable in sending beyond component processes, so in this article we decided to introduce a model of pathology components to resolve the implementation of beyond component processes.

Keywords: ESB, Data-centric architecture, architecture Component-based, Plug in architecture, distributed systems.

55. PaperID 310316112: A Novel Energy Efficient Connected Target Coverage Heuristic in WSN (pp. 471-479)

Sunita Gupta, Ph.D. Scholar, Suresh Gyan Vihar University, Jaipur

Dr. K. C. Roy, Professor, Kautilya Institute of Technology & Engineering, Jaipur

Dr. Dinesh Goyal, Professor, Suresh Gyan Vihar University, Jaipur

Sakar Gupta, Associate Professor, Kautilya Institute of Technology & Engineering, Jaipur

Abstract - Wireless Sensors Networks (WSNs) are able to work in insensitive environments where real observations by human being are dangerous, incompetent and sometimes not feasible. A most significant characteristic of a WSN application is lifetime. Wireless sensor network can be used till they can sense and communicate the sensed data to base station. Sensing as well as communication, both are important functions and they use energy .Energy management and scheduling of sensors can effectively help in rising the networks lifetime. Energy efficiency in a region monitored by a sensor network is achieved by dividing the sensors into cover sets. Every cover set is able to monitor the targets for a definite time period. At a time only single cover set is in active state and rest others are in low power sleep state. Thus energy is preserved and lifetime of Wireless Sensor Network is increased. Creating the greatest number of such set covers is proved to be an NPC problem. An energy minimization heuristic called Q-Coverage P-Connectivity Maximum Connected Set Cover (QC-PC-MCSC) is proposed. Functioning of Sensor nodes is scheduled in such a manner that they are having Q-Coverage and P-Connectivity constraint and thus they improves the working duration of Wireless Sensor Network. A comparative study of performance of QC-PC-MCSC and existing heuristic is also done over Energy Latency Density Design Space for Wireless Sensor Network.

Keywords:- Wireless Sensor Network, Connected Target Coverage, Network Lifetime, Cover Set, Coverage, Connectivity, Q-Coverage, P-Connectivity.

56. PaperID 310316115: A Novel Hybrid Encryption Scheme to Ensure Hadoop Based Cloud Data Security (pp. 480-484)

Danish Shehzad (1), Zakir Khan (2), Hasan Dağ (3), Zeki Bozkuş (4)

*(1, 4) Department of Computer Engineering, (3) Department of Management Information Systems,
Kadir Has University, Istanbul, Turkey*

(2) Department of Information Technology, Hazara University, Mansehra, Pakistan

Abstract - Cloud computing and big data have provided a solution for storing and processing large amount of complex data. Despite the fact that they are quite useful, the threat to data security in cloud has become a matter of great concern. The security weakness in Hadoop, which is an open source framework for big data and cloud computing, has setback its deployment in many operational areas. Different symmetric, asymmetric, and hybrid encryption schemes have been applied on Hadoop for achieving suitable level of data security. In this paper a novel hybrid encryption scheme, which combines symmetric key algorithm using images as secret keys and asymmetric data key encryption using RSA, is proposed. The suggested scheme reduced the overhead of the secret key computation cycles as compared to the other

existing encryption schemes. Thus, it is safe to claim that the proposed scheme retains adequate security level and makes data encryption more efficient.

Keywords: Hadoop, Hadoop distributed file systems (HDFS), Matlab, Data encryption scheme (DES), RSA.

57. PaperID 310316118: Enhancing Users' Satisfaction Using an Agent-Based Negotiation System (pp. 485-496)

Omid R. B. Speily (1), Yosra Bahrani (2), Negin Razavi Rajayi (2)

(1) Department of Information Technology & Computer Engineering, Urmia University of Technology, Urmia, Iran

(2) Department of Information Technology & Computer Engineering, AmirKabir University of Technology, Tehran, Iran

Abstract - The increasing importance of operating automated systems arises with emerging competitive e-commerce environment. Nowadays, operating automated systems used in conducting all business transactions are enhanced substantially to achieve beneficial trade and decrease frequent messaging overhead of transactions. In spite of the highly competitive electronic marketplace, it is necessary to design a system which automates tasks including group negotiation and, payment and delivery. In this paper, we apply the purchasing groups to enhance the bargaining power of customers still satisfying all users' needs and preferences. We propose a flexible system called UUT-Trade to purchase laptop computers. This system uses a novel negotiation algorithm which diminishes all prices offered by potential sellers as much as possible, and then users will have the chance to choose between potential sellers by performing a weighted voting. Unlike similar systems which also exploit group purchasing, this system suggests no scarification of buyers' needs.

Keywords: Negotiation, Automation, Scarification, UUT-Trade, AHP tree.

58. PaperID 310316123: Parallelizing K-Way Merging (pp. 497-503)

H M Bahig (1, 2) and Ahmed Y Khedr (1, 3)

(1) College of Computer Science and Engineering, Hail University, Hail, KSA

(2) Department of Mathematics, Faculty of Science, Ain Shams University, Cairo, Egypt

(3) Systems and Computer Department, Faculty of Engineering, Al-Azhar University, Cairo, Egypt

Abstract — The k-way merging problem is to find a new sorted array as an output from k sorted arrays as an input. In this paper, we consider the elements of the k sorted arrays are data record, where the value of the key for each record is a serial number. The problem is used to design efficient external sorting algorithm. We proposed two optimal parallel algorithms for k merging. The first one is based on merging k sorted arrays of n records in a new sorted array of length n. The second one is based on merging k sorted arrays of n records in a new sorted array of length n+o(n) which is called padded merging. The running time for each algorithm is O(log n) and O(1) under EREW and CRCW PRAM respectively.

Keywords - merging; k-merging; padded merging; PRAM; optimal algorithm; parallel algorithm.

59. PaperID 310316130: Extended Smart Metering Display for Improved Energy Economy (pp. 504-512)

Nisar Ahmed (1), Muzafar Khan (2), Muhammad Tahir (3), Shahid Yousaf (1)

(1) School of Engineering, Blekinge Institute of Technology, Karlskrona, Sweden

(2) College of Computer and Information Sciences (Muzahmiyah Branch), King Saud University, Riyadh, Saudi Arabia

(3) Faculty of Computing and Information Technology, University of Jeddah, Jeddah, Saudi Arabia

Abstract - Human dependency on technology is increasing day by day and environmental conditions are getting worse as a result. Energy consumption is increasing while the traditionally available energy sources like oil and gases are depleting. One of the major consumers is the domestic consumer, who plays the least part in energy management. One

way to increase efficiency in energy management is, therefore, to pass part of it to the domestic consumer, what is known as self-management. For the consumers to do self-management, they require the relevant information pertaining to their consumption patterns. Smart heat meters are already being used to provide this information. However, they are still being under-utilized in terms of their capability. In this research work an Extended Smart Metering Display (ESMD) is proposed; it is based on the interviews conducted with the representatives of smart heat meter manufacturers, District Heating (DH) providers and domestic consumers of DH in the Blekinge county of Sweden. The proposed ESMD was evaluated by the member companies of Swedish District Heating Association and domestic consumers in the workshop conducted for this purpose. The proposed ESMD may help the domestic consumers in monitoring their energy consumption on real-time basis, and improving their energy consumption behavior. It is also suggested that how it can be made more financially viable for the energy consumers and providers during the peak hours, if the proposed system is used.

Keywords: consumer behavior measurement, district heating, energy economy, metering display, smart heat meter

60. PaperID 310316132: Classifying Facial Expressions using DWT, Moments and Genetic Algorithm (pp. 513-522)

M. Mahadevi (1), Dr. C. P. Sumathi (2)

(1) Research Scholar (M. S. University) & Asst. Professor, SDNB Vaishnav College for women, Chennai, Tamilnadu, India

(2) Associate Professor & Head, Department of computer science, SDNB Vaishnav College for women, Chennai, Tamilnadu, India

Abstract - Facial expressions are the actions of the thoughts that arise in a mind. Such expressions are categorized as simple basic and complex expressions which are a mixture of two or more expressions. This research focuses on identifying the basic expressions and classifying them based on Naïve Bayes classifier. The database considered for the research is Japanese Female Facial Expression (JAFFE) consisting seven expressions happy, sad, disgust, fear, angry, neutral and surprise. The image is pre-processed using Discrete Wavelet Transform (DWT) and created a feature set containing spatial statistical features of the facial parts and moments of the DWT image. The features were selected using genetic algorithm and classified the database using Naïve Bayes classification to acquire an overall accuracy rate of 92.5%.

Keywords: Spatial Statistical features, DWT, Genetic algorithm, Naïve Bayes

61. PaperID 310316141: A Modern Approach to Integrate Database Queries for Searching E-Commerce Product (pp. 523-531)

*Ahmad Tasnim Siddiqui, College of Computers and Information Technology, Taif University, Taif, Saudi Arabia
Mohd. Muntjir, College of Computers and Information Technology, Taif University, Taif, Saudi Arabia*

Abstract - E-commerce refers to the utilization of electronic data transmission for enhancing business processes and implementing business strategies. Explicit components of e-commerce include providing after-sales services, promoting services/products to services, processing payment, engaging in transaction processes, identifying customer's needs, processing payment and creating services/products. In recent times, the use of e-commerce has become too common among the people. However, the growing demand of e-commerce sites have made essential for the databases to support direct querying of the Web page. This re-search aims to explore and evaluate the integration of database queries and their uses in searching of electronic commerce products. It has been analyzed that e-commerce is one of the most outstanding trends, which have been emerged in the commerce world, for the last decades. Therefore, this study was undertaken to ex-amine the benefits of integrating database queries with e-commerce product searches. The findings of this study suggested that database queries are extremely valuable for e-commerce sites as they make product searches simpler and accurate. In this context, the approach of integrating database queries is found to be the most suitable and satisfactory, as it simplifies the searching of e-commerce products.

Keywords: E-commerce product search, e-commerce, query optimization, business processes, Query integration

62. PaperID 310316144: Evaluation of Machine Vision for Robot Navigator: Mini Review (pp. 532-540)

Arefe Esalat Nejad

Young Researchers and Elite Club, Baft Branch, Islamic Azad University, Baft, Iran

Abstract - Machine vision (MV) is the technology and methods used to provide imaging-based automatic inspection and analysis for such applications as automatic inspection, process control, and robot guidance in industry. This paper presents some of the underlying concepts and principles that were key to the design of our research robots. Vision is an ideal sensor modality for intelligent robots. It provides rich information on the environment as required for recognizing objects and understanding situations in real time. Moreover, vision-guided robots may be largely calibration-free, which is a great practical advantage. Three vision-guided robots and their design concepts are introduced: an autonomous indoor vehicle, a calibration free manipulator arm, and a humanoid service robot with an omnidirectional wheel base and two arms. Results obtained, and insights gained, in real-world experiments with them are presented. Researchers and developers can take it as a background information for their future works.

Keywords: *Machine vision (MV), Intelligence robots, human service, Robot guidance*

63. PaperID 31031694: Significant Approach for Detaining Unpromising Contestant for Mining Pattern Based on Profit (pp. 541-544)

Vijay Kumar Verma, Lord Krishna College of Technology Indore

Kanak Saxena, Ph.D., Samrat Ashok Technological Institute, Vidisha M.P

Abstract - Todays every business organizations needs profit. Professional might give attention on recognizing its most treasured consumers who give a major portion of the profits to the business. Frequency based mining of items do not fulfill all are the requirement of business. They only provide the information that an item has high low frequency based on a given value. There is one important factor profit has to be consider by every business. In past year a lot of method have been developed for mining profit based pattern but efficiency, accuracy and scalability are important factor that has always to be considered. In this paper we proposed a significant approach for detaining unpromising contestant for mining profit based pattern. The proposed approach mine profit based pattern accurately and remove all unpromising contestant at different levels.

Keywords: *Profit, Pattern, unpromising, frequency, efficiency*

64. PaperID 31031676: Scalable and Secure Network Storage in Cloud Computing (pp. 545-551)

Muhib Ahmad Khan, M. Munwar Iqbal, Fahad Ubaid, Rashid Amin, Asima Ismail

Department of Computer Science, University of Engineering and Technology Taxila Pakistan

Abstract - Cloud Computing is a newly born type of computation, which depends on the shared resources of the network. Cloud Computing term discovered from that time when the system can access the different types of applications as well as different types of services remotely. Cloud Computing is the unique, next generation of IT architecture, in which computation is done on the open network shared resources, which create a security risk. In comparison to the existing conventional infrastructure, The IT services come under the IT expert control. In a market there is a different type of service provider using cloud computing features offers many different services like virtualization, applications, servers, data sharing, and try to the reduce client-side computation overhead. Nevertheless, most of these services are outsourced to the third party, which creates the risk of data confidentiality as well as the data integrity. These days cloud computing, and its security is the hot topic for the research. In this paper, a new model proposed for storage data on the network for the secure data storage on the cloud server, which achieve the security, availability, confidentiality and integrity.

Keywords - *Cloud Computing, Data Integrity & Security, Data Confidentiality & Availability*

65. PaperID 310316139: HSAG-FC: Hybrid of Simulated Annealing with Genetic algorithm and Fuzzy Classification for IDS (pp. 552-561)

Mrs. J. Lekha, Department of Computer Science, Avinashilingam Institute for Home Science and Higher Education for Women & Sri Krishna Arts and Science College, Coimbatore, Tamil Nadu

Dr. G. Padmavathi, Department of Computer Science, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, Tamil Nadu

Abstract - Nowadays signature attacks are termed as very big problem because it leads to software vulnerability. Malware writers confuse their malicious code to malicious code detectors such as Signature-based detection. However, it fails to detect new malware. This research article addresses the signature based intrusion detection from Intrusion Detection (IDS) systems. The proposed hybrid techniques for Generation of Signature are done using Genetic Algorithm (GA) and Simulated Annealing (SA) approaches. For this, signature-set in execution statements are selected by using simulated annealing and genetic algorithm, which produce the optimal solution of selection. Then the generated signatures are matched with IDS by using the two pattern matching techniques, namely (i). Finite state automaton based search for Single Pattern matching technique and (ii) Rabin Karp string search algorithm for multiple pattern matching technique. These techniques are used to match the signature as in an effective manner. In addition to this the Fuzzy Logic classification is used to find the degrees of truth of vulnerability for classification. The aim of the proposed work is to improve the final resultant accuracy in compared to existing techniques. The proposed Rabin Karp- fuzzy logic system returns the higher performance metrics namely precision is 88% and Recall is 80% and in open source dataset it contains 30 vulnerabilities this proposed worked well in detecting 28 vulnerabilities/ defect, the accuracy of this proposed is 94.27%.

Keywords: Degrees of truth, Finite state automaton, Fuzzy logic, Genetic algorithms, Intrusion Detection (IDS) systems, Optimization, Signature Generation, Signature matching, Simulated Annealing, Traffic detection.

66. PaperID 310316110: A Novel Technique for Jobs Scheduling In Cloud Computing Systems (pp. 562-568)

Muneer Bani Yassein, Yaser Khamayseh, Ali Hatamleh

Department of Computer Science, Jordan University of Science and Technology, Irbid, Jordan

Abstract — Recently, cloud computing has occupied a large place in the world, especially in the field of information technology. It is characterized as mainly rely on the Internet to provide services for organizations and consumers and to take advantage of resource sharing, in addition to that it is associated with many of the central remote servers to maintain user data, so it has become an effective way that will allow the world to use the many kind of applications without making an effort to be downloaded. Many job scheduling algorithms have been proposed to achieve both customer satisfaction and high resource utilization. However, better algorithms to achieve these goals efficiently are still needed. This paper proposes a hybrid technique for jobs scheduling based on Neural Network (NN) algorithm. The proposed algorithm classifies the jobs into four different classes. Furthermore, a Heuristic Resource Borrowing Scheme (HRBS) is proposed to exploit all services which has offered by cloud computing. Simulation is conducted using extensive (Cloud-Sim) simulator to measure the efficiency of the suggested algorithm in terms of average throughput, average turnaround time and average of context switch. The obtained results show that the proposed scheme outperforms other state of the art scheduling schemes.

Keywords - Cloud Computing, Job Scheduling, Hybrid Technique, Virtualization.

67. PaperID 310316116: Residual Energy based One-Hop Data Gathering in Wireless Sensor Networks (pp. 569-574)

Gaurav Kumar Pandey, Dept. of Computer Science and Engineering, Lovely Professional University, Jalandhar, India

Amritpal Singh, Dept. of Computer Science and Engineering, Lovely Professional University, Jalandhar, India

Abstract — The key constraint which hampers the performance of Wireless Sensor Networks is the limited battery power of the sensor nodes. Nodes once deployed cannot be recharged therefore data gathering from the sensor field should be done in such a manner that the energy of sensor nodes can be saved. Multi Hop routing and data relay protocols tend to deplete the battery power of the forwarding nodes at a large extent. Also, Clustering Algorithms generate extra overhead which affects the lifetime and performance of the network. In this paper we introduce Residual Energy based One-Hop Data Gathering (REO-HDG) in Wireless Sensor Networks by making use of a Mobile Data Collector (MDC) that traverses the sensor field and collects data from the sensors using single hop only, which in turn eliminates the problem of data relay. We make use of rendezvous locations, one-hop neighbor sets and residual energy of sensors to gather data from the sensor nodes. The union of all neighbor sets include all the candidate sensor nodes. REO-HDG tends to maximize the lifetime of the sensor network by eliminating data relay and clustering.

Index Terms— *Mobile Data Collector (MDC), Data gathering, Residual Energy, Energy Conservation, MDC Scheduling, Wireless Sensor Networks.*

Flexible Hardware Implementation of Hyperelliptic Curves Cryptosystem

Anissa Sghaier #¹, Chiraz Massoud #², Medien Zeghid *³, Mohsen Machhout #⁴

Faculty of Sciences, University of Monastir, E&E Lab

Avenue of the environment 5019 Monastir

¹ first.author@first-third.edu

² massoud.chiraz@hotmail.fr

⁴ machhout@yahoo.fr

* Higher Institute of Applied Sciences and Technology

Taffala City, 4003 Sousse Tunisie

³ medien.zeghid@fsm.rnu.tn

Abstract—Due to the resolution of key distribution problem, asymmetric scheme become the most popular cryptographic technique compared to symmetric scheme. One of the well-known asymmetric encryption algorithms are (Hyper)Elliptic Curve Cryptosystem (ECC and HECC). They provide equal security levels compared with the RSA algorithm with shorter operand size. Although, the HECC outperform the ECC due to its shorter operand size. The objective of this paper is to present an efficient hardware architecture using Cantor's method, to implement a new way of explicit formula over genus curve 2, and analyze the performance of the two implementations. HECC cryptosystem was implemented over $GF(2^{83})$ on XC5V240 FPGA, it takes about 5086 slices, and it runs at 175 MHz in 0.287 ms.
keywords ECC, HECC, hardware implementation, Cantor's method, explicit formula

I. INTRODUCTION

The primary goal of Public-key (PK) cryptosystems is providing information security services such as confidentiality, integrity , authentication, and non-repudiation in electronic systems. Based on mathematical problems, PK schemes provide a strong data-security which presents a revolution in cryptography. Nowadays, when speaking about modern cryptography we touch three fields: mathematics, computer science, and electrical engineering. To have an efficient algorithm hard to break theoretically and practically, it must be based on a hard mathematical problem. In the few last years, an important cryptographic field of research was given to cryptographic scheme based on algebraic curves such as the HECC, ECC and pairing computation (using ECC or HECC). These schemes are based on the hardness of solving the discrete logarithm problem. They outperform the most used asymmetric encryption algorithm which is RSA. Thus, security strength of HECC cryptosystem is the fact that it uses much shorter operand length comparing to all PK cryptosystems. Having a wide range of features, HECC can be implemented easier in both hardware and software; it requires less memory resources and less power consumption, because it uses much shorter operand length. HECC become a popular cryptosystem wherefore many researchers were done to develop used algorithms and to improve the HEC group operations. They prove

that modular arithmetic operations in binary fields curves are cheaper to be implemented in hardware than prime field curves, contrarily to software implementation, fast integer multiplication is less efficient in hardware. Because they require smaller fields than EC, HEC became more suitable to embedded hardware: a 160-bit group is given by an EC with $q \approx 2^{160}$, by an HEC of genus 2 with $q \approx 2^{80}$, and genus 3 with $q \approx 2^{53}$. HECCs' algorithms are heavily based on arithmetic operations such as modular multiplication and inversion, which are very expensive in term of area occupancy. Our HECC implementation over $GF(2^n)$ uses affine coordinates which reduces the number of intermediate results by reducing intermediate register number.

In this paper, we propose a hardware architecture of hyperelliptic curve cryptosystem (HECC) suitable to restrained environment. Using Virtex5 FPGA platform, we find that our HECC cryptosystem implemented over $GF(2^{83})$ on XC5V240 FPGA takes about 5086 slices, it runs at 175 MHz in 0.287 ms. Our results prove that HECC can respect the requirements of restrained environment with a comparable performance. One scalar multiplication takes ... clock cycle .

This paper is organized as follows: Section 2 lists some related works and highlight the difference between them. Section 3 gives a brief HECC mathematical background. Section 4 presents the first HECC implementation using Cantor's method over finite field. Section 5 gives the second implementation architecture based on explicit formula. Section 6 presents the implementation results and provides the table of comparison . Finally, a conclusion and results discussion are given in Section 7.

II. RELATED WORKS

This section lists some relevant previous work. HEC was been used in cryptographic applications, it has been implemented in both software and hardware. After using Cantors' method, many researches was been done to increase the efficiency of HEC group operations. In [1], [2], [3], authors tried to find efficient explicit formula which can reduce the group operations number on HEC. As it's mentioned in the

diagram of time below that , between 2003 and 2011, a lot of effort was done to implement HECC in both software and hardware. But, from 2011 until now only one result was be proposed.

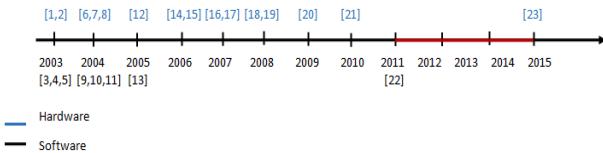


Fig. 1. Diagram of HECC related works

Software implementations was done from 2003 to 2005, and then in 2011, another implementation appear. They can be found in [4], [5], [6]. They used HECC explicit formula over binary field. In [5], authors implemented the Harley's explicit formula for genus 2 and 4. They improved that cantors' algorithm can be efficiently used to implement genus 3 HECC. HECC hardware implementations was done in [7], [8], [2], [9], [10], [3]. They used genus 2 explicit formula to calculate the operations group only [7], authors implemented HECC using cantor's algorithm. The aim of the hardware implementation in [2], [9], [10], [7] was to improve the architecture efficiency in term of speed. Whereas, the goal of [3], [8] implementation is to improve HECC hardware design in term of power.

III. MATHEMATICAL BACKGROUND OF HYPERELLIPTIC CURVE CRYPTOGRAPHY

In this section, we will give a brief overview of the HEC mathematical background. HECC was appeared in 1988 with koblitz. It's the generalization of the elliptic curve, EC is a HEC of genus g=1.

A. HEC curve and genus choice

An hyperelliptic curve C of genus $g \geq 1$ over finite filed \mathbb{F} is the set of solution $(x, y) \in \mathbb{F} \times \mathbb{F}$ to the equation:

$$C : y^2 + h(x)y = f(x) \quad (1)$$

where:

$$\begin{cases} \text{degree}(h(x)) \leq g, & h(x) \in \mathbb{F} \times \mathbb{F}. \\ \text{degree}(f(x)) = 2g + 1, & f(x) \in \mathbb{F} \times \mathbb{F}. \end{cases}$$

The curve C should be non-singular curve, if there are no pairs $(x, y) \in \mathbb{F} \times \mathbb{F}$. The polynomial f(x) and h(x) are chosen such that it has to satisfy the following equations:

$$\begin{cases} 2y + h(x) = 0 \\ h'(x)y - f'(x) = 0 \end{cases}$$

As the value of genus g defines the polynomial degree of the curve C, we can note that it have an impact on the processing time of the global Cryptosystem. Many researches demonstrated that HEC of genus 2 and 3 are more secure than genus 3, and genus 3 is more complex than genus 2 with a greater calculation times [7], [11], [9]. For this reason, curves

with genus 2 have been more extensively studied. Therefore, we chose the genus 2 curves to be implemented in this work. To ensure efficient implementation hardware or software it is necessary to choose carefully the type of field: binary or prime.

B. Jacobian of HEC and Scalar multiplication

a) *Jacobian of HEC*.: In EC, the curve is a set of points, whereas in HEC, the curve represents a group of divisors called the Jacobian of HEC denoted by $\mathbb{J}_C(F)$. They are a finite sums of the points of the HEC curve. The a finite sum of two points of the curve is called a "reduced divisor". Each element of the $\mathbb{J}_C(F)$ can be represented uniquely by a divisor D as shown:

$$\begin{cases} \mathbb{J}_C(F) = \frac{\mathbb{D}^0}{\mathbb{P}} \\ D = \sum m_i P_i \end{cases}$$

Where

D^0 is the set of divisors of degree 0; \mathbb{P} is the set of principal divisors; m_i Number of points ; P_i Points on the Curve C. Using the set of reduced divisors, then, a "divisor addition" operation can be defined on the Jacobian group as:

$$\begin{cases} P_1, P_2 \in C \rightarrow D_1 = \text{div}(u_1; v_1) \in \mathbb{J}_C, \\ Q_1, Q_2 \in C \rightarrow D_2 = \text{div}(u_2; v_2) \in \mathbb{J}_C, \\ D_1, D_2 \in J_C \rightarrow D_1 \oplus D_2 = D_3 \in J_C, \\ D_3 \in \mathbb{J}_C \rightarrow -R_1, -R_2 \in C \end{cases}$$

With: $P_1 = (x_{P_1}, y_{P_1})$, $P_2 = (x_{P_2}, y_{P_2})$, $Q_1 = (x_{Q_1}, y_{Q_1})$, $Q_2 = (x_{Q_2}, y_{Q_2})$, $R_1 = (x_{R_1}, y_{R_1})$ and $R_2 = (x_{R_2}, y_{R_2})$. The reflection of $-R_1$ and $-R_2$ in the x-axis intersects the curve C at exactly two points R_1 and R_2 which are the desired result of the the divisor addition. Here, to perform divisor addition and divisor doubling we should define the coordinates of D_i , so we speak about Mumford representation: the Jacobian can be represented as pair of polynomials u(x) and v(x) satisfying the following condition:

$$P_1 = (x_{P_1}, y_{P_1}), P_2 = (x_{P_2}, y_{P_2}) \in C \rightarrow D \in J_C,$$

- $D = \text{div}(u(x), v(x)) = [u(x), v(x)]$,
- $u(x)$ is monic polynomial ,
- $\deg v(x) < \deg u(x) \leq g$,
- $u(x) = x^2 + u_1x + u_0 = (x - x_{P_1})(x - x_{P_2})$,
- $v(x) = v_1x + v_0, v(x_{P_1}) = y_{P_1}, v(x_{P_2}) = y_{P_2}$.

b) *Scalar Multiplication*.: The main operation in HECC or ECC is the scalar multiplication. The HEC scalar multiplication is done by multiplying a divisor by an integer based on repeated additions and doublings.

$$E = [k]D = \underbrace{D \oplus D \oplus D \oplus \dots \oplus D}_{k \text{ times}}$$

For elliptic/ hyperelliptic curves, many scalar multiplication algorithms exist but the most useful one is Montgomery's ladder because it can resist to side channel attacks. In software or hardware implementation, scalar multiplication have an effect on the execution time of HEC cryptosystems. To perform this operation we need to calculate the addition and doubling divisors operations which will be more detailed in the next section.

IV. HECC IMPLEMENTATION DESIGN

In this section, we will present two ways of implementing HEC cryptosystem, the first based on Cantor's algorithm and the second using Explicit Formulae. We will use a curve C with genus 2, over \mathbb{F}_{2^m} and of the following form : $y^2 + xy = f(x)$. We choose hyperelliptic curves defined with: $h(x) = x$ and $f(x) = x^5 + f_3x^3 + x^2 + f_0$. And, in order to reduce the area, we choose a low Hamming-Weight irreducible polynomial, $P(x) = x^{83} + x^7 + x^4 + x^2 + 1$.

A. HECC using Cantors' Method

Our goal in this paper is to minimize the area of both datapath and the data memory. We use affine instead of projective coordinates, in order to reduce the registers number in which intermediate values will be stored.

Algorithm 1 : Composition Cantor Algorithm

```

Input:  $D_1 = \text{div}(a_1; b_1)$ ,  $D_2 = \text{div}(a_2; b_2)$ , H, F
Output:  $D_3 = \text{div}(a_3; b_3) = D_1 + D_2$  Perform first extended GCD:
 $d_1 = \text{gcd}(a_1; a_2)$  Perform Second extended GCD:
 $d = \text{gcd}(d_1; b_1 + b_2 + H) = s_1a_1 + s_2a_2 + s_3(b_1 + b_2 + H)$ 

 $a_3 = a_1a_2/d^2$ 
 $b_3 = (s_1a_1b_2 + s_2a_2b_1 + s_3(b_1b_2 + F))/d(\text{mod } a_3)$ 
while  $\deg(a_3) > g$  do
     $a_3 = (F - Hb_3 - b_3^2)/a_3$ 
     $b_3 = -H - b_3(\text{mod } a_3)$ 
end while
Return  $D_3$ 
```

Algorithm 1 gives the main steps to compute composition which is the first operation in point addition. It's based on modular arithmetic operations: the GCD computation, multiplication (M), square (S), division (D) and inversion (I). Thus, high performance implementation is based on an optimized hardware architecture. Its efficiency is decided by the efficiency of multiplication and inversion modules, because they are the most greedy component in term of area and execution time. Figure 2 gives the datapath of the HECC processor design. It's based on 6 main blocks.

- 1) Controller Unit (CU): is based on a hard finite state machine responsible in the activation of each step of Cantor's algorithm at the appropriate clock cycle. Various registers are used in order to store intermediate data, and temporary data are sent into the available computation unit. In every step of Cantors' algorithm, the results are then stored in the intermediate registers.
- 2) Composition Unit (CU): Cantor's algorithm point addition is based on two main operations: composition and reduction. Composition in Cantor's algorithm requires GCD computation, polynomial multiplications, polynomial Squares and polynomial divisions which are very time consuming in hardware. CU uses the arithmetic blocks of the $GF(2^n)$ Arithmetic Unit ($GF(2^n)$ AU) and store results in the intermediate registers.

- 3) Reduction Unit (RU): results of composition step and doubling step should be reduced, so from a semi-reduced divisor $D' = \text{div}(a', b')$ we find an equivalent reduced divisor $D = (a, b)$. It can be implemented by Cantor reduction, Gauss reduction or Lagrange reduction. Gauss reduction will be implemented such that the computation of the a_k (with k is the iteration number) uses only one multiplication and one division, and the different steps are independent.
 - 4) Doubling Unit (DU): point doubling requires doubling then reduction. It's a point addition case with an equal inputs. In this case, multiplications are replaced with squaring operations, here there are a gain in area occupation because squaring is very quickly and faster.
 - 5) $GF(2^n)$ Arithmetic Unit ($GF(2^n)$ AU): it's one of the main unit, it contain all arithmetic operation blocks; GCD, multiplication, squaring and division.
- *Greatest Common Divisor:* In Cantor's algorithm, three greatest common divisor (GCD) must be computed. To calculate 3-GCD, two different GCD need to be calculated: $d_1 = \text{gcd}(a_1; a_2)$, $d = \text{gcd}(d_1; b_1 + b_2 + H)$ in order to obtain the final result: $d = s_1a_1 + s_2a_2 + s_3(b_1 + b_2 + H)$.
 - *Binary Divider:* to divide two polynomials A and B, such that $A = Q \times B + R$ with Q is a quotient and R is the remainder. This operation can be done using the standard algorithm of binary division.
 - *Square:* is faster than multiplication because it's a linear operation. Squaring a binary polynomial is obtained by inserting a bit '0' between consecutive bits. For example, $A(x) = x^2 + x + 1$ has the following binary representation: "111", after inserting '0' between A_i and A_{i+1} the square is $A^2(x) = (10101)_2$. Using look-up table, squaring can be computed very quickly and then reduced modulo the irreducible polynomial P(x) to obtain the final result.
 - *Multiplier:* to implement an efficient modular multiplier, we used Montgomery's algorithm [12], it has various benefits comparing to ordinary modular multiplication algorithms, but the main one is that the division step to compute the modulus is replaced by shift operations. This method is easy to implement in hardware and decrease the area occupancy.
 - *Inverter:* requires high-complexity and high-occupancy. Modular inversion algorithm need not less than twice the time of modular multiplications. There are two approaches to compute it: using Fermat's theorem or using the Extended Euclidean Algorithm (EEA). But, the most efficient algorithm is the Almost Inverse Algorithm because it performed EEA-shifting-operations in the end at once.
 - 6) A'/B' Unit ($A'/B'U$): it represent the calculus of a_3 and b_3 in Algorithm 1. They can be performed in pipeline or

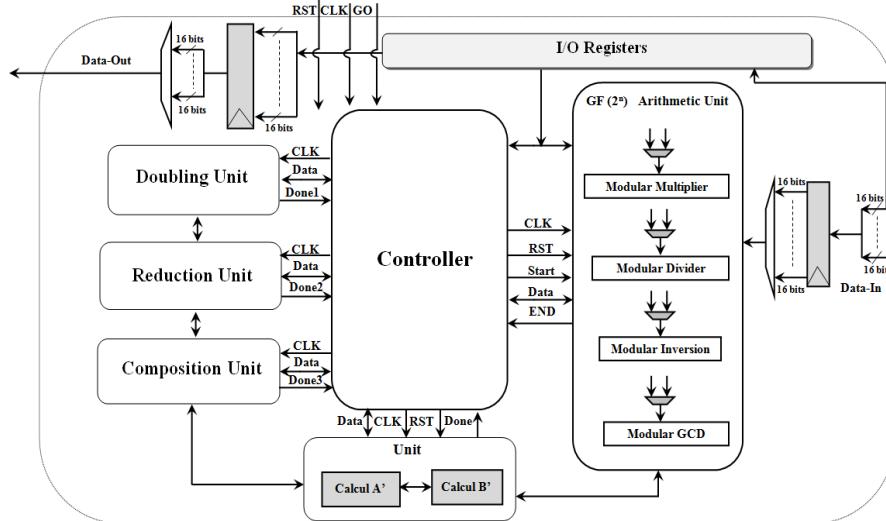


Fig. 2. HECC Processor Design

serial because B' calculus need A' result. The proposed design compute firstly A' then B' in order to minimize the area use.

Our contribution is to reduce area of memory block of Cantor's algorithm in order to be well suitable for constrained devices. Thus, the final coprocessor contains 2 multipliers, 1 squarer, 1 GCD block, 1 divider and 1 Inverter.

B. HECC using Explicit Formula

This section presents the difference between Cantor and Harley Explicit Formula, then an optimized (Opt.) Harley's algorithm was proposed (Appendix).

TABLE I
NUMBER OF USED COMPONENTS FOR POINT ADDITION IN DIFFERENT EXPLICIT FORMULA ALGORITHMS.

	Cantors'			Harleys'			Harleys' Opt.	
	M	S	I	M	S	I	M	I
Step1	8	2	1	3	1	0	3	0
Step2	2	0	0	0	0	0	3	0
Step3	22	0	0	5	0	0	3	0
Step4	7	2	1	5	2	1	1	
Step5	5	0	0	2	0	0	3	0
Step6	-	-	-	3	0	0	2	0
Step7	-	-	-	-	-	-	3	0
Step8	-	-	-	-	-	-	3	0
Step9	-	-	-	-	-	-	1	0
Step10	-	-	-	-	-	-	3	0
Step11	-	-	-	-	-	-	3	0
Total:	44M+4S+2I			22M+3S+I			25M+I	
Nº comp.:	22M+2S+I			5M+2S+I			3M+I	

The main goal in this section is to use less registers for storing intermediate results in order to reduce area occupancy. Table I presents the number of components needed for point addition in every algorithm and the number of component used in the entire architecture. As it's mentioned in Table I, the Harleys' Optimized algorithm uses 31% less than the Harleys' one of the total operation needed, and a decrease of 40% of components used.

Cantors' Algorithm needs a big number of arithmetic operation specially multiplication, whereas Harley's Algorithm needs 50% less than Cantors' one. Cantors' Algorithm uses 22 multiplication blocks, 2 square blocks and 1 inversion block, but Harley's Algorithm uses only 5 multiplication blocks, 2 square blocks and 1 inversion block. The optimized Harley's algorithm decrease the number of multiplier blocks used to 86% comparing to Cantor Algorithm, and to 40% comparing to the original Harley's Algorithm. Here, the Harley's optimized Algorithm presents a gain in components number so in area occupancy with a little loose in computation time.

TABLE II
NUMBER OF USED COMPONENTS FOR POINT DOUBLING IN DIFFERENT EXPLICIT FORMULA ALGORITHMS.

	Cantors'			Harleys'			Harleys' Opt.	
	M	S	I	M	S	I	M	I
Step1	8	0	1	3	2	0	0	0
Step2	0	3	0	0	0	0	3	0
Step3	22	4	0	1	0	0	2	0
Step4	7	1	1	5	0	0	3	1
Step5	5	0	0	5	2	1	3	0
Step6	-	-	-	2	0	0	0	0
Step7	-	-	-	2	1	-	2	0
Step8	-	-	-	4	0	-	2	0
Total:	42M+8S+2I			22M+5S+I			15M+I	
Nº comp.:	22M+4S+I			5M+2S+I			3M+I	

Table II presents the number of components needed for point doubling in every algorithm and the number of component used in the entire architecture. Harley's Algorithm needs 47% less than Cantors' one of necessary arithmetic operation, and 77% less of component blocks. Whereas, the Harley's optimized Algorithm uses 31% less than Harley's one of the total operation needed, and a decrease of 40% of components used.

Due to its shorter operand sizes, HCC presents good performance on embedded processors and constrained environments, that will be proved by the implementation results shown in the next section.

V. HECC IMPLEMENTATION RESULTS

In this section, we will firstly give a comparison of results between ECC performances and those of HECC. Then, we will compare the performance of proposed HECC processor with those of the other reported designs.

TABLE III
HECC POINT ADDITION/DOUBLING HARDWARE IMPLEMENTATION RESULTS

Operation	Clock Cycles	Area (Slices)	Frequ. (MHz)	Time (μ s)
Point Addition	2,500	8,100	105 MHz	75
Point Doubling	2,070	6,700	105 MHz	63

Table III gives implementation results of point addition and point doubling using Cantors' Algorithm. It's clear that both point operations are greedy in term of area occupation.

TABLE IV
COMPARISON OF PROPOSED HECC PROCESSOR WITH ECC RESULTS

Design	Platform	Field	Freq. [MHz]	Time (ms)	Area [Slices]
D1	<i>XC5V240</i>	$GF(2^{83})$	85	6,5	13,870
D2	<i>XC5V240</i>	$GF(2^{83})$	175	0.287	5086
ECC[13]	<i>XC5V240</i>	$GF(2^{163})$	221	0.258	9670

Table IV compares our implementation results of both ECC in [13] and HECC using Cantors' Algorithm and Explicit Formula in VirtexV FPGA XC5V240. We remark that ECC provides the best performances in frequency, time, and area comparing to HECC using Cantor Algorithm. The gain in area is about 30.28%.

Note: FE: Explicit Formula, KG: Kilo Gate.

Having keys and operands of half the size of ECC, EF-HECC over $GF(2^{83})$ can provide the same theoretical level of security as ECC over $GF(2^{163})$. Thus, HECC using Explicit Formula presents a decrease in area about 47.4% which is almost the half of ECC area. Table V lists the implementation results of both hardware and software architectures. For genus-2 curves, we implemented the explicit formula based on optimized Harley's algorithm and $h(x) = x$ (Design D₁), and Cantors' Algorithm (Design D₂) over GF_2^{83} using VirtexII FPGA platform. Comparing D₁ and D₂, we remark that D₂ presents a decrease of 62.28% in area occupancy. Thus, Explicit Formula for genus-2 is more efficient than Cantor's algorithm, for this reason, the most implementations was done using EF method. Cantor's algorithm presents a problem in a hardware implementation, it needs a big number of arithmetic

units separately synthesized, for this reason it requires much more FPGA resources. The increase in area occupancy makes Cantors' Algorithm unattractive for hardware implementation. Implementation in [7] based on Cantors' algorithm uses 33.91% more resources than D₁. D₂ is more efficient than implementation in [10] in term of frequency and time, it presents a decrease of area about 26.35%. Authors in [8] present an FPGA implementation over GF(p) using 81 bits operands sizes. Various Software implementations was done such as in [19], [20], [11] and [4]. D₂ give a tradeoffs between computation time, and implementation costs.

VI. CONCLUSION

Algebraic curves was widely used to implement asymmetric cryptosystem such as ECC and HECC. These cryptosystems can be more efficient to be implemented in power and area restricted environment. In this paper, we implemented HECC cryptosystem over binary field on Xilinx FPGA using two methods: Cantors' and Explicit Formula. Implementation results prove that Explicit Formula presents best tradeoffs between time and area occupancy comparing to Cantors' method. Thus, HECC provides the same level of security as ECC with the half keys size and operands size. The HECC area occupancy is almost the half of ECC one.

REFERENCES

- [1] Batina L., Mentens N., Preneel B., Verbauwheide I.: Flexible Hardware Architectures for Curve-based Cryptography, In Proc. of IEEE International Symposium on Circuits and Systems (ISCAS 2006), 4 pages, Island of Kos, Greece, May 2006.
- [2] Kim H., Wollinger T., Choi D.H., Han D.G., Lee M.K.: Hyperelliptic Curve Crypto-Coprocessor over Affine and Projective Coordinates, ETRI Journal, Vol. 30, pp. 365–376 , 2008.
- [3] Fan J., Batina L., Verbauwheide I.: Light-Weight Implementation Options for Curve-Based Cryptography: HECC is also Ready for RFID, In The 1st International workshop on RFID Security and Cryptography - RISC, London, UK, pp. 1–6, 2009.
- [4] Chatterjee K., De A., Gupta D. : Software Implementation of Curve based Cryptography for Constrained Devices, International Journal of Computer Applications, 24(5):18-23, June 2011.
- [5] Wollinger T., Pelzl J., Paar C.: Cantor versus Harley: Optimization and Analysis of Explicit Formulas for Hyperelliptic Curve Cryptosystem. IEEE Transactions on Computers, vol. 54 , pp. 861–872, 2005.
- [6] Pelzl J., Wollinger T., Paar C.: High Performance Arithmetic for special Hyperelliptic Curve Cryptosystems of Genus Two, International Conference on Information Technology: Coding and Computing, Proceedings ITCC, pp. 513–517, 2004.
- [7] Clancy T.: FPGA-based Hyperelliptic Curve Cryptosystems, invited paper presented at AMS Central Section Meeting, April 2003.
- [8] Ahmadi H. R., Afzali-Kusha A., Pedram M., Mosaffa M.: Flexible Prime-Field Genus 2 Hyperelliptic Curve Cryptography Processor with Low Power Consumption and Uniform Power Draw, ETRI journal, vol. 37, no. 1, pp. 107–117, 2015.
- [9] Preneel B., Sakiyama K., Batina L., Verbauwheide I.: Superscalar Coprocessor for High-Speed Curve-Based Cryptography. Cryptographic Hardware and Embedded Systems-CHES, pp. 415–429, 2006.
- [10] Wollinger T.: Software and Hardware Implementation of Hyperelliptic Curve Cryptosystems. PhD thesis, Ruhr-University Bochum, Germany, 2004.
- [11] Hodjat A., Hwang D., Batina L., Verbauwheide I.: A Hyperelliptic Curve Crypto Coprocessor for an 8051 Microcontroller, In proceedings of the IEEE Workshop on Signal Processing Systems: Design and Implementation SIPS, IEEE, pp. 93–98, Athens, Greece, 2005.
- [12] Montgomery P.: Modular multiplication without trial division, Mathematics of Computation, Vol. 44, pp. 519–521, 1985.

TABLE V
COMPARISON OF PROPOSED HECC PROCESSOR WITH RELATED WORKS

Design	Platform	Field	Alg.	Freq. [MHz]	Time (ms)	Area [Slices]
Hardware Implementations						
D_1	Virtex - II	$GF(2^{83})$	Cantor	85	6.5	15,200
D_2	XC2V4000	$GF(2^{83})$	EF	145	0.30	5734
[7]	Virtex - II	$GF(2^{83})$	Cantor	-	10	23,000
[10]	XC2V4000	$GF(2^{81})$	EF	56.7	0.415	7785
[14]	XC2V4000	$GF(2^{89})$	EF	62.9	0.436	9950
[1]	Virtex II pro	$GF(2^{83})$	EF	166	0.496	11296
[9]	Virtex II pro	$GF(2^{83})$	EF	100	0.420	6586
[15]	XC2VP30	$GF(2^{67})$	EF	500	532	7652
[16]	Virtex-II	$GF(2^{113})$	EF	45.3	2.030	25271
[2]	FPGA	$GF(2^{89})$	EF	62.9	0.436	9950
[17]	XC2V4000	$GF(2^{83})$	EF	125	0.311	2316
[3]	ASIC	$GF(2^{83})$		300	456	14.55KG
[18]	FPGA	$GF(2^{83})$		0.5	740	-
[8]	FPGA	$GF(p)$	EF	1	502.8	-
Software Implementations						
[19]	ARM7	$GF(2^{162})$	EF	-	128×10^6	-
[20]	Power PC	$GF(2^{160})$	EF		117	-
[11]	8051 μ C	$GF(2^{83})$	EF	12	149.8×10^3	-
[4]	2DUO CPU T6400	$GF(2^{91})$	EF	2G	2.86	-

- [13] Sghaier A., Zghid M., Bouallegue B., Baganne A., Machhout M.: Area-Time Efficient Hardware Implementation of Elliptic Curve Cryptosystem, Cryptology ePrint Archive, [web page] <https://eprint.iacr.org/2015/1218.pdf>, 2015.
- [14] Kim H., Wollinger T., Choi Y., Chung K., Paar C. C.: Hyperelliptic curve coprocessors on a FPGA, In Workshop on Information Security Applications-WISA, Jeju Island, Korea, August 2004.
- [15] Sakiyama K.: Secure Design Methodology and Implementation for Embedded Public-key Cryptosystems, PhD thesis, Katholieke Universiteit Leuven, Belgium, 2007.
- [16] Elias G., Miri A., Yeap T. H.: On efficient implementation of FPGA-based hyperelliptic curve cryptosystems, Computers and Electrical Engineering, pp. 349–366, 2007.
- [17] Fan J., Batina L., Verbauwhede I.: HECC Goes Embedded: An Area-efficient Implementation of HECC, Selected Areas in Cryptography, Springer, vol. 5381 of the series Lecture Notes in Computer Science, pp. 387–400, 2008.
- [18] Batina L., Sakiyama K., Verbauwhede I.M.R.: CompactPublic-Key Implementations for RFID and Sensor Nodes, in Secure Integrated Circuits and System, New York, USA: Springer US, 2010, pp. 179–195.
- [19] Pelzl J., Wollinger T., Guajardo J., Paar C.: Hyperelliptic Curve Cryptosystems: Closing the Performance Gap to Elliptic Curves, Cryptographic Hardware and Embedded Systems-CHES, volume 2779 of the series Lecture Notes in Computer Science pp. 351–365, 2003.
- [20] Wollinger T., Pelzl J., Wittelsberger V., Paar C., Saldamli G., Koc G. K. : Elliptic and Hyperelliptic Curves on Embedded,2003 Journal ACM Transactions on Embedded Computing Systems (TECS) TECS Homepage archive, volume 3 Issue 3, pp. 509–533, 2004.

APPENDIX

TABLE VI
NEW EXPLOITATION OF HARLEY EXPLICIT FORMULA FOR DOUBLING IN A HEC OF GENUS TWO

Input	Weight two reduced divisors $D = (u, v)$ $u = x_2 + u_1x + u_0, v = v_1x + v_0$ furthermore: $h = x$ and $f = x_5 + f_1x + f_0$	
Output	A weight two reduced divisor D $u' = x_2 + u'_1x + u'_0, v' = v'_1x + v'_0$	
Step	Procedure	Cost
1	$r = u_0; inv_1 = 1; inv_0 = u_1;$	-
2	$w_0 = v_1^2; w_1 = u_1^2; k_1 = w_1;$ $t_1 = u_1k_1; k_0 = t_1 + w_0 + v_1;$	3M
3	$t_2 = u_0k_0; s'_1 = k_0; s'_0 = (w_0 + u_1)(k_0 + k_1) + t_1 + t_2;$ If $s'_1 = 0$ perform Cantor's Algorithm	2M
4	$n_1 = r^2; w_4 = w_3^2; n_2 = s'^2_1; t_3 = t_2^{-1};$	3M
5	$w_3 = n_1t_3; t_6 = t_1 + k_1s_1; S_1 = n_2t_3;$	3M
6	$z_0 = s'_0; z_1 = t_6 + s'_1; z_2 = w_1; z_3 = s_1;$	-
7	$u'_2 = 1; u'_1 = w_4; u'_0 = w_4k_1^2 + k_1 + w_3;$	2M
8	$t_4 = w_3; t_7 = t_4 + z_2; t_5 = t_7u'_0;$ $v'_1 = (z_3 + t_7)(u'_0 + u'_1) + t_4 + t_5 + 1 + z_1 + v_1;$ $v'_0 = t_5 + z_0 + v_0;$	2M

TABLE VII
NEW EXPLOITATION OF HARLEY EXPLICIT FORMULA FOR ADDING IN A HEC OF GENUS TWO

Input	Weight two reduced divisors $D_1 = (u_1, v_1)$ and $D_2 = (u_2, v_2)$ with $u_1 = x^2 + u_{11}x + u_{10}; u_2 = x^2 + u_{21}x + u_{20};$ $v_1 = v_{11}x + v_{10}; v_2 = v_{21}x + v_{20};$ furthermore: $h = h_2x^2 + h_1x + h_0$; where $hi \in 0, 1$; $f = x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0$; where $f_i \in 0, 1$;	
Output	A weight two reduced divisor $D_0 = (u_0, v_0) = D_1 + D_2$ with $u' = x^2 + u'_1x + u'_0; v' = v'_1x + v'_0;$	
Step	Procedure	Cost
1	$z_1 = u_{11} - u_{21}, z_2 = u_{20} - u_{10}, r = z_2z_3 + z_1^2u_{10}$ $inv_1 = z_1, inv_0 = z_3$	3M
2	$z_3 = u_{11}z_1 + z_2, w_1 = v_{10} - v_{20}, w_2 = v_{11} - v_{21}$ $w_3 = inv_0w_1, w_4 = inv_1w_2$	3M
3	$s'_1 = (inv_0 + inv_1)(w_1 + w_2) - w_3 - w_4(1 + u_{11}), s'_0 = w_3 - u_{10}w_4$ If $s_1 = 0$ perform Cantor	3M
4	$w_1 = (rs'_1)^{-1}$	M+I
5	$w_2 = rw_1, w_3 = s'^2_1w_1$	3M
6	$w_4 = rw_2, s''_0 = s'_0w_2$	2M
7	$w_5 = w_4^2, l'_2 = u_{21} + s''_0, l'_1 = u_{20} + u_{21}s''_0, l'_0 = u_{20}s''_0$	3M
8	$u'_0 = (s''_0 - u_{11})(l'_2 + h_2w_4 - u_{11}) - u_{10} + l'_1 + (h_1 + 2v_{21})w_4 + (u_{11} + u_{21} - f_4)w_5$	3M
9	$u'_1 = h_2w_4 + s''_0 + l'_2 - u_{11} - w_5$	M
10	$w_1 = l'_2 - u'_1, w_2 = u'_1w_1 + u'_0 - l'_1, w_4 = u'_0w_1 - l'_0, t = h_2u'_0$	3M
11	$v'_1 = w_3w_2 - v_{21} - h_1 + h_2u'_1, v'_0 = w_3w_4 - v_{20} - h_0 + t$	3M

Phishing Identification Using a Novel Non-Rule Neuro-Fuzzy Model

Luong Anh Tuan Nguyen
Faculty of Information Technology
Ho Chi Minh City University of Transport
Ho Chi Minh City, Vietnam
Email: nlatuan@hcmutrans.edu.vn

Huu Khuong Nguyen
Faculty of Information Technology
Ho Chi Minh City University of Transport
Ho Chi Minh City, Vietnam
Email: nhkuuong@hcmutrans.edu.vn

Abstract—This paper presents a novel approach to overcome the difficulty and complexity in identifying phishing sites. Neural networks and fuzzy systems can be combined to join its advantages and to cure its individual illness. This paper proposed a new neuro-fuzzy model without using rule sets for phishing identification. Specifically, the proposed technique calculates the value of heuristics from membership functions. Then, the weights are trained by neural network. The proposed technique is evaluated with the datasets of 22,000 phishing sites and 10,000 legitimate sites. The results show that the proposed technique can identify with an accuracy identification rate of above 99%.

Keywords—*Phishing; Fuzzy; Neural Network; Neuro-Fuzzy*

I. INTRODUCTION

According to a study by Gartner [1], 57 million US Internet users have identified the receipt of email linked to phishing scams and about 2 million of them are estimated to have been tricked into giving away sensitive information. According to the reports of the Anti-Phishing Working Group [2], the number of phishing attacks is increasing by 5% monthly. Figure 1 shows the phishing website report received in the first quarter of 2014, showing that the risk of phishing is extremely high. For these reasons, identifying phishing attacks is very urgent and important in modern society.

Recently, there have been many studies that against phishing based on the characteristics of site, such as URL of website, content of website, combining both the website URL and content, source code of website or interface of website, etc. However, each of studies has its own strengths and weaknesses. There is still not a sufficient method. In this paper, a new approach is proposed to identify the phishing sites that focuses on the features of URL (PrimaryDomain, SubDomain, PathDomain) and the web traffic (PageRank, AlexaRank, AlexaReputation, GoogleIndex, BackLink). Then, a proposed neuro-fuzzy network is a system which reduces the error and increases the performance. The proposed neuro-fuzzy model uses computational models to perform without rule sets. The proposed solution achieved identification accuracy above 99% with low false signals.

The rest of this paper is organized as follows: Section II presents the related works. System design is shown in section III. Section IV evaluates the accuracy of the method. Finally, Section V concludes the paper and figures out the future works.

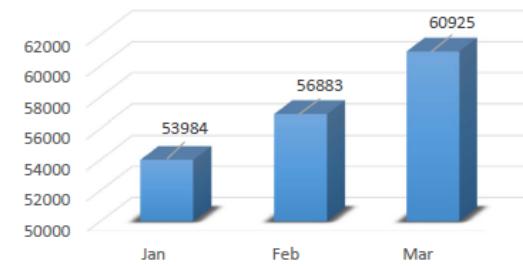


Fig. 1: Phishing reports received in the period of January-March 2014

II. RELATED WORK

Up to now, methods for identifying phishing can be divided into three groups: blacklist, heuristic and machine learning. In the first approach, the phishing identification technique [3][4][5][6] maintains a list of phishing websites called blacklist. The blacklist technique is inefficient due to the rapid growth in the number of phishing sites. Therefore, the heuristic and machine learning approaches have received more attraction of researchers.

Cantina [7] presented the algorithm TF-IDF based on 27 features of webpage. This technique can identify 97% phishing sites with 6% false positives. Although this technique is efficient, the time extracting 27 features of webpage is too long to meet real time demand and some features are not necessary for improving the phishing identification accuracy. Similarly, Cantina+ [8] used machine learning techniques based on 15 features of webpage and only six of 15 features are efficient for phishing identification such as bad form, Bad action fields, Non-matching URLs, Page in top search results, Search copyright brand plus domain and Search copyright brand plus hostname. In [9], the author used the URL to identify phishing sites automatically by extracting and verifying different terms of a URL through search engine. Even though this paper proposed a new interesting technique, the identification rate is quite low (54.3%). The technique [10] developed a content-based approach to identify phishing called CANTINA, which considers the Google PageRank value of a page, the evaluation dataset is quite small. The characteristic of the source code is used to identify phishing sites in [11].

The authors in [12] have proposed fuzzy technique based on 27 features of webpage, classified into 3 layer. Each feature has three linguistic values: low, moderate, high. The technique has built a rule set, triangular and trapezoidal membership functions. The achieved rate of the technique is 86.2%. But, there exist many drawbacks in [12]. First, the rule sets are not objective and greatly depend on the builder. Second, the weight of each main criteria is used without any clarification. Finally, the used heuristics are not optimal and really effective.

The authors in [13] have proposed neural network technique. Three layers were used in the neural network including input layer, hidden layer and output layer. The best achieved rate of the technique is 95%. However, there exist some drawbacks in [13]. First, a number of hidden nodes and activation function must be determined through experimentation. Second, the authors do not explain why using one hidden layer. Third, the value of features do not know how is it calculated. Finally, the datasets are not big enough.

In the previous techniques, the URL plays a minor role in identifying phishing websites. In this paper, we focus on URL's features and design a new neuro-fuzzy model to identify phishing sites. Our work contributes four new aspects: i) The new heuristics have been proposed to identify phishing website more effectively and rapidly. ii) The parameter values used in the membership functions are derived from the big data set so that the model is still equivalent for the new data set. iii) The weights are trained by neural network, so they were more efficient. iv) The rule sets are not utilized. Hence, the result will be more precise and objective.

III. SYSTEM DESIGN

A. URL

A URL (uniform resource locator) is used to locate the resources[16].

The structure of URL is as follows:

< protocol >: // < subdomain > . < primarydomain > . < TLD > / < pathdomain >

For example, with the URL: <http://www.paypal.abc.net/login/web/index.html>, there are six components as follows: Protocol is http, Subdomain is paypal, Primarydomain is abc, TLD is net, Domain is abc.net, Pathdomain is login/web/index.html

B. Features of URL

Phishers usually try to make the Internet address (URL) of phishing sites look similar to legitimate sites to fool online users. They cannot use the exact URL of the legitimate site, they make more spelling mistake the features of URL such as PrimaryDomain, SubDomain, PathDomain. For example, the URL www.applle.com looks similar to well known website www.apple.com, or <http://www.apple.attack.com> if users are not careful, they will think that they are on the Apple site.

C. Features of web traffic

Most of the time, legitimate websites are safe for users to browse and have high ranking from search engines [14].

Phishers usually create fake sites to mimic famous sites; however phishing sites do not have high rankings, which cannot be faked. This can be explained by the long-lived nature and the increasing number of in-links of legitimate websites as opposed to the short-lived nature and small number of in-links (usually none) of phishing site [15]. Therefore, in this paper, we use ranking values in the famous ranking systems of PageRank, AlexaRank, AlexaReputation, GoogleIndex and BackLink to identify phishing sites. These famous ranking websites provide accurate and reliable ranking values. We collect many ranking values from many search engines and ranking systems in order to improve the identifying accuracy. This combination makes the ranking parameters more robust and confident for identifying phishing sites.

D. System Model Design

The model can be depicted in Fig 2.

1) Phase I - Selecting four features of URL: Four features are extracted from URL such as *Domain*, *PrimaryDomain*, *SubDomain* and *PathDomain*.

2) Phase II - Calculating eight values of the heuristics: Eight values of the heuristics are calculated and eight heuristics are eight input nodes of the neuro-fuzzy network.

3) Phase III - Neuro-Fuzzy Network: The neuro-fuzzy network performs to calculate the value of the output node.

4) Phase IV - Identifying the sites: We based on the value of the output node to decide whether a site is a phishing site.

E. Neuro-Fuzzy Network Model

1) The model: The neuro-fuzzy network model was designed as in Fig 3. The model was designed with five layers as follows:

- The first layer, called the input layer, contains eight nodes that are eight heuristics such as PrimaryDomain, SubDomain, PathDomain, PageRank, AlexaRank, AlexaReputation, GoogleIndex, BackLink.

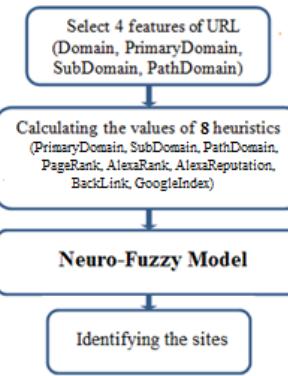


Fig. 2: The System Model

- The second layer contains 16 nodes. The value of each node is calculated from the left sigmoid membership functions and the right sigmoid membership function.
- The third layer contains two nodes which are π_L and π_P . π_L and π_P are calculated by (1) and (2).

$$\pi_L = \prod_{i=1}^8 L_i \quad (1)$$

$$\pi_P = \prod_{i=1}^8 P_i \quad (2)$$

- The fourth layer contains two nodes which are NL (Normalization Legitimate) and NP (Normalization Phishing). NL and NP are calculated by (3) and (4).

$$NL = \frac{\pi_L}{\pi_L + \pi_P} \quad (3)$$

$$NP = \frac{\pi_P}{\pi_L + \pi_P} \quad (4)$$

- The fifth layer, called the output layer, has one output node.

The neural network performs from the fourth layer to the output layer. The weights are trained by the training algorithm and the sigmoid activation function is used in the proposed model, so the output value of the output node ranges from 0 to 1. The proposed model is classified into two classes so the site is phishing if the value of the output node is less than 0.5 and the site is legitimate, if the value is greater than or equal to 0.5.

2) *The value of eight input nodes:* Based on experimental results and statistics from the dataset of 11,660 phishing sites. We found that:

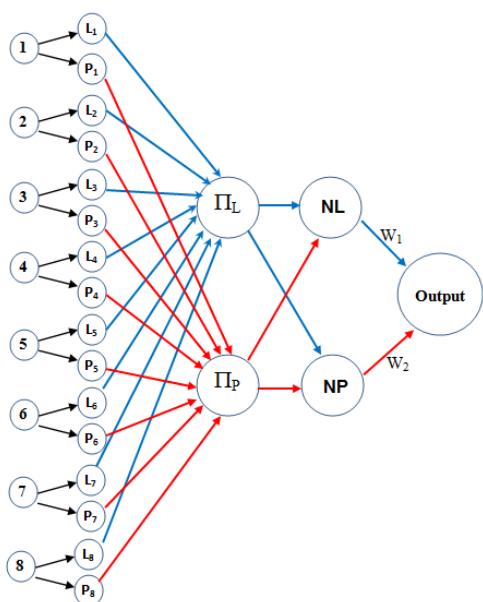


Fig. 3: The neuro-fuzzy network model

- The phishing site has the Levenshtein distance [17] between 'PrimaryDomain', 'SubDomain', 'PathDomain' and the result of GOOGLE search engine spelling suggestion that is less than 4.
- The PageRank value varies from 0 to 10. The phishing site has the PageRank value that is less than 6.
- The phishing site has the AlexaRank value that is greater than 300,000.
- The phishing site has the AlexaReputation value that is less than 20.
- The phishing site has the GoogleIndex value that is less than 20.
- The phishing site has the BackLink value that is less than 20.

Eight values of the heuristics are calculated as follows:

- Calculating the value of heuristic 'PrimaryDomain': The algorithm is shown in Algorithm 1.
- Calculating the value of heuristic 'SubDomain' and 'PathDomain': The algorithm is shown in Algorithm 2.

Data: PrimaryDomain

Result: The value of heuristic "PrimaryDomain"

if PrimaryDomain is IP **then**

| value = 0; //doubt phishing

else

| Result =

Suggestion_Google(PrimaryDomain);

if Result is NULL **then**

| value = 100; //No doubt phishing

else

| value =

Levenshtein(Result, PrimaryDomain);

end

Algorithm 1: Calculating the value of PrimaryDomain

Data: m //m is SubDomain or PathDomain

Result: The value of heuristic m

if m is Null **then**

| value = 100; //No doubt phishing

else

| Result = Suggestion_Google(m);

if Result is NULL **then**

| value = 100; //No doubt phishing

else

| value = Levenshtein(Result, m);

end

Algorithm 2: Calculating the value of SubDomain/PathDomain

- Calculating the value of heuristic 'PageRank': The Googles PageRank value can be obtained from [18]. PageRank value varies from 0 to 10.

- Calculating the value of heuristic 'GoogleIndex' and 'BackLink': GoogleIndex and BackLink value can be obtained from [18].
- Calculating the value of heuristic 'AlexaRank' and 'AlexaReputation': AlexaRank and AlexaReputation value can be obtained from [19].

3) *The value of 16 nodes in the second layer:* Classifying heuristics into two linguistic labels and assigning membership functions such as left sigmoid and right sigmoid for each of the linguistic value. Each of these heuristics is classified into linguistic labels as "Phishing" and "Legitimate". Based on experimental results and statistics from the dataset of 11,660 phishing sites, membership functions are calculated as follows:

- Membership functions for 'PrimaryDomain', 'SubDomain', 'PathDomain', 'PageRank', 'AlexaReputation', 'GoogleIndex' and 'BackLink': Equation (5) and (6) are two membership functions that are built to calculate fuzzy values and the graph of the membership functions is shown in Fig 4 .

$$L(x) = \frac{1}{1 + e^{-(x-b)}} \quad (5)$$

$$P(x) = \frac{e^{-(x-b)}}{1 + e^{-(x-b)}} \quad (6)$$

Where, parameter b for 'PrimaryDomain', 'SubDomain', 'PathDomain', 'PageRank', 'AlexaReputation', 'GoogleIndex' adn 'BackLink' are 4, 4, 4, 6, 20, 20 and 20 respectively.

- Membership functions for 'AlexaRank': Equation (7) and (8) are 2 membership functions built to calculate fuzzy values with parameter b of 300.000 and the graph of the membership functions is shown in Fig 5.

$$P(x) = \frac{1}{1 + e^{-(x-b)}} \quad (7)$$

$$L(x) = \frac{e^{-(x-b)}}{1 + e^{-(x-b)}} \quad (8)$$

4) *Neural Network Training Algorithm:* The proposed algorithm is shown in Fig 6. The algorithm performs two phases as follows:

- The "propagation" phase calculates the input value of the output node and the output value of the output node. The input value of the output node is calculated by (9)

$$O_I = \sum_{i=1}^8 W_i * I_i \quad (9)$$

Where, O_I , I_i and W_i are the input value of the output node, the value of the i th input node and the weight of the i th input node respectively.

The output value of the output node is calculated by (10)

$$O_O = \frac{1}{1 + e^{-O_I}} \quad (10)$$

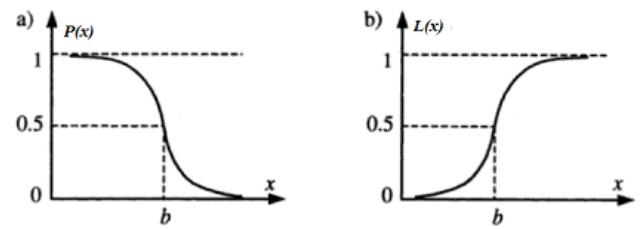


Fig. 4: Graph of membership function

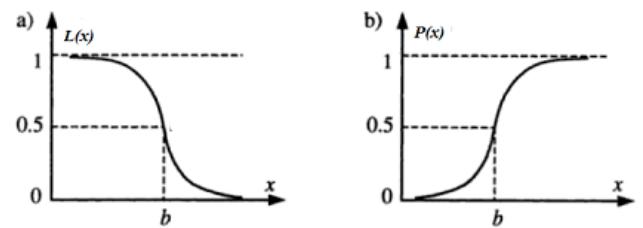


Fig. 5: Graph of membership function for "AlexaRank"

Where, O_O and O_I are the output value of output node and the input value of output node respectively.

- The "weight update" phase calculates the error of the output node and updates the weights. The error of the output node is calculated by (11).

$$Err_O = O_O * (1 - O_O) * (T - O_O) \quad (11)$$

Where, T is the actual value of sample in training dataset.

The system error is calculated by (12).

$$Err_S = \sqrt{\frac{\sum(Err_O_i^2)}{N}} \quad (12)$$

Where, Err_O_i is the error of the output node at the i^{th} sample of the training dataset.

The weights are updated by (13).

$$W_i = W_i + R * Err_S * O_S \quad (13)$$

Where, R and W_i are learning rate and the weight of the i^{th} input node. O_S is the system value calculated by (14).

$$O_S = \sqrt{\frac{\sum(O_i^2)}{N}} \quad (14)$$

Where, O_i is the output value at the i^{th} sample of the training dataset.

IV. EVALUATION

We have collected 22,000 phishing sites from PhishTank [3] and 10,000 legitimate sites from DMOZ [20]. The training dataset contains 17,000 phishing sites from PhishTank and 5,000 legitimate sites from DMOZ. We build 2 testing datasets, each of which contains 5,000 phishing sites or 5,000 legitimate sites. Experimental procedure is divided into 2 phases (Training and Testing) through PHP and MYSQL.

phish_id	url	phish_detail_url	submission_time	verified	verification_time	online
2111050	http://www.montenegrodrive.me/components/googledoc/index.htm	http://www.phishtank.com/phish_detail.php?phish_id=2111050	2013-11-17 09:12:02	yes	2013-11-17 14:21:40	yes
2111010	http://itunesconnect.apple.com.joitec.com.br/updat.../7e22ebef2732eeb0930c3daecfd49b3/	http://www.phishtank.com/phish_detail.php?phish_id=2111010	2013-11-17 09:08:17	yes	2013-11-17 13:58:52	yes
2111001	http://kuznyanova.org.ua/deal/googledocss	http://www.phishtank.com/phish_detail.php?phish_id=2111001	2013-11-17 09:07:32	yes	2013-11-17 14:07:39	yes
2110997	http://parmasseweb.tn/wp-includes/js/my.screenname.aol.com/my.screenname.aol.com/_cqr/index.php	http://www.phishtank.com/phish_detail.php?phish_id=2110997	2013-11-17 09:07:09	yes	2013-11-17 14:08:15	yes
2110988	http://paypal.com-inc-security-account-454536123584538489612545f45f456f45841.sorpi.fr/c20a4a1436d9442655a15c6b2b730d1a/?cmd=_home&dispatch=2f643150d63de9bd3e4d110f71b5d4a42f64:	http://www.phishtank.com/phish_detail.php?phish_id=2110988	2013-11-17 09:06:17	yes	2013-11-17 14:01:12	yes

Fig. 7: Training dataset of 22,000 sites in MySQL

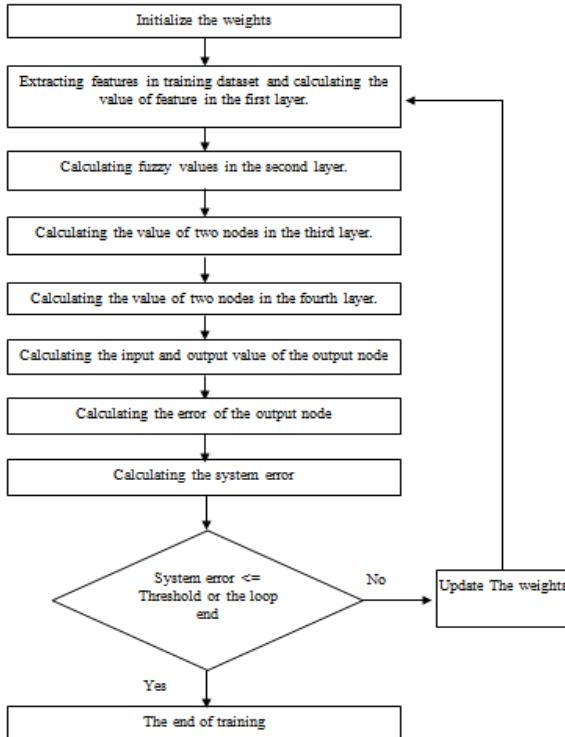


Fig. 6: Neural Network Training Algorithm

A. Training Phase

1) *Import Training Dataset*: Training dataset is imported into MYSQL. The result is shown in the Fig 7.

2) *Extracting four features of URL*: Four features (PrimaryDomain, SubDomain, PathDomain and Domain) are extracted. Fig 8 shows the obtained result.

3) *Calculating the value of eight input nodes*: Google search engine spelling suggestions and alexa.com are used to calculate the value of the input nodes. The result is shown in the Fig 9.

4) *Calculating the fuzzy value of 12 nodes in the second layer* : Two membership functions left sigmoid and right sigmoid are used to calculate the value of the nodes in the second layer. The result is shown in the Fig 10

5) *Network Training phase*: We performed the network training with 9 values of learning rate. In the training phase, the parameters are set as follows:

- Learning rate: 0.1, 0.2, 0.3, 0.4, 0.5, 0.6, 0.7, 0.8 and 0.9
- Mean error threshold value: 1×10^{-5}
- Number of Epochs: 10,000
- The weights: initialize weights random values from 0 to 1

B. Testing Phase

In this phase, the proposed technique is tested with 2 testing datasets based on the weights of the network training with learning rate of 0.1, 0.2, 0.3, 0.4, 0.5, 0.5, 0.6, 0.7, 0.8, 0.9. RMSE (Root Mean Square Error) is a good measure of identifying accuracy. RMSE is calculated by (15)

$$RMSE = \sqrt{\frac{\sum(A_i - I_i)^2}{N}} \quad (15)$$

Where, I_i is the number of identifying sites, A_i is the number of actual sites and N is the number of samples in the testing dataset. Accuracy ratio is calculated as follows: Accuracy_Ratio = 100 - RMSE. The results of the test with learning rate of 0.1, 0.2, 0.3, 0.4, 0.5, 0.5, 0.6, 0.7, 0.8, 0.9 will be shown in Table I. From the obtained results, RMSE and accuracy are shown in Table II. We have found It shows the best ratio of 99.29% with learning rate of 0.7 and the worst ratio of 98.31% with learning rate of 0.2.

C. Comparing to technique [12]

We experimented with the technique [12] and compared to the result of our proposed technique. First, we collect 10 testing datasets, each of which contains 1,000 phishing sites or 1,000 legitimate sites. Second, we experiment the technique [12] and the results will be shown in Table III. From the obtained result and using RMSE, we have found that the technique [12] with the accuracy of 86.06%.

D. Comparing to technique [13]

We experimented with the technique [13] using 8 hidden nodes and hyperbolic tangent activation function. First, we collect 2 testing datasets, each of which contains 5,000 phishing sites or 5,000 legitimate sites. Second, we experiment the technique [13] and the results will be shown in Table IV. Then, the obtained results of RMSE and accuracy are shown in Table V. By using the technique in [13], we obtained the best accuracy of 94.68%.

phish_id	domain	primarydomain	subdomain	pathdomain
2111050	montenegrodrive.me	montenegrodrive		components,googledoc,index.htm
2111010	jooltec.com.br	jooltec	itunesconnect.apple.com	updat,
2111001	kuznyanova.org.ua	kuznyanova		deal,googledocss,googledocss,sss
2110997	paraseweb.tn	paraseweb		wp,includes.js,my.screenname.aol.com,my.screenname.aol.com,cqr.index.php
2110988	sorpi.fr	sorpi	paypal,com,inc,security,account	cmd,home&dispatch,2f643150d63de9bd3e4d110f71b5d4a42f643150d63de9bd3e4d110f7

Fig. 8: Four features are extracted

phish_id	primarydomain	subdomain	pathdomain	pagerank	alexarank	alexareputation	backlink	googleindex
2111050	100	100	2	0	6274104		2	0
2111010	100	0	100	0	6274104		2	0
2111001	100	100	0	1	6274104		2	6280750
2110997	23	100	0	0	160379		18	0
2110988	5	0	100	0	7104259		1	7111380

Fig. 9: Value of heuristics

phish_id	P1	P2	P3	P4	P5	P6	P7	P8	L1	L2	L3	L4	L5	L6	L7	L8
2111050	0.00	0.00	0.88	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.12	0.00	0.00	0.00	0.00	0.00
2111010	0.00	0.98	0.00	1.00	1.00	1.00	1.00	1.00	1.00	0.02	1.00	0.00	0.00	0.00	0.00	0.00
2111001	0.00	0.00	0.98	0.99	1.00	1.00	0.00	1.00	1.00	1.00	0.02	0.01	0.00	0.00	1.00	0.00
2110997	0.00	0.00	0.98	1.00	0.00	0.88	1.00	0.88	1.00	1.00	0.02	0.00	1.00	0.12	0.00	0.12
2110988	0.27	0.98	0.00	1.00	1.00	1.00	0.00	1.00	0.73	0.02	1.00	0.00	0.00	0.00	1.00	0.00

Fig. 10: Fuzzy values in the second layer

TABLE I: result of testing with proposed technique

Learning Rate	Testing dataset	A_i	I_i
0.1	No.1	5,000	4,925
0.1	No.2	5,000	4,917
0.2	No.1	5,000	4,913
0.2	No.2	5,000	4,918
0.3	No.1	5,000	4,926
0.3	No.2	5,000	4,933
0.4	No.1	5,000	4,946
0.4	No.2	5,000	4,935
0.5	No.1	5,000	4,933
0.5	No.2	5,000	4,927
0.6	No.1	5,000	4,925
0.6	No.2	5,000	4,927
0.7	No.1	5,000	4,965
0.7	No.2	5,000	4,964
0.8	No.1	5,000	4,914
0.8	No.2	5,000	4,915
0.9	No.1	5,000	4,920
0.9	No.2	5,000	4,912

V. CONCLUSIONS

In this paper, we have proposed a new technique to identify phishing sites effectively. The system model is built to identify phishing sites by using neuro-fuzzy network and eight

TABLE II: RMSE and Accuracy with proposed technique

Learing rate	RMSE	Accuracy
0.1	1.58	98.42%
0.2	1.75	98.25%
0.3	1.41	98.59%
0.4	1.20	98.80%
0.5	1.40	98.60%
0.6	1.48	98.52%
0.7	0.78	99.22%
0.8	1.71	98.29%
0.9	1.68	98.32%

TABLE III: result of testing with technique [12]

(1):Very Phishy and Phishy (2) : Very Legitimate and Legitimate (3) : Suspicious

Testing dataset	(1)	(2)	(3)
No.1	867	82	51
No.2	865	76	59
No.3	847	90	63
No.4	902	172	26
No.5	841	109	50
No.6	64	873	63
No.7	50	911	39
No.8	39	895	66
No.9	97	871	32
No.10	85	863	52

TABLE IV: result of testing with technique [13]

Learning Rate	Testing dataset	A_i	I_i
0.1	No.1	5,000	4,612
0.1	No.2	5,000	4,520
0.2	No.1	5,000	4,624
0.2	No.2	5,000	4,478
0.3	No.1	5,000	4,689
0.3	No.2	5,000	4,735
0.4	No.1	5,000	4,456
0.4	No.2	5,000	4,792
0.5	No.1	5,000	4,732
0.5	No.2	5,000	4,736
0.6	No.1	5,000	4,721
0.6	No.2	5,000	4,678
0.7	No.1	5,000	4,599
0.7	No.2	5,000	4,725
0.8	No.1	5,000	4,772
0.8	No.2	5,000	4,697
0.9	No.1	5,000	4,719
0.9	No.2	5,000	4,699

TABLE V: RMSE and Accuracy with technique [13]

Learing rate	RMSE	Accuracy
0.1	8.73	91.27%
0.2	9.10	90.90%
0.3	5.78	94.22%
0.4	8.24	91.76%
0.5	5.32	94.68%
0.6	6.03	93.97%
0.7	6.88	93.12%
0.8	5.36	94.64%
0.9	5.82	94.18%

heuristics (primarydomain, subdomain, pathdomain, pagerank, alexarank, alexareputation, googleindex, backlink). The technique is experimented with the training dataset containing 22,000 sites and 2 testing datasets that each dataset contains 5,000 phishing sites or 5,000 legitimate sites. The best results show that 99.29% phishing websites are identified by using the system model. Our work is compared to the results in [12], [13] and found that it is more efficient. In the future, our neuro-fuzzy model will be improved to enhance the identification ratio. Besides, the system could be furthermore enhanced by using larger datasets and more heuristic parameters.

ACKNOWLEDGMENT

We express our sincere thanks to the reviewers for their valuable comments and suggestions on this manuscript.

REFERENCES

- [1] Ollman, G. (2004) The Phishing Guide —Understanding and Preventing. White Paper, Next Generation Security Software Ltd.
- [2] Anti-phishing working group. URL <http://www.antiphishing.org>.
- [3] PhishTank. (2015, May). [Online]. Available: <http://www.phishtank.com>
- [4] D. Goodin. (2012) Google bots detect 9,500 new malicious websites every day. [Online]. Available: <http://arstechnica.com/security/2012/06/>
- [5] S. Sheng, B. Wardman, G. Warner, L. Cranor, J. Hong, and C. Zhang. (2009) An empirical analysis of phishing blacklists. [Online]. Available: <http://ceas.cc/2009/papers/ceas2009-paper-32.pdf>

- [6] McAfee. (2011, July) McAfee site advisor. [Online]. Available: <http://www.siteadvisor.com>
- [7] Y. Zhang, J. I. Hong, and L. F. Cranor, Cantina: a content-based approach to detecting phishing web sites, in The 16th international conference on World Wide Web, 2007, pp. 639—648
- [8] G. Xiang, J. Hong, C. P. Rose, and L. Cranor, Cantina+: a feature-rich machine learning framework for detecting phishing web sites, ACM Transactions on Information and System Security, vol.14, no.2 .pp. 1—28, Sept. 2011.
- [9] M. E. Maurer and D. Herzner, Using visual website similarity for phishing detection and reporting, in CHI 12 Extended Abstracts on Human Factors in Computing Systems, 2012, pp. 1625—1630.
- [10] A. Sunil and A. Sardana, A pagerank based detection technique for phishing web sites, in IEEE Symposium on Computers & Informatics, 2012, pp. 58—63.
- [11] M. G. Alkhozae and O. A. Batarfi, Phishing websites detected based on phishing characteristic in the webpage source code, in International Journal of Information and Communication Technology Research, vol. 1, no. 6, Oct. 2011, pp. 283—291
- [12] M. Aburous, M. Hossain, K. Dahal, and F. Thabtah (2010). Intelligent phishing detection system for e-banking using fuzzy data mining. Expert Systems with Applications, 37 (12), pages 7913 - 7921. Elsevier.
- [13] N. Zhang and Y. Yuan, Phishing Detection Using Neural Network, CS229 lecture notes, <http://cs229.stanford.edu/proj2012/ZhangYuan-PhishingDetectionUsingNeuralNetwork.pdf>, 2012
- [14] A Naga Venkata Sunil and Anjali Sardana. A pagerank based detection technique for phishing web sites. In Computers & Informatics (ISCI), 2012 IEEE Symposium on, pages 58-63. IEEE, 2012.
- [15] Jun Ho Huh and Hyoungshick Kim. Phishing detection with popular search engines: Simple and effective. In Foundations and Practice of Security, pages 194–207. Springer, 2012.
- [16] Wikipedia. [Online]. Available (2015) : <http://en.wikipedia.org/wiki/Uniformresourcelocator>
- [17] Levenshtein. [Online]. Available (2015) : <http://en.wikipedia.org/wiki/Levenshteindistance>
- [18] G. Inc. [Online]. Available (2015) : <http://toolbarqueries.google.com>
- [19] Alexa. [Online]. Available (2014) : <http://data.alexa.com/data?cli=10&dat=sbamz&url=>
- [20] DMOZ. [Online]. Available (2015, May) : <http://rdf.dmoz.org/rdf/>

A Predictable Markov Based Cache Replacement Scheme in Mobile Environments

Ahmed. A. A. Gad-ElRab

Faculty of Science
Al-Azhar University
Cairo, Egypt

Kamal A. ElDahshan

Faculty of science
Al-Azhar University
Cairo, Egypt

Ahmed Sobhi

Faculty of Science
Al-Azhar University
Cairo, Egypt

Abstract—Mobile Location-dependent services are popular services that the mobile environments support. Data caching is an effective technique that plays an important role in improving these services. In mobile environments, due to the limited cache size of mobile devices, the cache replacement which is finding a suitable subset of items for eviction from cache becomes important. Most of the existing cache replacement schemes use the cost functions in the replacement operation. In this paper we propose a Predictable Markov based Cache Replacement (PMCR) scheme for Mobile Environments. The proposed scheme uses a markov model with cost function in the replacement operation. The key idea of the markov model is the prediction of future client locations by giving us the weight of visiting each location whose data is cached. Simulation results show that our approach improves the system performance compared to the existing schemes.

Keywords-Mobile Location-dependent services; Data dissemination; Cache replacement; Predicted region; Markov model; PMCR.

I. INTRODUCTION

The development of wireless communication systems and computer hardware technology has led to mobile computing. The mobile computing research area includes the effect of mobility on hardware, software, users, data and computing in wireless computer applications. With this technology, users can access a variety of information from anywhere and at any time via a wireless channel [1], [2].

The main properties of mobile environments include unrestricted mobility, asymmetric communication, limited wireless communication, limited client power, frequent disconnections, and limited client capacities has opened many challenging problems of mobile data applications [3], [4].

In wireless environments, a mobile client can move and access information anytime and anywhere. So, to enable mobile data access there are methods methods. One of the main methods of wireless data access is data dissemination.

Data dissemination refers to broadcasting of database items to mobile clients through one or more wireless channels. There are three mechanisms of data dissemination: **push-based Mechanism**, **On-demand (or pull-based) Mechanism**, and **Hybrid Mechanism**. In **the push based mechanism**, a server disseminates data generally without any request from clients. For example, advertising, weather reports, and news reports scenarios. In **the On-demand mechanism**, a server disseminates data based on the outstanding requests submitted by clients. For example, finding the nearest restaurant, buying a music album, or bank account activity scenarios. In **the hybrid mechanism**, push based and on demand data are combined to complement each other. For example, advertising and selling music albums scenario. The advertisements are pushed and the mobile devices pull for buying the album.

The important two issues of data dissemination are: *Minimizing access time* and *Minimizing tuning time*. Access time is the period of time elapsed from the moment a mobile client requesting a data item(s) to the moment when the requested data item(s) is received by the client. While the tuning time is the time that a client spends actively listening to the broadcast wireless channel to receive the requested data items [5], [6], [7].

Data-caching is a common technique for minimizing access time, it is an effective technique to reduce access time by caching of frequently accessed data item on client side. When the client issues a query, it first searches the cache. If there is a valid answer of requested data in the cache, an answer is returned immediately. Otherwise, the client attempts to obtain the answer item from a server.

Client data caching is important due to the limitations of mobile environments. Therefore, there are two common issues involved in client cache management: *Cache Invalidation* and *Cache Replacement*. Cache invalidation maintains data consistency between client's cache and the server database. While cache replacement determines which subset of data items is replaced when it does not have enough free space to store a new data item [1], [2], [6], [8].

Due to the limitations of client capacities, there is a need to design an efficient cache replacement algorithm to find a subset of data items for replaced from the cache. Also, the design of an efficient cache replacement scheme becomes very important and challenging to ensure good cache performance [9], [10].

Several cache replacement schemes have been proposed in the literature. Most of them are suitable if the client changes its movement's direction quite often, but do not take into account the future location of a client. To find the most suitable cache replacement scheme, it is very important to take into account a current and future location of a client in the replacement operation. In this paper, A Predictable Markov based Cache Replacement (PMCR) scheme for Mobile Environments is proposed. The proposed scheme uses a markov model with a cost function to support the replacement decision [2], [10], [11].

The rest of this paper is organized as follows: section 2 present the related work. Section 3 introduces the client/server mobile system model. Section 4 describes the predicted region with Markov Model based Cache Replacement. In Section 5; the simulation model, the experimental results and analysis are presented. Conclusion and further work are given in Section 6.

II. RELATED WORK

Several location dependent cache replacement schemes have been proposed. Most of these schemes use cost functions, which take into account both the spatial and temporal properties of the client's movement, that incorporates different factors considered in cache replacement schemes including access probability, valid scope area, data distance and data size. Access probability, is considered to be the most important factor that affects cache performance. Data with the least access probability will have the highest priority to be replaced by the new data object. Valid scope area refers to the geometric area of the valid scope of a data value. The larger the valid scope area of the data, the higher the probability that the mobile client requests this data. This is because, generally, the mobile client has a higher chance of being in large regions than small regions. Data distance refers to the distance between the current location of a mobile client and the valid scope of a data value. In a location-dependent data service, the server responds to a query with the suitable value of the data item according to the client's current location. As such, when the valid scope of a data value is far away from the client's current location, this data will have a lower chance to become usable again since it will take some time before the client enters the valid scope area again. Data size refers to the size of the data stored in the mobile client's cache. The amount of space required to store the data item in the cache is used to select an item for replacement, so keeping smaller size data items in the cache helps to accommodate a large number of data items [1], [2], [10], [11].

The Manhattan Distance-based cache replacement policy considers the distance between a client's current location and the location of each object whose data is cached when there is need of cache replacement. The data items with the highest Manhattan distance are replaced. The Manhattan

policy is limited because it considers the distance and spatial properties only. While the temporal properties and the direction of the client movement is not taken into account when making cache replacement decisions [11], [12].

The Farther Away Replacement (FAR) replacement policy considers the mobile client current location and its direction to make the replacement decision. The replacement policy is based on the fact that the data which are not in the moving direction and farthest away from the user will not be visited in the near future. FAR considers only the spatial properties for cache replacement and the temporal properties are not taken into account, it is also not very useful when the mobile client changes its direction (random movement) [11], [13].

Probability Area (PA) policy considers only temporal property of data for replacement, the cost function for cache replacement is considering the parameters access probability and valid scope area. The data with low access probability and a small valid scope area is replaced first. PA does not take into account the data distance and the size of the data object whose data is stored in cache. PA is ineffective for random movement of mobile client [1], [11].

Probability Area Inverse Distance (PAID) policy considers both spatial and temporal properties of data for replacement. The cost function for replacement is considering the parameters access probability, valid scope area and data distance. The data with low access probability, a small valid scope area, and a long distance is replaced first. PAID does not take into account the size of the data object stored in cache, considers only the clients current movement direction, and ineffective for random movement of mobile client [1], [11].

Mobility Aware Replacement Scheme (MARS) is also considering the cost function for cache replacement decisions. It makes cache replacement decisions through a cost function which takes into account both the spatial and temporal properties of the client's movement. The cost function takes into account both the spatial and temporal properties of the client's movement. The data item with the lowest cost function is removed from the client's cache and replaced by the new object. MARS is ineffective for random movement of mobile client [11], [14].

None of these cache replacement schemes is suitable for mobile client random movements. Existing cache replacement schemes only consider the data distance but not the distance based on region where the client may be in the near future. In ***Prioritized Predicted Region based Replacement Policy (PPRRP)*** [10] and ***Distance-based Predicted Region Policy (DPRP)*** [15] instead of taking the direction of client's movement they predict an area/region in which the client will be in the near future. PPRRP and DPRP tried to get the benefit of both temporal and spatial properties, and they are also suitable when the mobile client frequently changes its movement's direction (random movement).

Associated with each cached data item is the replacement cost; the cost function is calculated based on the access probability, valid scope area, data size in cache and distance of

data based on the predicted region. When a new data needs to be cached and there is insufficient space, the data item out of the predicted region with lowest cost function is removed from the client's cache and replaced by the new data item. PPRRP and DPRP uses only the cost function but does not take into account the future location of a client when making cache replacement decisions [10], [11], [15].

Markov Model based Cache Replacement Policy (MMCRP) and Markov Graph Cache Replacement Policy (MGCRP) predict the next client location by first and/or second order Markov Models. The graph is used to represent locations whose data is cached. If the cache is full and requires replacement then data items will be evicted of the location which is not in the close proximity. In the worst case, if all locations are in the close proximity then replacement will be based on invalid scope, minimum access probability and large distance. MMCRP and MGCRP use only the markov models but do not take into account the cost function and the predicted region when making cache replacement decisions [2], [16].

III. MOBILE SYSTEM MODEL

This section describes the general mobile computing model. It consists of two sets of entities: mobile clients and fixed hosts (see Figure 1). A mobile client (MC) is a mobile unit which is capable of connecting to fixed network through wireless channel. Fixed networks are classified as either fixed hosts (data server) or base stations, and connected together through a fixed high-speed wired network. Mobile clients and the fixed network can communicate with each other through wireless channels via Base stations (BS). The wireless channel between MC and BS is separated into two sub-channels: an uplink channel and a downlink channel. The uplink channel is used by MCs to send queries to the server via a BS, while the downlink channel is used by BSs to forward the answers from the server to the mobile client. The entire geographical area is divided into one or more cells, each of which is supported by base station. An MC movement from one cell to another, while retaining its wireless connection is called hand-off. After hand-off, its wireless connection is switched to the new cell [1], [17].

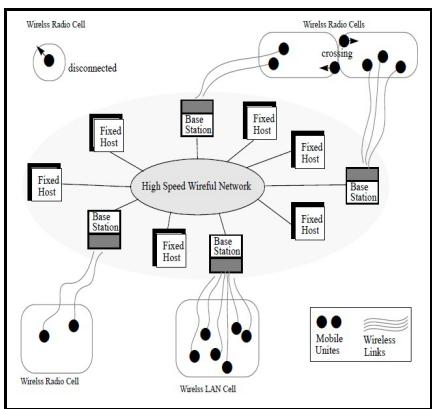


Figure 1. A mobile system model [17]

The mobile computing system model provides location dependent services to mobile units. When the mobile client

issues a query, a data item can show different values when it is queried from different cells. The valid scope is defined as the set of cells within which the data item value is valid. For example (see Figure 2), the "nearby-restaurant" is a data item, the data item value for this data item is {A} with the valid scope {1, 2} or {B} with the valid scope {3, 4}. Note that, a data item value varies when it is queried from different cells [2], [10].

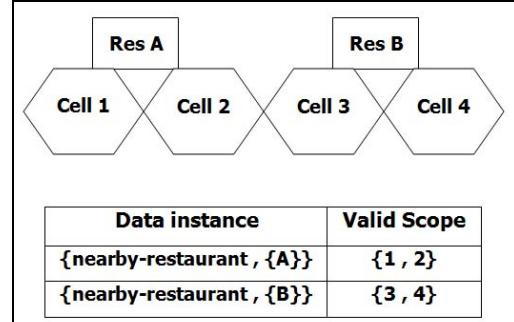


Figure 2. Data instance and valid scope representation [15].

IV. A PREDICTABLE MARKOV BASED CACHE REPLACEMENT (PMCR)

In this section, a new cache replacement scheme based on a predicted region with Markov model is proposed. Firstly, a predicted region which is defined in DPR [15] will be introduced. Secondly, the replacement cost function. Thirdly, the Markov model. Fourthly, New cost for replacement. Finally, the proposed cache replacement scheme will be described.

A. Predicted region

A predicted region is important in improving the system performance. One of the main advantages of predicted regions is considering unrestricted mobility for mobile units. Using the predicted region, the data values around the client's current position are not replaced from cache. The predicted region is based on the root-mean squared distance which is defined in DPR [15]. The root-mean squared distance that is based on the distance between a client's current location and the locations of each object whose data is cached.

Let the radius r be calculated as the root-mean squared distance (see Figure 3). So, if the current location (center of the predicted region) is c , the radius of the predicted region is:

$$r = \sqrt{\frac{\sum_{i=1}^K (c_i - c)^2}{K}} = \sqrt{\frac{\sum_{i=1}^K (d_i)^2}{K}}$$

Where: r Radius of the predicted region.

$(c_i - c)$ Distance (d_i) between the current location (c) and valid scope (c_i).

K Number of object whose data is cached.

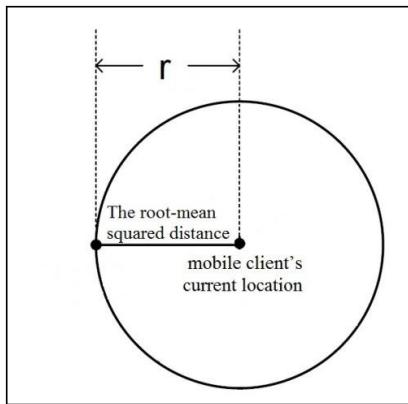


Figure 3. Distance-based predicted region [15]

One of the advantages of using the DPR is that it reduces computation overhead and also takes into account the unrestricted mobility of the mobile client. Reducing the computation overhead plays an important role in improving the performance of cache replacement schemes.

B. The cost function for replacement

The cost function is based on the access probability, valid scope area, size of data in the cache and the distance between the mobile client's current location and the locations of objects whose data is cached. The cost of data value j of data item i in client's cache is [10], [11]:

$$Cost_{i,j} = \begin{cases} \frac{P_i \cdot A(vs'_{i,j})}{S_{i,j}} \cdot \frac{1}{\min\{r, D(vs'_{i,j})\}} & \text{if } vs'_{i,j} \in \text{DPR} \\ \frac{P_i \cdot A(vs'_{i,j})}{S_{i,j}} \cdot \frac{1}{D'(vs'_{i,j})} & \text{if } vs'_{i,j} \notin \text{DPR} \end{cases}$$

Where

- P_i The access probability of data item i .
- $A(vs'_{i,j})$ The area of the valid scope $vs'_{i,j}$ for data value j .
- $S_{i,j}$ The size of data value j and valid scope $vs'_{i,j}$.
- $D(vs'_{i,j})$ The distance of the valid scope $vs'_{i,j}$ from the current position.
- $D'(vs'_{i,j})$ The distance of the valid scope $vs'_{i,j}$ from the centre of the predicted region.
- DPR The distance-based predicted region.

The distance is calculated as follows:

- The distance of data items outside PR is calculated from the centre of the region.
- The distance of data items inside PR is the minimum of $\{r, \text{distance of the valid scope from the current position of the user}\}$.

Items outside PR have the lower priority than those inside the predicted region.

C. Markov model

Markov model has been used to predict the future client locations by giving the weight of visiting each location whose data is cached. The fundamental assumption of predictions based on Markov models is that The previous locations affect the predication of next location.

The input data for building Markov models consists of the actions and the states. The actions for the Markov model correspond to the previous location visited by the mobile client (i.e. the client's path). Some of them are subject to queries, so they are stored in the cache and called the states. If allocation is removed from the cache, it no longer belongs to the states (see Fig 4). Once the states of the Markov model and the client's path have been identified, the transition probability matrix (TPM) can be computed. The TPM can be built by using the client's path and each t_{ji} may be calculated as the frequency of the event that action a_i follows the state s_j [15], [16].

For example consider the client's path ($\{L3, L5, L2, L1, L4, L5, L2, L3, L4\}$) and one of the locations whose data is cached is $L5$. The location $L5$ corresponds to the state s_j , and the action a_1 ($L2$) follows the state s_j ($L5$), thus the entry t_{ji} in the TPM will be updated (see Fig. 4).

		actions i			
		a_1	$a_i = L2$	a_n	
states j	s_1				
	$s_j = L5$		$t_{ji} = 2$		
	s_m				

Figure 4. The actions and the states of Markov models

Once the transition probability matrix is built, making the prediction by giving the weight of visiting each location whose data is cached is straightforward as follow (see Fig. 5):

- Compute S_j , the summation for all elements of TPM (t_{ji}) for each state (s_j) : $S_j = \sum_{i=1}^n t_{ji}$, $j = 1, \dots, m$.
- Where: n is the number of the actions and m is the number of the states.
- Compute S , the summation for all S_j : $S = \sum_{j=1}^m S_j$
- The weight of visiting each location whose data is cached: $W_{s_j} = \frac{S_j}{S}$, $0 \leq W_{s_j} \leq 1$, $j = 1, \dots, m$.

	a_i			
s_j	t_{ji}		$S_j = \sum_{i=1}^n t_{ji}$	$W_{S_j} = \frac{S_j}{S}$
			$S = \sum_{j=1}^m S_j$	

Figure 5. TPM for Markov models

D. New cost for replacement

In the data-caching method, the data item outside the predicted region with minimal for cost function is replaced by the new data item. The replacement decision depends only on the cost function. We can find a new cost for replacement by integrating the cost function and the weight results from the markov model using normalization by rescaling. This method is used to standardize the range of independent variables of data measured on different scales to a common scale [18], [19]. The general formula of rescaling independent variables between 0 and R is given as:

$$x' = \frac{x - \min(x)}{\max(x) - \min(x)} \times R$$

Where: x is an original value and x' is the normalized value

The new cost value is the average of two normalized values, cost function and the weight results from markov model. When a new data item needs to be cached and there is insufficient cache space, the data value out of the predicted region with lowest new cost value is removed from the client's cache and replaced by the new data value [10].

E. The proposed cache replacement scheme

Here, based on DPR and markov model, a new scheme called a *Predictable Markov based Cache Replacement* (PMCR) in Mobile Environments is proposed. In PMCR, data is cached at the mobile client.

When the mobile client issues a query, it searches first on its cache. If there is a valid answer in the cache, an answer is returned immediately. Otherwise, the client attempts to obtain the data value from the server [20]. If the client's cache does not have enough space to store a new data value, PMCR does the following steps for the cached data items in the mobile client:

- Compute the access probability, valid scope area, data size and data distance.
- Compute the radius (r) of DPR by using the root-mean squared distance.
- Determine which data inside or outside the DPR

If $d_i > r$ then the data value $_i$ outside DPR.

If $d_i \leq r$ then the data value $_i$ inside DPR.

d_i is the distance between the mobile client current location and the valid scope of data value $_i$.

- Compute the cost value.
- Compute the weight of visiting each location whose data is cached by Markov Model.
- Compute the new cost value.
- The data item out of DPR and has lowest new cost value is removed from the client's cache and replaced by the new data item.

Algorithm 1 shows the steps of PMCR.

Algorithm 1: Steps of PMCR Algorithm

Mobile Client (MC) requests for data item D_i

if D_i is valid and in cache **then** return D_i

else if cache misses D_i **then**

send the request to the server

get D_i from the server

server send D_i to MC

if enough free space in client's cache **then** store D_i in cache

else if not enough free space **then**

replacing data value (s) from cache which:

- out of predicted region
- has lowest new cost value

end if

end if

V. SIMULATION AND RESULTS

This section shows the simulation model which is used to evaluate the performance of PMCR. To show the effectiveness of PMCR, it is compared with DPRP [15]. The discrete-time simulation package OMNeT++ [21] was used to implement this simulation model.

A. Simulation Model Description

The simulation model consists of three main entities: network, mobile client, and sever. These entities are described as follows [1].

(a) **Network** is a cellular network that consists of many cells and provides seamless handoffs between cells. As such, the network can be considered as a large service area, the clients can move and obtain location-dependent services. The service area is represented by a rectangle of fixed size. The database items may display different values for different client locations within the service area. The wireless network is modeled by an uplink and downlink channel. The uplink channel is used by the client to send queries to the server and the downlink

channel is used by the server to forward the answers to the mobile client.

(b) **Mobile client** is modeled with two processes: the query process and the move process. The query process generates location-dependent queries for different data items. After the current query is completed, the client waits for a query interval, QI, before the next query is generated. To answer a query, the client's cache is checked first. If the answer for the requested item corresponding to the current location is available, the query is satisfied locally. Otherwise, the client sends the query and its location to the server and retrieves the answer from the server through the downlink channel. The move process controls the client's movement using MovingInterval. After the client keeps moving at a constant velocity for a period of time, it changes the velocity in a random way for next MI. The next speed is selected randomly between MinSpeed and MaxSpeed and the next moving direction is selected randomly between 0 and 360. The mobile client is assumed to have a fixed size cache, which is a ratio of the size of database.

(c) **Server** is modeled by a single process that offers to the requests from mobile clients. To answer a location-dependent query, the server locates the data value with respect to the specified location.

B. Performance Evaluation

In this subsection, DPRP [15] and PMCR are evaluated to show the performance of PMCR. Table 1 shows the default values of different parameters for the simulation model. To compute the distance between valid scope and current location, a reference point is selected for each valid scope and calculates the *Euclidean distance* between the current location and this reference point. The reference point is the endpoint that is closest to the current location. To find the access probability, two parameters are maintained for each data item i : a running probability (P_i) and the time of the last access to data item (t_i'). Initially, P_i is set equal 0. When a new query is issued for data item i , P_i is updated using the formula:

$$p_i^{new} = \alpha / (t_c - t_i') + (1 - \alpha) p_i^{old}$$

Where, t_c is the current time and α is a constant factor to weight the importance of most recent access in the probability estimation.

In the performance evaluation, "cache hit ratio", "energy consumption" and "access time" are used as performance evaluation metrics. The cache hit ratio defined as the ratio of the number of queries answered by the client's cache to the number of queries generated by the client. The access time is the time elapsed from the moment a mobile client requests a data to the moment when the requested data is received by the client [1], [10].

TABLE1. THE DEFAULT PARAMETER SETTINGS OF THE SIMULATION MODEL

Parameter	Description	Setting
Size	Size of the service area	1200 * 1200 m
MCNum	Number of mobile client in the service area	5
LNum	Number of location in the service area	36
ItemNum	Number of data item in the server database	360
UplinkBand	Bandwidth of the uplink channel	1Mbps
DownlinkBand	Bandwidth of the downlink channel	2Mbps
QueryInterval	average time interval between two consecutive queries	25 s
MovingInterval	Time duration that the mobile client keeps moving at a constant velocity	50 s
MinSpeed	minimum speed of the client	2 m s ⁻¹
MaxSpeed	maximum speed of the client	5 m s ⁻¹
CacheSizeRatio	Ratio of the cache size of the database size	5% = 18
α	Weight factor for running access rate estimate	0.25

In the rest of this section, to prove the efficiency of our scheme compared to the DPRP [15], the effect of query interval, moving interval, cache size, number of queries, and number of clients will be shown in details.

1) Effect of Changing the Query Interval

The query interval is the time interval between two consecutive queries. In this set of experiments, the query interval was increased from 20 to 100 seconds. Table 2 gives the default parameters for changing the query interval.

TABLE2. THE DEFAULT PARAMETER FOR CHANGING QUERY INTERVAL

Moving Interval (MI)	Cache Size	Number of Queries	Number of clients
50 s	5%	200	5

Figure 6 depicts the performance results of query interval versus the cache hit ratio. As shown in Figure 6, as the query interval increases, the cache hit ratio decreases. This is because, the mobile client would make more movements between two queries, thus the client has a lower probability of residing in one of the valid scopes of the previously queried data items when a new query is issued. Consequently, the cached data are less likely to be re-used for subsequent queries. This leads to a decreased performance of the cache hit ratio with increase in the query interval. Also, the cache hit ratio of PMCR is higher than its value in DPRP. This is because the proposed scheme outperforms the existing scheme.

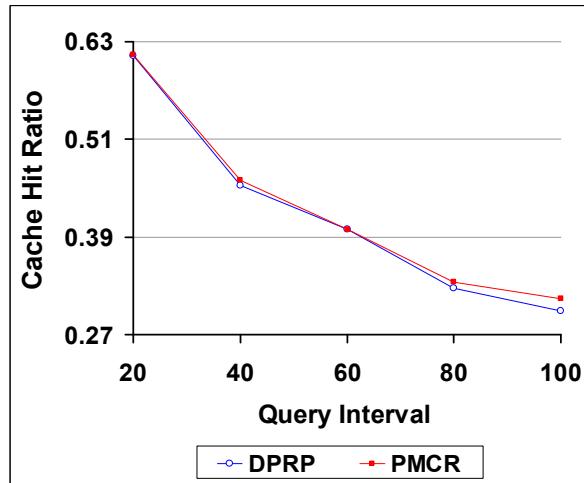


Figure6. Cache hit ratio vs query interval

Figure 7 depicts the performance results of query interval versus access time. As shown in Figure 7, as the query interval increases, the access time increases. This is because, the client would make more movements between two queries, thus the client has a lower probability of residing in one of the valid scopes of the previously queried data items when a new query is issued. Consequently, the cached data are less likely to be re-used for subsequent queries. This leads to, with moving interval, number of query and cache size invariant, the access time increased as the query interval increased. Also, access time of PMCR is lower than its value in DPRP. This is because the proposed scheme outperforms the existing scheme.

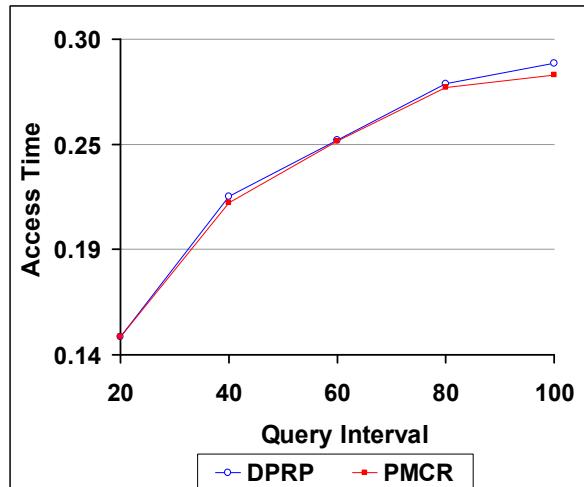


Figure7. Access time vs query interval

Figure 8 depicts the performance results of query interval versus energy consumption. As shown in Figure 8, as the query interval increases, the energy consumption increase. This is because, the client would make more movements between two queries, thus the client has a lower probability of residing in one of the valid scopes of the previously queried data items when a new query is issued.

Consequently, the cached data are less likely to be re-used for subsequent queries. This leads to, with moving interval, number of query and cache size invariant, the energy consumption increased as the query interval increased. Also, the energy consumption of PMCR is lower than its value in DPRP. This is because the proposed scheme outperforms the existing scheme.

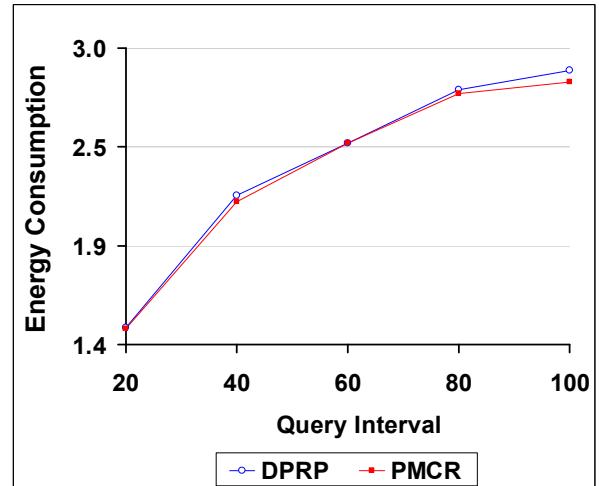


Figure8. Energy consumption vs query interval

As shown, when the two cache replacement schemes are compared, the PMCR has a better performance when the query interval is changed.

2) Effect of Changing the Moving Interval

This subsection investigates the performance of the proposed replacement scheme when the moving interval is varied. MI is the time period that the client keeps moving at a constant velocity and direction. In this set of experiments, the moving interval was varied from 25 seconds to 225 seconds. Table 3 gives the default parameters for changing MI.

TABLE 3. THE DEFAULT PARAMETER FOR CHANGING MOVING INTERVAL

Query Interval (QI)	Cache Size	Number of Queries	Number of clients
25 s	5%	200	5

Figure 9 depicts the performance results of MI versus cache hit ratio. As shown in Figure 9, as MI increases, the cache hit ratio decreases. This is because, there is a high probability of the client leaving one valid region and entering another. Consequently, the cached data are less likely to be re-used for subsequent queries. This leads to, with query interval, number of query and cache size invariant, a decreased performance of cache hit ratio with increase in MI. Also, the cache hit ratio of PMCR is higher than its value in DPRP. This is because the proposed scheme outperforms the existing scheme.

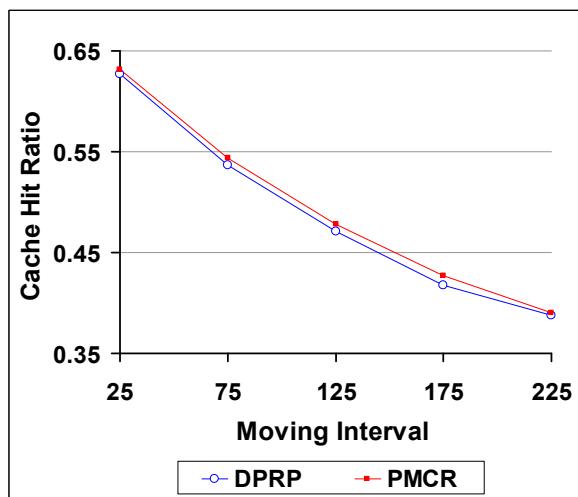


Figure9. Cache hit ratio vs moving interval

Figure 10 depicts the performance results of MI versus access time. As shown in Figure 10, as MI increases, the access time increases. This is because, there is a high probability of the client leaving one valid region and entering another. Consequently, the cached data are less likely to be re-used for subsequent queries. This leads to, with query interval, number of query and cache size invariant, the access time increased as the MI increased. Also, access time of PMCR is lower than its value in DPRP. This is because the proposed scheme outperforms the existing scheme.

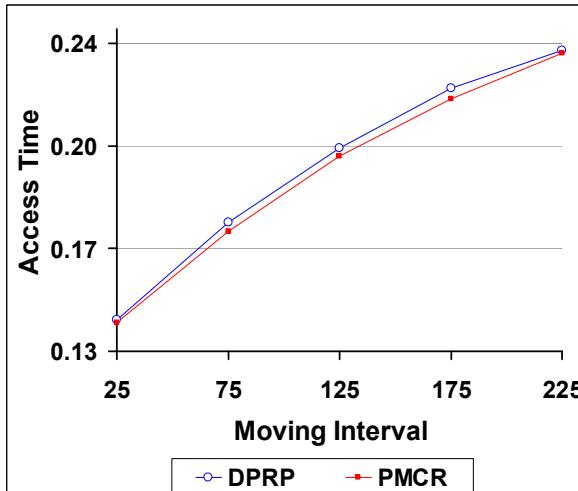


Figure10. Access time vs moving interval

Figure 11 depicts the performance results of MI versus energy consumption. As shown in Figure 11, as MI increases, the energy consumption increases. This is because, there is a high probability of the client leaving one valid region and entering another. Consequently, the cached data are less likely to be re-used for subsequent queries. This leads to, with query interval, number of query and cache size invariant, the energy consumption increased as the MI increased. Also, the energy

consumption of PMCR is lower than its value in DPRP. This is because the proposed scheme outperforms the existing scheme.

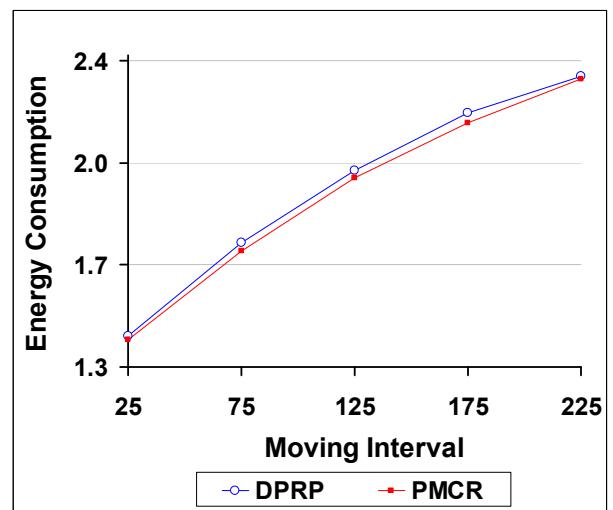


Figure11. Energy consumption vs moving interval

As shown, when the two cache replacement schemes are compared, the PMCR has a better performance when the moving interval is changed.

3) Effect of Changing the Cache Size

This subsection investigates the performance of the proposed replacement scheme when the cache size is varied. In this set of experiments, the cache size was varied from 5% to 15%. Table 4 gives the default parameters for changing cache size.

TABLE 4. THE DEFAULT PARAMETER FOR CHANGING CACHE SIZE

Query Interval (QI)	Moving Interval (MI)	Number of Queries	Number of clients
25 s	50 s	200	5

Figure 12 depicts the performance results of the cache size versus the cache hit ratio. As shown in Figure 12, as the cache size increases, the cache hit ratio increases. This is because; the cache can hold a large number of data items. Consequently, the cached data are likely to be re-used for subsequent queries which increase the probability of getting a cache hit. This leads to, with query interval, MI and number of query invariant, an increased performance of cache hit ratio with the increase in cache size. Also, the cache hit ratio of PMCR is higher than its value in DPRP. This is because the proposed scheme outperforms the existing scheme.

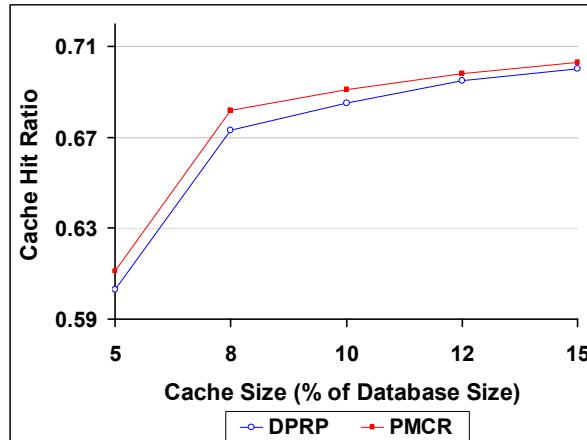


Figure12. Cache hit ratio vs cache size

Figure 13 depicts the performance results of the cache size versus the access time. As shown in Figure 13, as the cache size increases, the access time decreases. This is because, the cache can hold large number of data items. Consequently, the cached data are likely to be re-used for subsequent queries. This leads to, with query interval, MI and number of query invariant, the access time decreases as the cache size increases. Also, access time of PMCR is lower than its value in DPRP. This is because the proposed scheme outperforms the existing scheme.

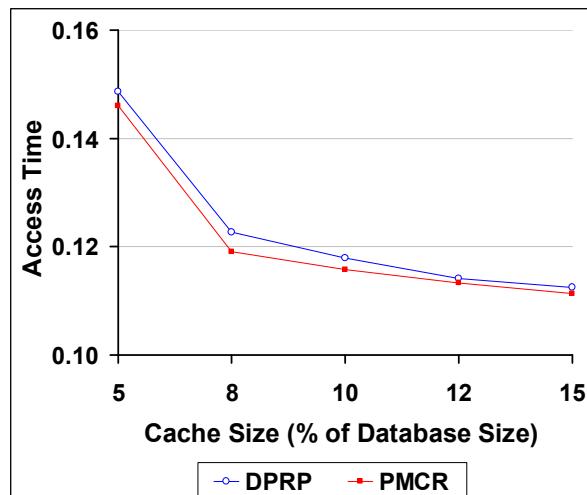


Figure13. Access time vs cache size

Figure 14 depicts the performance results of the cache size versus the energy consumption. As shown in Figure 14, as the cache size increases, the energy consumption decreases. This is because; the cache can hold large number of data items. Consequently, the cached data are likely to be re-used for subsequent queries. This leads to, with query interval, MI and number of query invariant, the energy consumption decreases as the cache size increases. Also, the energy consumption of PMCR is lower than its value in DPRP. This is because the proposed scheme outperforms the existing scheme.

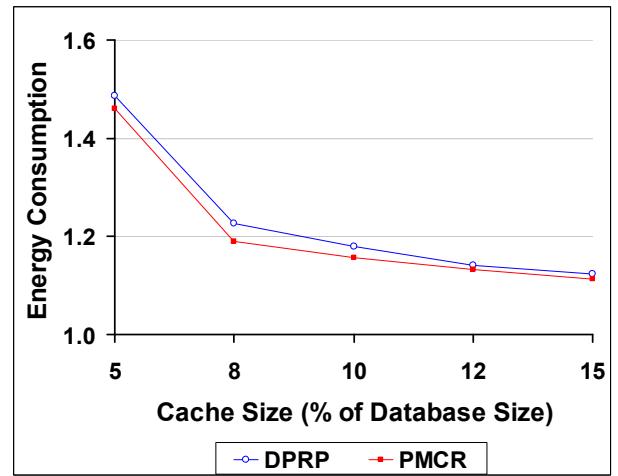


Figure14. Energy consumption vs cache size

As shown, when the two cache replacement scheme are compared, the PMCR has a better performance when the the cache size is changed.

4) Effect of Changing the Number of Queries

This subsection investigates the performance of the proposed replacement scheme when the number of queries is varied. In this set of experiments, the number of queries was varied from 100 to 250. Table 5 gives the default parameters for changing the number of queries.

TABLE 5. THE DEFAULT PARAMETER FOR CHANGING NUMBER OF QUERIES

Moving Interval (MI)	Query Interval (QI)	Cache Size	Number of clients
50 s	25 s	5%	5

Figure 15 depicts the performance results of the number of queries versus the cache hit ratio. As shown in Figure 15, as the number of queries increases, the cache hit ratio increases. This is because, with MI and QI invariant, there is a high probability of the client would make more two queries one valid region, thus the cached data are likely to be re-used for subsequent queries which increase the probability of getting a cache hit. This leads, with the total number of queries is increased, to an increased performance of cache hit ratio with the increase in number of queries. Also, the cache hit ratio of PMCR is higher than its value in DPRP. This is because the proposed scheme outperforms the existing scheme.

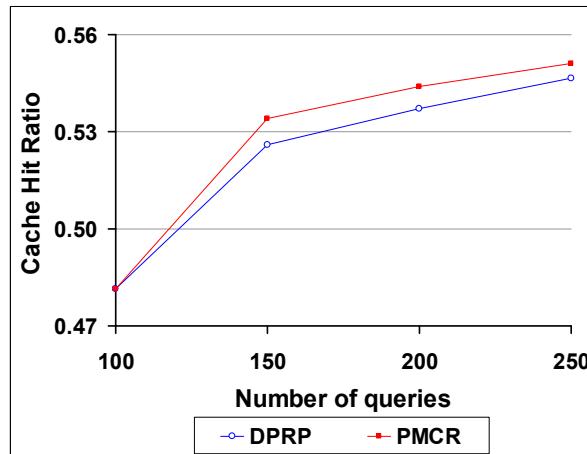


Figure15. Cache hit ratio vs number of queries

Figure 16 depicts the performance results of number of queries versus the access time. As shown in Figure 16, as the number of queries increases, the access time increases. This is because, with MI and QI invariant, there is a high probability that the client would make more two successive queries on the valid region, thus the cached data are likely to be re-used for subsequent queries. This leads to the access time decreased as the number of queries increased, but the total number of queries is increased with MI,QI and cache size invariant. For all these reasons, the access time increased as the number of queries increased. Also, access time of PMCR is lower than its value in DPRP. This is because the proposed scheme outperforms the existing scheme.

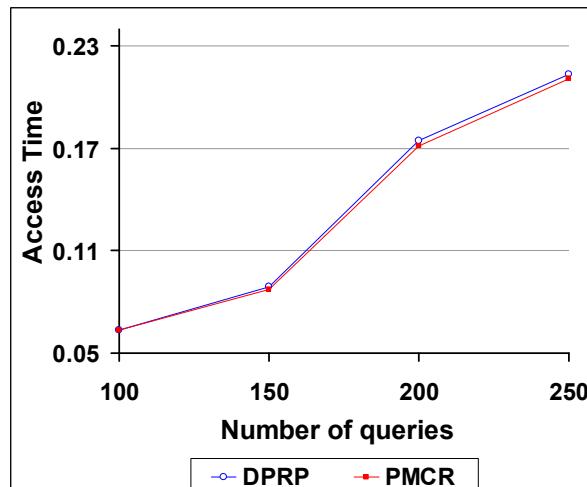


Figure16. Access time vs number of queries

Figure 17 depicts the performance results of number of queries versus the energy consumption. As shown in Figure 17, as the number of queries increases, the energy consumption increases too. This is because, with MI and QI invariant, there is a high probability that the client would make more two successive queries on the valid

region, thus the cached data are likely to be re-used for subsequent queries. This leads to the energy consumption decreases as the number of queries increases, but the total number of queries is increased with MI, QI and cache size invariant. For all these reasons, the energy consumption increases as the number of queries increases. Also, the energy consumption of PMCR is lower than its value in DPRP. This is because the proposed scheme outperforms the existing scheme.

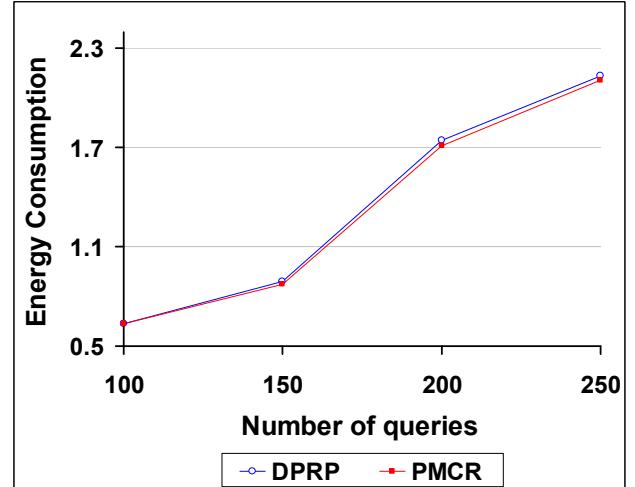


Figure17. Energy consumption vs number of queries

As shown, when the two cache replacement scheme are compared, the PMCR has a better performance when the number of queries is changed.

5) Effect of Changing the the Number of Clients

This subsection investigates the performance of the proposed replacement scheme when the number of clients is varied. In this set of experiments, the number of clients was varied from 5 to 20 clients. Table 6 gives the default parameters for changing the number of clients.

TABLE6. THE DEFAULT PARAMETER FOR CHANGING NUMBER OF CLIENTS.

Query Interval (QI)	Moving Interval (MI)	Cache Size	Number of Queries
25 s	50 s	5%	200

Figure 18 depicts the performance results of the number of clients versus the cache hit ratio. As shown in Figure 18, as number of clients increases, the cache hit ratio decreases. This is because, with increase the number of clients, there is a high probability of the client less likely to be re-used the cached data. This leads to, with QI, MI, number of queries and cache size invariant, a decreased performance of cache hit ratio with increase in number of clients. Also, the cache hit ratio of PMCR is higher than its value in DPRP. This is because the proposed scheme outperforms the existing scheme.

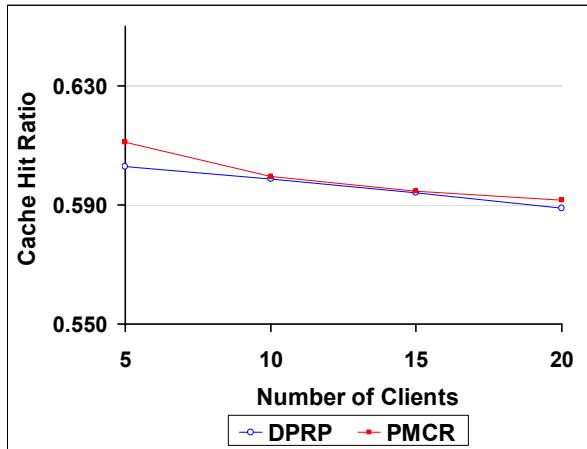


Figure18. Cache hit ratio vs number of clients

Figure 19 depicts the performance results of number of clients versus the access time. As shown in Figure 19, as the number of clients increases, the access time increase. This is because, with increase the number of clients, there is a high probability of the client less likely to be re-used the cached data. This leads to, with QI, MI, number of queries and cache size invariant, the access time is likely to be increased as the number of clients increases. Also, access time of PMCR is lower than its value in DPRP. This is because the proposed scheme outperform the existing scheme.

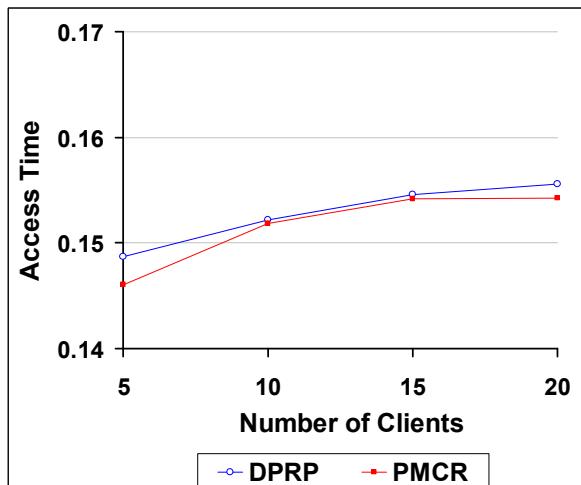


Figure19. Access time vs number of clients

Figure 20 depicts the performance results of number of queries versus the energy consumption. As shown in Figure 20, as the number of clients increases, the energy consumption increase. This is because, with increase the number of clients, there is a high probability of the client less likely to be re-used the cached data. This leads to, with QI, MI, number of queries and cache size invariant, the energy consumption is likely to be increased as the number of clients increases. Also, energy consumption of PMCR is lower than its value in DPRP. This is because the proposed scheme outperforms the existing scheme.

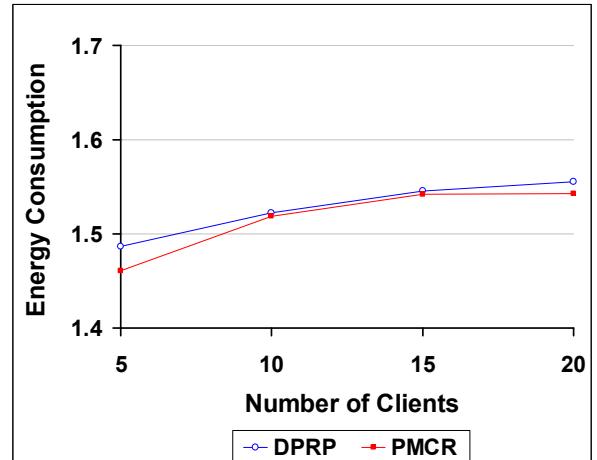


Figure20. Energy consumption vs number of clients

As shown, when the two cache replacement schemes are compared, the PMCR has a better performance when the number of clients is changed from a small to a large number of clients.

VI. CONCLUSION AND FURTHER WORK

In this paper, a predictable markov based cache replacement called PMCR for Mobile Environments is introduced. PMCR is based on Markov Model and cost function for selecting data items to be replaced from the cache. PMCR uses the root-mean squared distance as a radius of the predicted region. In addition, PMCR uses the cost function that considers access probability, data distance, valid scope area and the data size in the cache and the weight of visiting each location whose data is cached by Markov Model in replacement decision. A number of simulation experiments have been introduced to evaluate the performance of the PMCR. The simulation results demonstrate that PMCR, with different system settings, gives better performance in comparison with DPRP. In the further work, we are planning to study the cache invalidation and incorporate it with the cache replacement issues.

REFERENCES

- [1] Zheng, B., Xu, J., and Lee, D. L. 2002. Cache invalidation and replacement strategies for location-dependent data in mobile environments. *Computers, IEEE Transactions on*, 51(10), 1141-1153.
- [2] Chavan, H., Sane, S., and Kekre, H. B. 2011. A Markov Model Based Cache Replacement Policy for Mobile Environment. In *Technology Systems and Management* (pp. 18-26). Springer Berlin Heidelberg.
- [3] Xu, J., Zheng, B., Zhu, M., and Lee, D. L. 2002. Research challenges in information access and dissemination in a mobile environment. In *Proceedings of the Pan-Yellow-Sea International Workshop on Information Technologies for Network Era*, 1-8.
- [4] Tabassum, K., Sved, M. O., and Damodaram, A. 2011. Enhanced-Location-Dependent Caching and Replacement Strategies in Mobile Environment. *IJCSI Issues*, 8(4).

- [5] Drakatos, S., Pissinou, N., Makki, K., and Douligeris, C. 2006. A future location-prediction replacement strategy for mobile computing environments. In Wireless Communications and Networking Conference, 2006. WCNC 2006. IEEE (Vol. 4, pp. 2252-2260). IEEE.
- [6] Tabassum, K., Hijab, M., and Damodaram, A. 2010. A data mining approach for Cache Replacement in Location-dependent Environment. In Computer Research and Development, 2010 Second International Conference on (pp. 126-130). IEEE.
- [7] Katsaros, D., Nanopoulos, A., and Manolopoulos, Y. (Eds.). 2005. Wireless Information Highways. IGI Global.
- [8] Chavan, H., and Sane, S. 2011. Mobile Database Cache Replacement Policies: LRU and PRRP. In Advances in Computer Science and Information Technology (pp. 523-531). Springer Berlin Heidelberg.
- [9] Kumar, A., Misra, M., and Sarje, A. K. 2006. A New Cost Function based Cache Replacement Policy for Location Dependent Data in Mobile Environment. In The 5th Annual Inter. Research Institute Student Seminar In Computer Science, Iriss.
- [10] Kumar, A., Misra, M., and Sarje, A. K. 2008. A predicted region based cache replacement policy for location dependent data in mobile environment. International Journal of Communications, Network and System Sciences, 1(1), 79-94.
- [11] Joy, P. T., and Jacob, K. P. 2012. A Comparative Study of Cache Replacement Policies in Wireless Mobile Networks. In Advances in Computing and Information Technology (pp. 609-619). Springer Berlin Heidelberg.
- [12] Dar, S., Franklin, M. J., Jonsson, B. T., Srivastava, D., and Tan, M. 1996. Semantic data caching and replacement. In VLDB, 96, 330-341.
- [13] Ren, Q., and Dunham, M. H. 2000. Using semantic caching to manage location dependent data in mobile computing. In Proceedings of the 6th annual international conference on Mobile computing and networking (pp. 210-221). ACM.
- [14] Lai, K. Y., Tari, Z., and Bertok, P. 2004. Mobility-aware cache replacement for users of location-dependent services. In Local Computer Networks. 2004. 29th Annual IEEE International Conference on (pp. 50-58). IEEE.
- [15] ElDahshan, K.A., Gad-EIRab, A.A. and Sobhi, A., 2015. A Distance-based Predicted Region Policy for Cache Replacement in Mobile Environments. International Journal of Computer Applications. 126.
- [16] Chavan, H., Sane, S. and Kekre, H., 2012. A Markov-Graph Cache Replacement Policy for mobile environment, Communication, Information & Computing Technology (ICCICT), 2012 International Conference on. IEEE, pp. 1-6.
- [17] "Wikipedia," 2016. [Online]. Available at: https://en.wikipedia.org/wiki/feature_scaling. [Accessed: 1-Jan-2016].
- [18] "Normalization by Scaling Between 0 and 1". 2016. [Online]. Available: https://docs.tibco.com/pub/spotfire/5.5.0-march-2013/UsersGuide/norm/norm_scale_between_0_and_1.htm. [Accessed: 1-Jan-2016].
- [19] Dunham, M. H., and Helal, A. 1995. Mobile computing and databases: Anything new?. Acm Sigmod Record, 24(4), 5-9.
- [20] Lee, D. L., Lee, W. C., Xu, J., and Zheng, B. 2002. Data management in location-dependent information services: Challenges and issues. IEEE Pervasive computing, 3(3), 65-72.
- [21] Varea, A.. 2013. The Omnet++ discrete event simulation system. Version 4.3. User Manual. URL: <http://www.omnetpp.org>

AUTHORS PROFILE

Ahmed. A. A. Gad-EIRab is an assistant professor of Computer Science at Mathematics and Computer Science Department, Al-Azhar University in Cairo, Egypt. He had B.Sc degree in Computer Science from faculty of Science, Alexandria University, Egypt, M.Sc degree in Computer Science from faculty of Science, Cairo University, M.Sc, Egypt, and PhD degree in Engineering and Computer Science from Graduate School of Information Science, Nara Institute of Science and Technology, Japan. Also, he had postdoctoral scholarship researcher at Nara Institute of Science and technology, Japan from March 2015 to September 2015. He got many awards during his research. The first award is the best paper award in The 55th Mobile Computing and Ubiquities communications Workshop (MBL55), Japan, 2010. The second award is the IPSJ Yamashita SIG Research Award from Information Processing Society of Japan, 2010. The third award is the Best PhD Student Award from Nara Institute of Science and Technology, March 2012, Japan. The last award is the Outperformance Award from Graduate School of Information Science, Nara Institute of Science and Technology, March 2012, Japan. His interested research topic are Ubiquitous and pervasive computing, Mobile computing, Wireless sensor networks, parallel and distributed systems, cloud computing, mobile cloud computing, context aware systems, smart home systems.

Kamal Abdelraouf ElDahshan is a professor of Computer Science and Information Systems at Al-Azhar University in Cairo, Egypt. An Egyptian national and graduate of Cairo University, he obtained his doctoral degree from the Universit de Technologie de Compigne in France, where he also taught for several years. During his extended stay in France, he also worked at the prestigious Institute National de Tlcommunications in Paris. Professor ElDahshan's extensive international research, teaching, and consulting experiences have spanned four continents and include academic institutions as well as government and private organizations. He taught at Virginia Tech as a visiting professor; he was a Consultant to the Egyptian Cabinet Information and Decision Support Center (IDSC); and he was a senior advisor to the Ministry of Education and Deputy Director of the National Technology Development Center. Prof. ElDahshan has taught graduate and undergraduate courses in information resources and centers, information systems, systems analysis and design, and expert systems. Professor ElDahshan is a professional Fellow on Open Educational Resources as recognized by the United States Department of State. Prof. Eldahshan wants to work in collaboration with the Ministry of Education to develop educational material for K-12 levels. Prof. Eldahshan is interested in training instructors to be able to use OER in their teaching and hopes to make his university a center of excellence in OER and offer services to other universities in the country.

Ahmed Sobhi graduated with a B.Sc. in mathematics and computer Science from faculty of Science, Al-Azhar University, Egypt, Master of computer science from faculty of Science, Menoufia University, Egypt. Now he is a P.hD student in computer Science at faculty of Science, Al-Azhar University, Egypt.

Developing an Intelligent System for Crowd Density Estimation

Dr. Ali Salem Ali Bin-Sama¹

Department of Engineering Geology,
Oil & Minerals Faculty, Aden University,
Aden, Yemen

Dr. Salem Saleh Ahmed Alamri²

Department of Engineering Geology,
Oil & Minerals Faculty, Aden University,
Aden, Yemen

Abstract— Crowd density estimation models are important for monitoring people behaviors in a crowd. In this paper a development of an intelligent system is introduced to achieve the goal of density estimation. Mainly, the proposed system consist of Gabor features texture pattern extraction and convolutional neural network for pattern classification. To assess the performance of the developed, a number of public benchmark images are used such as LIBRARY Dataset, QUT Dataset, and Fudan Pedestrian Dataset.

Keyword: Crowd Density Estimation, Gabor filters, Convolutional neural network, Texture Image.

I. INTRODUCTION

Crowd size estimation is an important task for both operational and security purposes. Therefore, studying crowd phenomenon is becoming of great interest mainly with the increasing number of popular events that gather many people such as in Hajj at Makah, religious festivals, markets, subways, public demonstrations, sport events, and high density moving objects like car traffic. Therefore, crowd analysis has emerged as a major topic for crowd monitoring and management in visual surveillance field. In particular, the estimation of crowd density is receiving much attention for safety control.

Furthermore, it could be used for developing crowd management strategies by measuring the comfort level in public spaces. Also, its automatic monitoring is extremely important to prevent disasters by detecting potential risk and preventing over crowd. To prevent such deadly accidents, early detection of unusual situations in large scale crowd is required and appropriate decisions for safety control have to be taken to insure assistance and emergency contingency plan.

II. LITERATURE REVIEW

In the literature, many techniques have been developed for estimating crowd density problem. For more accurate foreground detection by represent complicated random motion patterns (like turning around, wandering about, and turning heads), a novel accumulated mosaic image difference feature (AMID) approach in [1] have been proposed. Furthermore, for describing a random tiny motions happening in stable crowds and found to be one of the inherent characteristics of high-density crowds, a new notion which is intra-crowd motions also in [1] have been proposed. Then for achieving accurate

crowd density estimation, the AMID feature has been used in order to represent these local intra-crowd motion patterns effectively. In their work, normalization process was applied on the obtained foreground based on the perspective distortion correction model. This model was used to estimate crowd density for observed areas.

For counting moving pedestrians in a scene, a more robust real time method in [2] has been proposed. Their system is much faster, simpler in implementation and does not require a complex setup procedure compared to [3]. Furthermore, in order to deal with the perspective distortion, this method has been subdivided the entire scene into smaller horizontal zones. Moreover, each zone has a special size depending on its distance weights from the camera. The results of people counting separately carried out for each zone and summed up at the end. In addition, density based clustering is used by applying shape technique which is more reliable to extract the shape of a set of points than the bounding box has been proposed in [3].

Based on feature points, a crowd flow tracking and counting method in [4] has been presented. Moreover, by employing a three-frame difference algorithm, this approach has been improved SURF point detecting process. Furthermore, for detecting the SURF feature points that really belong to the moving crowd and also for reducing the time complexity, the binary image of moving foreground as a mask image has been exploited. Then, for more enhancement and only clustering the motion feature points, the Density Based Spatial Clustering of Application with Noise (DBSCAN) clustering algorithm has been improved. Finally, for estimating the moving orientation and count the crowds, a Lucas Kanade local optical flow with Hessian matrix method with a support vector regression machine has been used.

For capturing the crowd properties, the algorithms that rely on holistic, local or histogram based features have been used. Then, for estimating the crowd size, the regression has been employed. Furthermore, for comparing the holistic, local and histogram based methods and to compare various image features and regression models, an evaluation across multiple datasets in [5] have been presented. For counting crowds directly, local feature mining in [6] has been used. Therefore, from equally sized cells in a rectangular grid, the Features have been extracted. Furthermore, for capturing both global and local trends in the image, the multiple output ridge

regression has been used. For representing the foreground humans from a training dataset, an example-based approach in [7], by constructing a mixture model of Bernoulli shapes has been proposed.

Gall and Lempitsky in [8] have been presented a Hough forest framework as a more general formulation which can be applied for tracking and action recognition beside object detection. Furthermore, this method has been showed as a robust to partial occlusions and a typical part appearances. Human region detector is used to filter parts of human like heads. Furthermore, for detecting true-foreground, which is counting only human-classified pixels rather than foreground pixels, pixel-based crowd counting system with a robust selective background model in [9] have been presented. Moreover, the system can reduce the loss of people by using a more robust people counting based classifier when they get absorbed into the background after beings low or stationary.

III. THE MODEL FOR CROWD DENSITY ESTIMATION

In general, for crowd estimation in public places such as train station and the square, a procedure Crowd Density Estimation has been utilized. Moreover, in these places, from the video, people always overlap when it is crowded and sometimes only their heads protrude. Therefore, the method to estimate crowd density by analyzing the individuals to count their numbers is out of the ability [10]. Furthermore, through years of researches, a general procedure of crowd estimation has been established. There are two steps of crowd density estimation. The first step is to find out an effective way to extract crowd features of different density levels and the second step is to discriminate these features with a classification model. According to the observation that textures are becoming more distinctive with the growing of crowd, texture analysis [11] has been chosen many times and shows good performance. So, in this paper, texture is also used by the Gabor wavelet.

The main steps of the proposed system methodology are

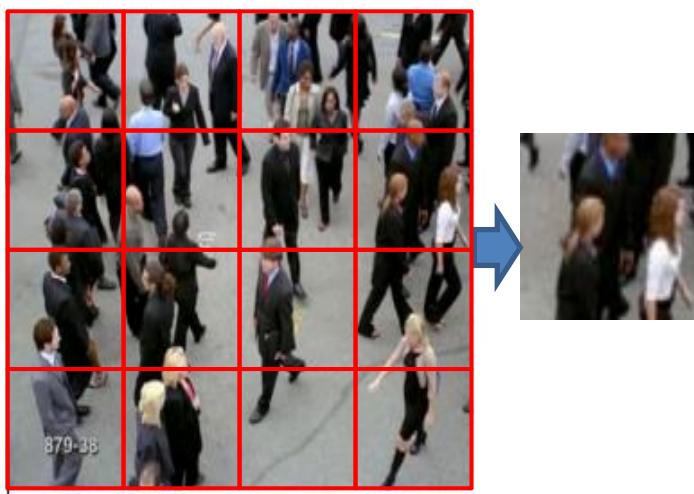


Fig. (1) The proposed crowd density estimation system

shown in Figure 1. Mainly, the proposed system consists of two stages i.e. texture feature extraction stage and pattern classification stage. The detail of each stage is explained as follows:

A. Texture feature extraction

In this paper, Gabor wavelet as a texture feature extraction technique is employed. Generally, Gabor features are computed by the convolution process of the input image with Gabor filters. Then, the feature vector computed as the mean and standard deviation of the magnitude value for each filter as shown in Figure 2.

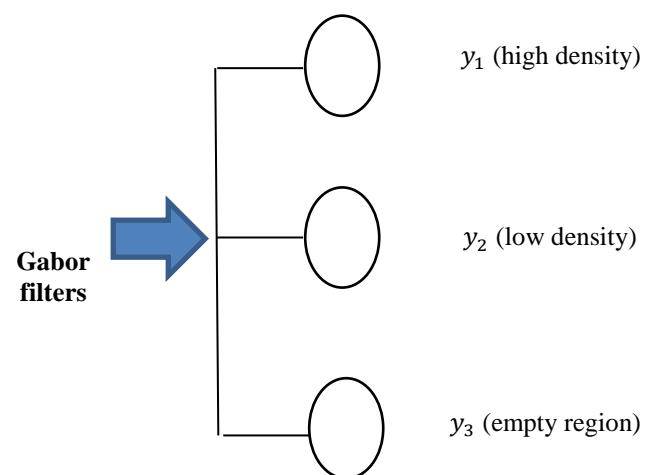
B. Gabor wavelet features

The aim of preprocessing step is to highlight license plate edges at different ordinations and scales. In this study we adopt Gabor filters to do preprocessing operation for input test image. Therefore, for different types of images, a Gabor filters have been successfully employed. The main idea of Gabor filters is to generate a bank of filters at different scales and orientations using the following formula:

$$G(x, y) = \left(\frac{1}{2\pi\sigma_x\sigma_y} \right) \exp \left(-\frac{1}{2} \left(\frac{x^2}{\sigma_x^2} + \frac{y^2}{\sigma_y^2} \right) \right) \exp(2\pi j W(x \cos \theta + y \sin \theta)) \quad (1)$$

Where W variable is the radial frequency of the Gabor filter and its value lie in $W \in [0, 0.5]$. The second variable of Gabor filters is the orientation variable θ which controls the angle of the filter and its value lie in $\theta \in [0, \pi]$. Finally, the scale variable σ controls the shape of the Gaussian function and its value within $\sigma \in [0, 2\pi]$.

In this work, a total of 40 Gabor filters are used for the preprocessing stage. Those filters are generated at eight orientations $(0, \frac{\pi}{4}, \frac{\pi}{2}, \frac{3\pi}{4}, \pi, \frac{5\pi}{4}, \frac{3\pi}{2}, \frac{7\pi}{4})$, and five scales $(0, \frac{\pi}{4}, \frac{\pi}{2}, \pi, \frac{3\pi}{4})$ as in Fig 3. We consider the filter size to be a small (8×8) in order to be able to localize low level edges.



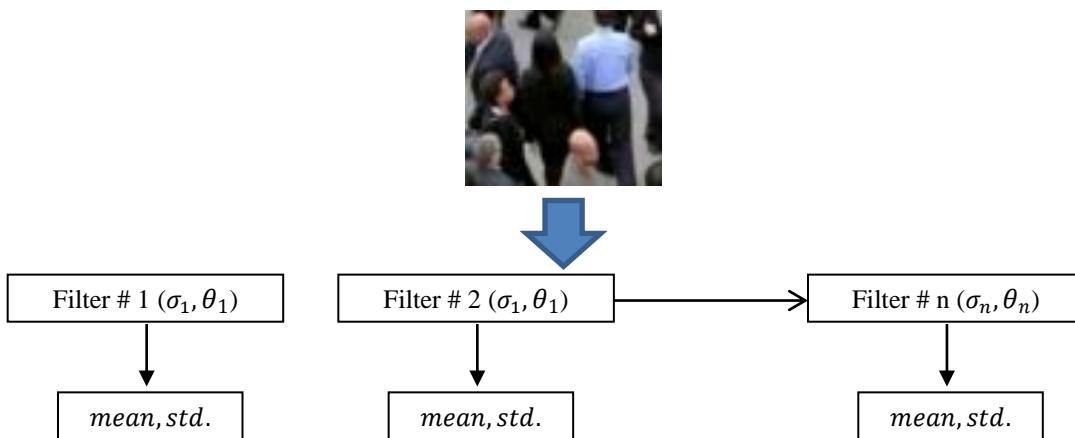


Fig. (2) Gabor wavelet feature vector

C. Neural Network Classifier for Pattern Recognition

Pattern recognition is a branch of machine learning that focuses on the recognition of patterns and regularities in data, although it is in some cases considered to be nearly synonymous with machine learning. Pattern recognition systems are in many cases trained from labeled "training" data (supervised learning), but when no labeled data are available other algorithms can be used to discover previously unknown patterns (unsupervised learning). Neural Network (NN), also known as Artificial Neural Network (ANN) is a collection of computing cells (artificial neurons) interconnected through weighted links [12]. ANN can be classified by their learning methods: supervised learning and unsupervised learning.

Generally, the neural network is a mechanism for machine learning which is constituted of an input layer, multiple hide layers and an output layer. Each layer is made up by several neuron nodes and the output of one node from the layer in the front connects to the input of anode from the layer in the next. Each connection carries a weight which indicates the influence of one node to another. Generally, the nodes in the front layers are full connected, which is known as full connection, to every node in the next layer. With the desired outputs, the network can learn the optimal solution of a special problem by adjusting the weights of connections [13]. In this paper, a hybrid of Gabor wavelet filters and neural network has been applied, which brings us the benefits of feature learning.

D. People counting using neural network

In our case, we have chosen BP neural network because of its excellence in prediction. BP neural network, a multilayer neural network which must include at least one hidden layer, is one of the most widely used models among ANNs. It is actually a feed-forward neural network trained with back propagation algorithms. The neural network has three layers: input layer, hidden layer, and output layer. In this crowd density estimation module, we want to predict the number of people (output) from the number of pixels (input). The number of people is then used to calculate the crowd density and classify the crowd based on distinct level of services.

E. Density calculation and classification

Many methods exist to estimate crowd density either using real time video or images. Crowd density can be presented in the form of an exact number of people per unit square, crowding percentage levels or density classes. Our system calculates crowd density after the number of people is successfully predicted by the neural network. A basic equation to estimate crowd density as shown in equation (2). This equation divides the number of people obtained from the BP neural network by the area of selected unit square. Crowd density is then classified based on three distinct groups shown in Table 2, according to the five levels of service as defined by Polus et al. (1983). Each level of service is defined based on the range of average area occupancy (the area of free expanse available) for a single pedestrian (Polus et al., 1983). The five density groups are very low, low, moderate, high, and very high. Since users are given the flexibility to select the ROI, we classify crowd density based on the range of density.

$$\text{Crowd density} = \text{Number of people} / \text{Area regain of unit square} \quad (2)$$

IV. EXPERIMENTS AND COMPARISONS

As there is no standard data set for crowd density estimation [14], the approach is tested on two data sets: PETS Dataset, and Fudan Pedestrian Dataset. The experimental results are described in below to demonstrate the validity of the improvements in crowd density estimation.

A. Data Sets

PETS dataset sequences from the Performance Evaluation in Tracking for Surveillance (PETS) Workshop 2001, 2 different cameras of an outdoor campus scene, high quality (from digital camera), with resolution (358,288) 30fps, stored as avis with no compression. The data from PETS01 was originally of higher resolution and stored as JPEG images.

Fudan pedestrian dataset contains 1500 ground-truth images, foreground masks and images, feature data of Matlab files, labels. In each feature data file, there is a 300*129 matrix,

300 is the number of samples, 129 is the dimension of the feature, which is set under the order of (Area(1), Perimeter(1), Edge(1), Minkowski(1), Ratio(1), SLF feature(124), digit means the dimension of each set of feature.

B. The Estimation of Crowd Density

The density estimation experiments mainly include training and testing. The experimental images are taken from Fudan pedestrian dataset and PETS datasets. Then the sequence square window are obtained by extracting the square window from the crowd images. The square window size is 20×20 . According to different crowd density, the experimental images are classified into low density, medium density and high density. Some crowd images of different density are shown in Fig.3. Totally 300 images are selected, including 100 images of low, medium and high density, respectively. We select 50 images for different density, totally 150 images. Having extracted the texture feature values of the foreground object, we train the artificial neural network and obtain the training parameters, then begin to test. Numerical experiments have been conducted on MATLAB7.0 (the computer's CPU is Intel Core i5, 2.8GHz, 4GB RAM).

In scenes of low, medium, and high density crowd, we extract means and standers deviations features generated by Gabor wavelet filter in the horizontal and vertical directions and constitute them into 11-dimensional, which is input into

artificial neural network classifiers. We obtain artificial neural network model by training samples.

VII. CONCLUSION

In summary, we have presented an approach of using the Gabor wavelet algorithm and Artificial Neural Network (ANN) for crowd density estimation in the sequences images from two databases. In the initial stage, the input images are reprocessed and the texture feature by using Gabor wavelet is extracted. Then, Gabor features are computed by the convolution process of the input image with Gabor filters. Also, the feature vector computed as the mean and standard deviation of the magnitude value for each filter. After that, the feature vectors are fed into the training system for solving the crowd density estimation problem. Besides this, the Artificial Neural Network is used for the classification in PETS and Fudan pedestrian databases. The low computational complexity enables our approach possible for estimating crowd density. Experimental results demonstrate the effectiveness of our method. Nevertheless, there is a lot of scope for improvement in our approach. In our future work we would like to reduce the false estimations, incorporate additional methods to reason out occlusions in a crowded scene and make the ANN approach more stable.



Fig. (3). The example of different crowd density level (a) low, (b) medium, (c) high

REFERENCES

- [1] Zhang, Z., Li, M., Crowd density estimation based on statistical analysis of local intra-crowd motions for public area surveillance. Opt. Eng. (2012), 51 (4) 047204-1.
- [2] Conte, D., Foggia, P., Percannella, G., Vento, M., 2013. Counting moving persons in crowded scenes. Mach. Vis. Appl. 24(5), 1029–1042.
- [3] Conte, D., Foggia, P., Percannella, G., Tufano, F., Vento, M., 2010a. A method for counting people in crowded scenes. In: 2010 Seventh IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS). IEEE, pp. 225–232, URL <http://doi.ieeecomputersociety.org/10.1109/AVSS.2010.86>.
- [4] Liang, R., Zhu, Y., Wang, H., 2014. Counting crowd flow based on feature points. Neuro computing 133, 377–384.
- [5] Ryan David, Simon Denman, Sridha Sridharan, Clinton Fookes, An evaluation of crowd counting methods, features and regression models, Elsevier, Computer Vision and Image Understanding 130 (2015) 1–17
- [6] Chen Ke, Chen Change Loy, Shaogang Gong, Tony Xiang. Feature mining for localised crowd counting, British Machine Vision Association, 2012, pp. 21.121.11. <http://www.eecs.qmul.ac.uk/_ccloy/downloads_mall_dataset.html>.
- [7] Ge Weina, Robert T. Collins, R. Barry Ruback, Vision-based analysis of small groups in pedestrian crowds, IEEE Trans. Pattern Anal. Mach. Intell. 34 (5) (2012) 1003–1016.
- [8] Gall, J., Lempitsky, V., 2013. Class-specific hough forests for object detection. In: Decision Forests for Computer Vision and Medical Image Analysis. Springer, pp. 143–157.
- [9] Choudri, S., Ferryman, J. M., Badii, A., 2009. Robust background model for pixel based people counting using a single uncalibrated camera. In: 2009 Twelfth IEEE International Workshop on Performance Evaluation of Tracking and Surveillance (PETS-Winter). IEEE, pp. 1–8, <http://dx.doi.org/10.1109/PETS-WIN.2009.5399531>.
- [10] Davies, A.C., Yin, J.H., Velastin, S.A., 1995. Crowd monitoring using image processing. Electronics & Communication Engineering Journal 7 (1).
- [11] Ma, R., Li, L., Huang, W., Tian, Q., 2004. On pixel count based crowd density estimation for visual surveillance. In: IEEE Conference on Cybernetics and Intelligent Systems, 1–3 December 2004, pp. 170–173.
- [12] Ghosh, J., Bovik, A.C., 1991. Neural networks for textured image processing. In: I.K. Sethi, A.K. Jain (Eds.), Progress in Artificial Neural Networks and Statistical Pattern Recognition. North-Holland, pp. 133–154.
- [13] Kim, G. A., TaekiKim, Moonhyun, 2012. Estimation of crowd density in public areas based on neural network. KSII Trans. Internet Inf. Syst. 6(9), 2 170–2190.
- [14] Zhou, B., Zhang, F., Peng, L., 2012. Higher-order SVD analysis for crowd density estimation. Comput. Vis. Image Understand. 116 (9), 1014–1021.

AUTORS PROFILE



1 Dr. Ali Salem Ali Bin Sama: Received the B.E degree in Computer Engineering, Balqa University, Faculty of Applied Engineering, Jordan, 1997, M.Sc. degree in Computer science from University of Science, Malaysia, 2006, PhD degree in computer Science, Malaysia, 2011, He has 11 international papers, 5 international conferences ,He is assist. professor of department of engineering geology in Minerals & Oil Faculty, Aden University, Yemen, Assistant Professor in a Department of Computer Science and Information, College of Sharia and Islamic Studies at Al-Ahsa, Imam Muhammad bin Saud Islamic University, in Saudi Arabia, From 25/08/2014 until now.



2 Dr. Salem Saleh Ahmed Alamri: Received the B.E degree in Mechanical Engineering, University of Aden, Yemen, 1991, M.Sc. degree Computer science (IT) from North Maharashtra University (N.M.U), India, Jalgaon, 2006, PhD degree in computer science (S.R.T.M.U), India, Nanded., 2011. He has 12 international papers, 8 international conferences. assist professor HOD of department of engineering geology in Minerals & Oil Faculty, Aden University, Yemen; He is membership in International Association of Engineers (IAENG)

A Security Scheme for Providing AIC Triad in Mobile Cloud Computing

Isra Sitan Al-Qasrawi

Department of Information Technology

Al-Balqa' Applied University, AL-Huson University College
Irbid, Jordan

Abstract—As mobile devices like smart phones and tablets continue to grow, the requirement of cloud computing in mobile devices continue to grow too, and becomes an important service to provide users the ability to manage files and data remotely, which gave birth of Mobile Cloud Computing (MCC). As a result, new web-based threats and attacks will continue to increase in number. The most important issues must be covered to provide users reliable and secure services of mobile cloud computing are: Availability, Integrity, and Confidentiality. In this paper, (i) the concepts of cloud computing and mobile computing are discussed, the challenges that face each one of them, the meaning of mobile cloud computing, the challenges of MCC. (ii) Different mechanisms to store data in secure manner are explored. (iii) Propose a new scheme to secure the data storage in Mobile Cloud Computing without exposing the data content to the cloud service providers to protect mobile users' privacy. This scheme provides the security AIC triad concepts (Availability, Integrity, and Confidentiality) for data by applying a number of operations.

Keywords-cloud computing; mobile computing; mobile cloud computing; security; data storage; mobile user.

I. INTRODUCTION

Using services over the Internet, to store files and personal information or share files to others, or using different applications at another location, are examples of using "Cloud Computing" service. "Cloud computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the datacenters that provide those services" [1].

Cloud computing provides access to computer resources from different locations where a connection is available, to provide different services to users such as: social media sites, or online file storage, or at least attaching files via E-mail. The main idea of cloud computing is to make storage and processing on data in other devices, which will not lead to need more storage devices and will not lead to increase overhead on user device's processor. Cloud computing reduces the cost and complexity of owning and operating computers and networks. Some benefits of cloud computing for users are: reliability, efficiency, scalability, flexibility of use, customization, and rapid deployment.

While Mobile Computing offers mobility with computing power to provide the ability of using the technology to wirelessly use and connect to data or information by portable devices, which will facilitate a large number of applications on a single device. Smartphone is one of the most used mobile devices as it is being used personally all over the world with the rapidly growing of wireless network technology.

The combination of mobile computing and cloud computing is a technology of "Mobile Cloud Computing" (MCC), where having the benefits of Ubiquity in mobile computing, and efficiency in cloud computing.

The Mobile Cloud Computing Forum defines MCC as follows [2]: "Mobile Cloud Computing at its simplest, refers to an infrastructure where both the data storage and the data processing happen outside of the mobile device. Mobile cloud applications move the computing power and data storage away from mobile phones and into the cloud, bringing applications and mobile computing to not just Smartphone users but a much broader range of mobile subscribers".

mobile cloud computing means to run an application such as mobile weather widgets or Twitter for mobile , or Google's Gmail for Mobile on a remote server while the user's mobile device acts like a client connecting over to the remote server by internet through wireless network.

As an inheritance of cloud computing, resources in mobile cloud computing are deployed in numerous distributed computers rather than in internal computers or local servers, and are provided to portable devices such as Smart phones, laptops, and tablets.

While mobile cloud computing provides many facilities in using data and applications to our daily lives, it also faces numerous challenges and problems. The adoption of cloud computing is not free from issues, some of the most important challenges are:

- Security and Privacy.
- Service Delivery and Billing.
- Interoperability and Portability.
- Reliability and Availability.

- Performance and Bandwidth Cost [3].

On the other hand, the technology of mobile computing faces many challenges which can be categorized into three major areas as: communication, mobility, and portability. In communication, Wireless networks will continue to have limited bandwidth, while the limitation in mobility area can be displayed as the problems of address migration, location – dependent Information. And finally, the challenge of portability, in short, is the fact about mobile devices that such these devices are small in size, with limited resources in processing and storage [4].

However, the critical point in MCC, is to merge the benefits of cloud computing and the benefits of mobile computing in seamless way to avoid the challenges in each technology. There are many issues in MCC which need to be studied and resolve such as limited resources in mobile devices, where others related to networks like heterogeneity, availability, and bandwidth. But the most important issue in MCC is the security. As many users often use Mobile devices to deal with personal files such as photos, social data, or working information, so it is very important provide security to the data of mobile user which will be stored in mobile cloud.

In this paper we discuss different schemes which have been suggested to secure data storage in MCC, and propose a new scheme to achieve confidentiality and data integrity as these are two of the most important issues in security for different users.

II. RELATED WORK

Mobile cloud computing has emerged in the last few years and become a focus of research, security and privacy are the most critical issues in mobile cloud computing applications, and still face some enormous challenges.

A secure framework for processing data in mobile cloud computing was proposed by Anand Surendra Shimpi [5]. This framework stores data in a secured fashion to help in protecting the user's privacy.

Jibitesh Mishra [6] proposed a secure architecture for MCC to integrate mobile applications with the various cloud services. This architecture aims to maintain data integrity and security, and improves the storage and processing of data on mobile devices in a secured manner.

Eugene E. Marinelli [7] developed Hyrax, a platform from Hadoop to support cloud computing on Smart phones. It offers a sane performance in data sharing and tolerates node departure.

A secure data service mechanism provided by Jia et al [8] through Identity based proxy re-encryption. In the proposed mechanism, the researches aim to provide confidentiality and access control for data stored in cloud by using a reliable and trusted way to outsource data security management to mobile cloud. So only authorized users can access the data while unauthorized users will learn nothing. Their proposed encryption scheme based on bilinear pairing, user can encrypt the data through his identity (Id). This kind of encryption is called Identity based encryption.

Itani et al [9] proposed a framework which was energy efficient for mobile devices to assure mobile user's integrity, using incremental cryptography and trusted computing. This framework results in saving 90% of processing energy on the mobile devices when compared to other conventional techniques with more security. It saves energy by the property of the incremental cryptography by updating the result of the algorithm that applied to a certain file to modify it, rather than re-computing it from scratch.

Zhou et al [10] proposed a scheme for data confidentiality and access control by introducing the concepts of Privacy Preserving Cipher text Policy Attribute Based Encryption (PP-CP-ABE) and Attribute Based Data Storage (ABDS) system. Mobile devices can outsource both encryption and decryption processes to Cloud Service Provider (CSP) in secure way through using PP-CP-ABE.

Yang et al [11] provides Provable Data Possession (PDP) scheme of resource constrained mobile devices by using Diffie-Hellman key exchange, Merkle Hash Tree (MHT) and bilinear mapping. This scheme is proposed to provide confidentiality, privacy and integrity of mobile user's data stored on cloud.

III. PROPOSED SCHEME

Mobile cloud computing deals with sensitive data since it deals with data of a mobile user and it can contain confidential information like personal photos or identity information. For this reason the most important issues must be covered to provide users reliable and secure services of mobile cloud computing, are: Availability, Integrity, and Confidentiality.

"Fig. 1" shows the elements of AIC triad (Availability, Integrity, and Confidentiality), which are considered the three most crucial components of security.

Availability is a guarantee of reliable access to data on the cloud by only authorized cloud users. Integrity is the assurance that the information is trustworthy and accurate. It can be indicated by an absence of any alteration in owner's data by another cloud user; it must ensure that the data owner only can modify the original data. Data may be stored in cloud to be used by others, but without making changes in the original copy of file, so determining authentication is very important to protect data.

Confidentiality is a set of rules that limits access to data and files on cloud. While data deployed in cloud, especially public cloud, it may be reached to others, because of the truth that data and services are provided to multiple clients using the same shared infrastructure. For this reason, MCC must make sure that data will be accessed only by the data owner, to assurance privacy.

In this paper we propose a security scheme to store and update user's files and applications on cloud servers, which can be migrated to and from a cloud to a mobile device, by achieving availability, integrity, and confidentiality.



Figure 1. AIC Triad's elements

The new scheme is based on a framework with four entities:

Cloud Service Provider (CSP): storage services provided to users by CSP, also CSP is responsible for managing, operating, and allocating resources in cloud in efficient way.

Trusted Front Party (TFP): TFP acts like front-end processor, TFP links mobile user or data owner with the cloud, where all interacting sessions with mobile users are established by TFP. It is associated with a number of registered mobile users, and it is responsible for generating different keys, authentication files, identity files, and encrypted/decrypted files, also it is responsible for sending data to and from CSP.

Owner of mobile-Data (OD): OD is the mobile user or in general, wireless mobile device which needs to store its data on cloud servers that provided by CSP.

Mobile User (MU): MU is the client who uses the storage services provided by CSP.

"Fig. 2" shows the communications between entities in the new scheme, and includes the following phases:

1) Sending file to TFP phase:

In this phase Owner of mobile-Data (OD) will send the file or data to be stored in cloud servers, to TFP through secure communication channel. It is assumed that mobile users have already registered to TFP.

2) Creating Authentication File (AF) phase:

TFP will generate a message authentication code named (Authentication File) for the file of Owner of mobile-Data (OD) using (kod).

$$AF = (file_{OD}, kod)$$

Furthermore, TFP is responsible for generating three different keys for each mobile user associated with the cloud, and store them in its database:

- Kod: represents the key used to create the Authentication File (AF) from the original data of owner (OD).

- Kmu: represents the key used to create the Identity File (IF) from the data of owner, to send it to the subscribed users who shares data with owner. This key provides the ability to subscribed users to explore data without making changes in them.

- Kenc: represents the key used to create the Encrypted File (EF) to be stored in cloud server, and the Decrypted File to be sent to mobile users.

3) Sending AF to OD phase:

After generating Authentication File (AF), TFP will send it to Owner of mobile-Data (OD), to store it on mobile's local storage. This phase is important to achieve data integrity, while the user that has the Authentication File is the only one who can make updates in that file.

The Authentication File will be small in size, from the fact that it aims just to determine the authorized user who can update the original file. So it can be stored in mobile's storage simply. A copy of Authentication File (AF) will be stored too in TFP's storage unit.

4) Creating Encrypted File phase:

TFP will generate the Encrypted File (EF) from the original file sent by OD using (Kenc).

$$EF = AES(file_{OD}, Kenc)$$

The Encrypted File (EF) is created based on Symmetric Key Encryption using Advanced Encryption Standard (AES), while the same key is used for encryption and decryption processes. In evaluation section, it will be shown why AES is chosen in our scheme.

5) Sending EF to CSP phase:

Encrypted File (EF) of owner's data will be sent to Cloud Service Provider (CSP) by TFP to be stored. The interaction between the owner of data (OD) and CSP is made in indirect way via the intermediate party TFP. This phase emphasizes that cloud servers will not store decrypted copies of owner's data, so unauthorized users cannot explore the data.

On the other hand, it provides to data owner a freedom from interacting with CSP, with the advantage of, no need to make encryption process in limited processing capability unit such as mobile device.

6) Creating Identity File (IF) phase:

TFP will generate an Identity File (IF) for the Mobile Users (MU) who have the right to explore owner's data using (Kmu). This phase ensures availability to authorized users.

$$IF = (file_{OD}, kmu)$$

7) Sending IF to MU phase:

After Identity File (IF) has been generated, it will be sent to Subscribed users who are authorized to explore data. These authorized users must be known to CSP in previous, as the owner identified them through list or group of "shared members."

The Identity File will be small in size, from the fact that it aims just to determine the authorized users who can only read

the file. So it can be stored in mobile's storage simply. A copy of Identity File (IF) will be stored too in TFP's storage unit.

8) Retrieving phase:

a) When the owner of mobile-data (OD) needs to retrieve his data, he sends a request to Trusted Front Party (TFP) with the associated Authentication File (AF). By sending AF from owner's mobile, TFP will match the (AF_{TFP}) stored in its storage unit with (AF_{OD}) sent from the mobile device, if these two AF matches, it means this user is the data owner (OD).

b) As a result, TFP sends a request to CSP to retrieve the Encrypted File (EF), and decrypt it using the same key (K_{enc}), where $DF = AES(EF, K_{enc})$.

c) Finally TFP sends the Decrypted File (DF) to owner of mobile-data (OD). In this case, OD will receive the original data without cipher text, where the mobile device has limited processing capabilities, and the MCC must provide reliable services to clients.

9) Updating files phase:

a) In every time the owner of mobile-data (OD) updates his file, TFP must update the Authentication File (AF) using the same (k_{od}) and resend it to OD, to keep file's assurance.

b) Also, TFP must update Identity File (IF) using the same (k_{mu}) and resend it to subscribed users (MU), to keep providing availability. As well as, the modified Identity File (IF) will be as a notification to mobile users that some updates were done by the owner.

c) Encrypting the updated file will be done using (k_{enc}), and sent to CSP to store the new one and delete the old one.

For every request of data, it must be sent directly to TFP not to CSP. Identity of user must be sent with the request, and one of the following cases will be achieved:

- If the request was sent for a specific file with its associated Authentication File (AF), TFP would indicate it was done by the owner of data (OD), and send a (read/write) decrypted file as a response.
- If the request was sent for a specific file with its associated Identity File (IF), TFP would indicate it was done by an authorized mobile user (MU), and send a (read only) decrypted file as a response.
- If the request was sent for a specific file without any identification, TFP would indicate it was done by an unauthorized mobile user, and reject the request as a response.
- If the request was sent for a specific file with a different identification such as AF or IF, which is not related to that file, TFP would indicate it was done by an unauthorized mobile user or a hacker who stole identification, and reject the request as a response.

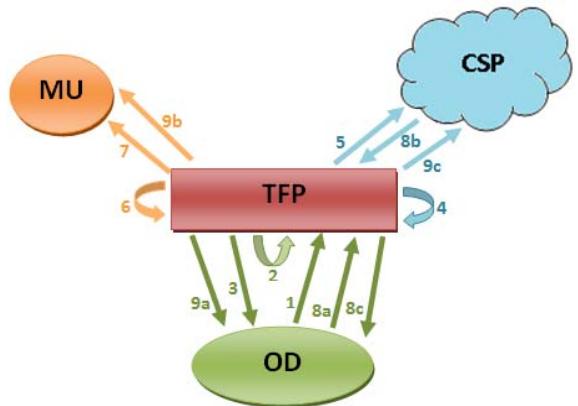


Figure 2. Communications between entities of the proposed scheme

IV. EVALUATION

In this section, we present the security assessments of the proposed scheme.

A presence of an intermediate party between mobile clients in general and cloud service provider, will contribute in effective manner in achieving security in MCC. That is, TFP is the third party that mobile user will only interact with. So, users' data will not be directly sent to CSP, it must be sent to TFP first to create three files, which are: AF, IF, EF.

Authentication File (AF) is the part that is created to obtain data integrity. While this file is created using the original file of owner of mobile-data (OD) and sent only to this owner, so the mobile user who owns this file has the privilege to explore and update the file. As no other user has this file, this means it will be safe from any changes and this is the idea of data integrity.

Furthermore, if any user can get AF in illegal way, he cannot distinguish to any file it belongs to. As the AF must be determined to particular file and there is no any hint in AF indicates the original file.

The second file created is the Encrypted File (EF), which represents owner's data sent by mobile device to be stored in CSP. The data will be encrypted before being sent to CSP to protect user's privacy and not be explored by unauthorized users or cloud servers owners. This operation is important to achieve confidentiality. There is no any file will be sent and stored in cloud servers provided by CSP without being encrypted.

The encryption process is made by Symmetric Key Encryption which considered being the most successful approach adopted to secure data, reduce memory consumption and reduce processing complexity, without the need of using asymmetric key encryption which uses two different keys. TFP is the only party who is responsible for encryption and decryption processes, that means there is no need to pass the key to OD or MU or CSP over the network. The key will be only known for TFP.

It was proven that symmetric algorithms are the more efficient in cloud environment, thanks to the high performance

in data processing, and among them the AES is determined to be the faster one. Many research papers have ensured that such as [12], [13].

As shown in [12], symmetric algorithms such as AES, DES, 3DES and Blowfish, and asymmetric algorithms like RSA and ElGamal, have been implemented and tested using different file sizes: 1 MB, 10 MB, 50 MB and 100MB in the same cloud environment in Table 1. Also in the case of changing data type such as image instead of text, it has been found that AES has advantage over RC2, RC6 and Blowfish in terms of time consumption.

The third file created is the Identity File (IF), which is created by TFP and transmitted to authorized mobile users (MU), to give them the ability to explore data. This gives the meaning of availability in the cloud where data remain available on demand by authorized users and can be accessed rapidly by sending request to TFP with the associated (IF).

When authorized user wants to explore a file, he will send a request to TFP by determining the file and the Identity File (IF) belongs to him. TFP will match the (IF_{TFP}) stored in its storage unit with (IF_{MU}) sent from the mobile device, if these two IF matches, it means this user is authorized. MU has not to resend the file to TFP as he/she will not make updates and received a read only copy.

It is distinguished to TFP that Identity File (IF) gives the privilege of read only, while Authentication File (AF) gives the privilege of read/write.

In addition to previous advantages, it is worthy to point out that all these operations (generating keys, creating files, encryption/decryption processes) are made in TFP without causing an additional overhead. While in mobile device with limited storage, it only needs to store a small-size file (AF or IF), and for it is limited processing capabilities it does not need to encrypt or decrypt any file.

TABLE 1 PROCESSING TIME AND KEY SIZE

		AES	DES	3 DES	Blowfish	RSA	ElGamal
Key size		256	64	192	256	2048	1024
File size (MB)	1	0.03	0.03	0.09	0.03	332.29	2935.90
	10	0.32	0.32	0.77	0.24	-	-
	50	1.61	1.89	4.49	2.13	-	-
	100	4.27	5.50	7.96	5.64	-	-

I. CONCLUSION

Due to limitations of mobile devices in processing capabilities and storage, many issues in mobile cloud computing are emerged. Security is considered to be the major issue in MCC, where data of owner is stored on the cloud, which is not secured. This paper provided the description of Mobile Computing, Cloud Computing, and Mobile Cloud Computing and issues associated with them. As well as discussing the main issue in MCC, the security. A number of mechanisms to store data in secure manner are explored. Also, a secure scheme for data storage in MCC is proposed to provide the security AIC triad concepts (availability, integrity, and confidentiality).

REFERENCES

- [1] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, "Above the clouds: a Berkeley view of cloud computing", Technical Report UCB/EECS-2009-28, 2009.
- [2] H. Dinh, C. Lee, D. Niyato, and P. Wang, "A survey of mobile cloud computing: architecture, applications, and approaches," Accepted in Wireless Communications and Mobile Computing - Wiley.
- [3] Cloud tweaks. 2012. *Top Five Challenges Of Cloud Computing*. [ONLINE] Available at: <http://cloudtweaks.com/2012/08/top-five-challenges-of-cloud-computing/>. [Accessed 26 March 2016].
- [4] R. B. Mannade and A. B. Bhande, "Challenges of Mobile Computing: An Overview", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, Issue 8, August 2013, pp. 3109-3114.
- [5] A. Surendra Shimpi and R. Chander, "Secure Framework in Data Processing for Mobile Cloud Computing", International Journal of Computer & Communication Technology, ISSN (Print) 0975- 7449, vol. 3, Iss. 3, 2012.
- [6] J. Mishra, S. Kumar Dash and Sweta Dash, "Mobile Cloud Computing: A Secure Framework of Cloud Computing for Mobile Application", Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 2012, pp. 347- 356.
- [7] Eugene E. Marinelli, "Hyrax: Cloud Computing on Mobile Devices", Dissertation of Thesis, Carnegie Mellon University, Pittsburgh, 2009.
- [8] W. Jia, H. Zhu, Z. Cao, L. Wei, X. Lin, "SDSM: a secure data service mechanism in mobile cloud computing," in: Proc. IEEE Conference on Computer Communications Workshops, INFOCOM WKSHPS, Shanghai, China, Apr. 2011.
- [9] W. Itani, A. Kayssi, A. Chehab, "Energy-efficient incremental integrat for securing storage in mobile cloud computing," in: Proc. Int. Conference on Energy Aware Computing, ICEAC '10, Cairo, Egypt, Dec. 2010.
- [10] Z. Zhou, D. Huang, "Efficient and secure data storage operations for mobile cloud computing," IACR Cryptology ePrint Archive: 185, 2011.
- [11] J. Yang, H. Wang, J. Wang, C. Tan, D. Yu1, "Provable data possession of resource constrained mobile devices in cloud computing," Journal of Networks 6 (7) (2011), pp. 1033–1040.
- [12] S. Belguith, A. Jemai, R Attia, "Enhancing Data Security in Cloud Computing Using a Lightweight Cryptographic Algorithm", The Eleventh International Conference on Autonomic and Autonomous Systems, ICAS 2015, ISBN: 978-1-61208-405-3, pp. 98-103.
- [13] A. Sachdev and M. Bhansali, "Enhancing Cloud Computing Security using AES Algorithm", International Journal of Computer Applications, vol. 67, No. 9, 2013, pp. 19-23.

AUTHORS PROFILE

Isra Sitam Mohammed Al-Qasrawi received the B.S. degree in Computer Science from Al-Balqa' Applied University, Jordan in 2004, the MSc in Computer Science from Yarmouk University, Jordan in 2009, Working as instructor in Al-Balqa' Applied University / Al-Huson University College- Department of Information Technology.

SimCT: A measure of semantic similarity adapted to hierarchies of concepts

Coulibaly Kpinna Tiekoura
National Polytechnic Institute
Department of Mathematics and Computer Science
Abidjan, Ivory Coast

Brou Konan Marcellin
National polytechnic Institute
Department of Mathematics and computers science
Yamoussoukro, Ivory Coast

Achiepo Odilon
National polytechnic Institute
Abidjan, Ivory Coast

Babri Michel
National Polytechnic Institute
Abidjan, Ivory Coast

Aka Boko
University of Nangui Abrogoua
Abidjan, Ivory Coast

Abstract— The Calculating of the similarity between data is a key problem in several disciplines such as machine learning, information retrieval (IR) and data analysis. In some areas such as social resilience, the similarity measures can be used to find the similarities between traumatized individuals or resilience's dimensions.

In this paper, we propose a measure of semantic similarity used in many applications including clustering and information retrieval. It relies on a knowledge base represented as a hierarchy of concepts (ontology, graph, taxonomy). Its uniqueness with respect to previous proposals is the difference between the indices of similarity that it establishes between brothers concepts located at the same hierarchical level and having the same direct ancestor. In addition, our semantic similarity measure provides better modularity in clustering compared with Wu and Palmer's similarity measure and Proxigena3.

Keywords- clustering, hierarchical tree, resilience, semantic similarity measure.

I. INTRODUCTION

The use of the similarity measures in a field meets a specific goal. The information retrieval, the calculation of Similarities between documents and users' queries is used to identify the relevant documents in relation to the information needs expressed by these users. In the field of clustering, these measures allow grouping objects in homogeneous classes according to their likeness.

In clustering, hierarchical representations such as ontologies are most often used to calculate the similarity between different concepts. In this proposal, we present a

measure of semantic similarity to calculate the semantic proximity between the concepts of a hierarchy.

The paper is organized as follows. In Section 2, we present the properties of similarity measures followed by a state of the art of the main proposals of semantic similarity measures, in Section 3. Section 4 is devoted to the description of our proposal. Finally, in Section 5, we present our experimental results highlighting a comparison between our measure of semantic similarity and two measures, especially, the widely used measure of Wu and Palmer [1] and the ProxiGenea3 measure of Damien D. and al [2].

II. PROPERTIES OF MEASURES OF SIMILARITY AND DISSIMILARITY

A. Definition

To calculate the proximity between two objects, we can either use a similarity or a dissimilarity or a distance [3].

Similarity / dissimilarity: We call similarity or dissimilarity, any application with numerical values that quantifies the relationship between two objects, according to their point of similarity and dissimilarity. The two objects to be compared must of course be of the same type. For a similarity, the link between two individuals is stronger when its value is great. For a dissimilarity, the link is stronger when its value is small [4].

B. Properties

Positivity property: An application $d : \Omega_I \times \Omega_I \rightarrow \mathbb{R}$ satisfies the positivity property if and only if:

$$\forall i, j \in \Omega_I, d(i, j) \geq 0 \quad (1)$$

Symmetry property: An application $d : \Omega_I \times \Omega_I \rightarrow \mathbb{R}$ verifies the symmetry property if and only if:

$$\forall i, j \in \Omega_I, d(i, j) = d(j, i) \quad (2)$$

Minimality property: An application $d : \Omega_I \times \Omega_I \rightarrow \mathbb{R}$ verifies the minimality property if and only if:

$$\forall i, j \in \Omega_I, d(i, j) = 0 \Leftrightarrow i = j \quad (3)$$

Maximality property: An application $d : \Omega_I \times \Omega_I \rightarrow \mathbb{R}$ checks the maximality property if and only if:

$$\forall i, j \in \Omega_I, d(i, i) \geq d(i, j) \quad (4)$$

Triangle inequality property: An application

$d : \Omega_I \times \Omega_I \rightarrow \mathbb{R}$ checks the triangle inequality property if and only if:

$$\forall i, j, k \in \Omega_I, d(i, j) \leq d(i, k) + d(k, j) \quad (5)$$

- The similarity is an application $s : \Omega_I \times \Omega_I \rightarrow \mathbb{R}^+$ which verifies the properties of symmetry, of positivity and of maximality.

- The dissimilarity is an application $d : \Omega_I \times \Omega_I \rightarrow \mathbb{R}^+$ which verifies the properties of symmetry, of positivity and of minimality.

- The Distance is an application $d : \Omega_I \times \Omega_I \rightarrow \mathbb{R}^+$ which verifies the properties of symmetry, of positivity, of minimality and of triangle inequality.

TABLE I. SUMMARY OF PROPERTIES OF SIMILARITY INDICES / DISSIMILARITY AND DISTANCE

Measurement Type	Symmetry	positivity	minimality	maximality	triangular inequality
Similarity	X	X		X	
dissimilarity	X	X	X		
Distance	X	X	X	X	X

III. STATE OF THE ART OF SEMANTIC SIMILARITY MEASURES

The choice of a similarity relates to the type of data used. In this paper, we focus on symbolic data, specifically to structured variables. These are variables represented as a hierarchy of concepts. These variables can be single-valued or variables with values composed (qualitative variable described by several terms or quantitative variable described by a range of values) in some cases. We present in this section Semantic similarity measures most used.

The semantic similarity can be defined according to two major approaches: those that include external information to

the hierarchy of concepts, for example, statistics on the use of the types of concepts [1] [5] [6] [7], and approaches based solely on the hierarchy of concepts [8] [9].

A. Similarity measures based on the hierarchy of concepts

These measures have to principle, the seeking of a taxonomic distance consisting to counting the number of edges that separate two senses. Thus, given two concepts, their similarity can be estimated from their position in the hierarchy. Every concept of the structure is represented by a node that is either a "child" called hyponym of another concept or a "parent" called hypernym.

The Measure of Rada and al. [8] is the first to use the distance between the nodes corresponding to the links of hyponymy and hypernym. The Semantic similarity between two concepts is the inverse of the distance between two concepts. More two concepts are distant, least they are similar. It is defined by:

$$Sim_{Rada}(x_i, x_j) = \frac{1}{1+dist_{edge}(x_i, x_j)} \quad (6)$$

With $dist_{edge}(x_i, x_j)$ is the length of the shortest path between two concepts x_i and x_j . According to Edge's approach, this distance can be measured by the geometric distance between the nodes representing the concepts x_i and x_j .

Leacock and Chodorow [9] are based on the fact that the lowest arcs in the hyponym's hierarchy, correspond to the smallest semantic distance. So, they have defined the following measure:

$$sim_{Lech}(x_i, x_j) = -\log \frac{longueur(x_i, x_j)}{2D} \quad (7)$$

Where D is the maximum depth or height of the hierarchy which is equivalent to the number of nodes between the highest concept in the hierarchy and the lowest concept.

$longueur(x_i, x_j)$ represents the length of the shortest path between x_i and x_j in terms of number of nodes.

The similarity measure of Wu and Palmer [1] measures the similarity between two concepts in WordNet taxonomy combining the depth of two given concepts and that of the lowest common ancestor (LCS or lowest common subsume). The authors rely on the fact that the terms are more deeply located in the taxonomy are always closer than the most general terms. It is defined as:

$$sim_{wup}(x_i, x_j) = \frac{2 \times d(LCS)}{d(x_i) + d(x_j)} \quad (8)$$

Where d (LCS) is the depth of the lowest common ancestor of the two concepts and $d(x_i)$, the depth of the concept x_i in the WordNet taxonomy.

Another measure of semantic similarity based on that of Wu and Palmer and the principle of family tree, was proposed

by Dudognon Gilles H. and B. Ralalason and baptized: ProxiGenea [2]. Its special feature is the inclusion of the distinction between the subsumption relations and sibling relationships unlike that proposed by Wu and Palmer. There are three versions of ProxiGenea to calculate the proximity

between two concepts x_i and x_j . They are defined as follows:

$$Pg_1(x_i, x_j) = \frac{d^2(LCS(x_i, x_j))}{d(x_i) \times d(x_j)} \quad (9)$$

$$Pg_2(x_i, x_j) = \frac{d(LCS(x_i, x_j))}{d(x_i) + d(x_j) - d(LCS(x_i, x_j))} \quad (10)$$

$$Pg_3(x_i, x_j) = \frac{1}{1+d(x_i)+d(x_j)-2d(LCS(x_i, x_j))} \quad (11)$$

With $d(x_i)$ all concepts that go into the genealogy of the concept x_i from the root to x_i and $d(LCS(x_i, x_j))$, the depth of the lowest common ancestor of concepts x_i and x_j such as

$$d(LCS(x_i, x_j)) = d(x_i) \cap d(x_j) \quad (12)$$

This similarity puts particular emphasis on the distance between concepts.

In [10], [11] and [12], a calculation method of the proximity between two sentences was proposed that combines a measure of structural similarity (n-gram based similarity) and the conceptual similarity measure (proxigenea 3) seen previously. The conceptual similarity between sentences p and q through an ontology is calculated as follows:

$$ss(p, q) = \frac{\sum_{x_i \in X_p} \max_{x_j \in X_q} s(x_i, x_j)}{|X_p|} \quad (13)$$

Where $s(x_i, x_j)$ is a measure of conceptual similarity between concepts x_i and x_j . That used by the authors, is ProxiGenea3 measure of Dudognon and al, presented above.

B. The similarity measures that include external information to the hierarchy of concepts

One of the most known measures of this type is that of Resnik proposed in [5] that uses the information content (IC) of the nodes (or concepts). It is generally based on a training corpus and measures the probability of finding a concept or one of his descendants in this corpus. Let \mathcal{X} be a concept, and $p(x)$ the probability of finding \mathcal{X} or find one of his descendants in the corpus. The information content associated with \mathcal{X} is then defined by:

$$IC(x) = -\log(p(x)) \quad (14)$$

$$\text{With } p(x) = \frac{freq(x)}{N} \quad (15)$$

$$\text{And } freq(x) = \sum_{a \in words(x)} count(a) \quad (16)$$

Where $word(c)$ is the set of words or terms representing the concept \mathcal{X} and concepts subsumed by \mathcal{X} ;

$freq(x)$ is the frequency of the concept in the corpus;

$count(a)$ denotes the number of occurrences of a term in the corpus;

N is the total number of occurrences of words found in the corpus.

Thus the similarity of Resnik between two concepts x_i and x_j is the following:

$$sim_{res}(x_i, x_j) = IC(LCS(x_i, x_j)) = -\log p(LCS(x_i, x_j)) \quad (17)$$

With $LCS(x_i, x_j)$ all concepts that subsume the two concepts x_i and x_j .

Another measure of semantic similarity based on the information content is proposed in [13]. Unlike the previous one, it is not based on the use of a corpus and calculates the information content of the nodes from WordNet [14] only. The hypothesis of Seco and al. is that, more a concept has descendants, the less it's informative. So, they use the hyponyms of a concept to calculate the information content thereof, as follows:

$$IC_{wn}(x) = \frac{\log \left(\frac{hypo(x)+1}{\max_{wn}} \right)}{\log \left(\frac{1}{\max_{wn}} \right)} = 1 - \frac{\log(hypo(x))+1}{\log(\max_{wn})} \quad (18)$$

Where $hypo(x)$ indicates the number of hyponyms of the concept \mathcal{X} , and \max_{wn} , the number of concepts in the taxonomy.

Lin in [7] proposes a measure that is only the standardization of Resnik's measure and an extension of the measure of Wu and Palmer mentioned above. This measure reuses the concepts of information content and lowest common ancestor (LCS).

$$sim_{lin}(x_i, x_j) = \frac{2 \times IC(LCS(x_i, x_j))}{IC(x_i) + IC(x_j)} = \frac{2 \times \log P(LCS(x_i, x_j))}{\log P(x_i) + \log P(x_j)} \quad (19)$$

Moreover, Lin defines a measurement class of similarity based on the metric distance between two concepts, from their metric

distance. Thus, if the distance metric between two concepts x_i and x_j is $dist(x_i, x_j)$, their similarity is defined by:

$$sim(x_i, x_j) = \frac{1}{1+dist(x_i, x_j)} \quad (20)$$

Finally, Jiang and Conrath [6], while also based on the measurement of Resnik, proposes to calculate the similarity between two concepts as follows:

$$sim_{jc}(x_i, x_j) = \frac{1}{IC(x_i)+IC(x_j)-2IC(LCS(x_i, x_j))} \quad (21)$$

C. Other similarity measures

The following similarity measures are based on corpuses. They don't require vocabulary or grammar of the language of the text. Among them, we can cite latent semantic analysis (LSA) in [15], the explicit semantic analysis (ESA) [16] or the normalized distance from Google (Normalized Google Distance (NGD)) [17].

IV. OUR PROPOSAL sim_{CT}

Among similarity measures presented in the previous section, we are particularly interested in that of Wu and Palmer and ProxiGénée 3 of Dudognon and al. In the hierarchy of concepts, there are two types of relationships between concepts: a sibling relationship and a subsumption relation. The sibling relationship is between two brothers-concepts and subsumption relationship is between two concepts whose meaning of one is included in the other (relationship of hyponymy and hypernymy). The measure proposed by Wu and Palmer [1] does not take sufficient account of the distinction between these relationships. It is certainly interesting, but has a limit because it essentially aims to detect the similarity between two concepts in relation to their distance from their lowest common ancestor. Dudognon and al, in their measure ProxiGenea 3, have certainly correct that aspect, however, a problem exist in the use of these two similarity measures: The concepts brothers (from the same concept father) always have the same value of similarity. In other words, for three concepts brothers data x_i , x_j and x_k , the value of similarity between

the concepts x_i and x_j is the same as that between x_i and x_k . This is abnormal in our view, at practical point of view. For our part, the concepts can be from the same concept father and not have the same semantic proximity. In this section, we propose an extension of the measure ProxiGenea 3 which takes into account this difference of values of similarity between such concepts. We illustrate further, our proposal by a practical case. Through the experimental results, we compare our proposal to those of Wu and Palmer and ProxyGenea 3.

A. Notation

Either a hierarchical tree.

- Nodes x_i represent different concepts;
- $\Omega = \{x_1, x_2, \dots, x_n\}$ denotes the set of all concepts of the hierarchy.
- x_{ij} means the lowest common ancestor (parent or immediate lowest common subsume (LCS)) of two concepts x_i and x_j .
- $d(x_{ij})$ is the depth of the common ancestor x_{ij} ;
- $d(x_i)$ is the depth of the hierarchy or the number of concepts which constitute his genealogy (from x_i to the root) ;
- $IC(x_i)$ is the information content of concept x_i ;
- For the use of our similarity measure, we first define a metric distance between concepts. This distance is the symmetric difference between the concepts.
- $LCS(x_i, x_j)$ is all common ancestors of both concepts x_i and x_j .
- $\zeta(x_i)$ is the set of concepts that go into genealogy x_i from the root to x_i .
- $\zeta(LCS(x_i, x_j))$ is the set of concepts that have the genealogy of the common ancestor of x_i and x_j .
- $\zeta(x_i) \Delta \zeta(x_j)$ denotes the symmetric difference of $\zeta(x_i)$ and $\zeta(x_j)$ that is to say all the concepts of the two concepts genealogies x_i and x_j which are not part of their common ancestors.
- $|\zeta(x_i) \Delta \zeta(x_j)|$ denotes the number of concepts of the symmetric difference of $\zeta(x_i)$ and $\zeta(x_j)$.

$$d(x_i) = card(\zeta(x_i)) \quad (22)$$

$$d(x_{ij}) = card(LCS(x_i, x_j)) \quad (23)$$

Given $\zeta(LCS(x_i, x_j))$ that intervenes in the genealogy of each concept ($\zeta(x_i)$ and $\zeta(x_j)$), we can define the cardinal of symmetric difference as follows:

$$|\zeta(x_i) \Delta \zeta(x_j)| = card(\zeta(x_i) \Delta \zeta(x_j)) \quad (24)$$

$$|\zeta(x_i)\Delta\zeta(x_j)| = d(x_i) + d(x_j) - 2d(x_{ij}) \quad (25)$$

Moreover, in calculating the length of the shortest path between two concepts, we also take account of a function that measures the difference of information content between these concepts. It is defined by:

$$f_{IC}(x_i, x_j) = 1 - \frac{1}{2} |IC(x_i) - IC(x_j)| \quad (26)$$

$$\text{With } IC(x) = \frac{\log\left(\frac{hypo(x)+1}{\max}\right)}{\log\left(\frac{1}{\max}\right)} = 1 - \frac{\log(hypo(x))+1}{\log(\max)} \quad (27)$$

Where $hypo(x)$ indicates the number of hyponyms of concept X , and \max , the total number of concepts in the taxonomy.

$$IC(x_i) - IC(x_j) = \frac{\log\left(\frac{hypo(x_i)+1}{\max}\right)}{\log\left(\frac{1}{\max}\right)} - \frac{\log\left(\frac{hypo(x_j)+1}{\max}\right)}{\log\left(\frac{1}{\max}\right)} \quad (28)$$

$$IC(x_i) - IC(x_j) = \frac{\log\left(\frac{hypo(x_i)+1}{\max}\right) - \log\left(\frac{hypo(x_j)+1}{\max}\right)}{\log\left(\frac{1}{\max}\right)} \quad (29)$$

$$IC(x_i) - IC(x_j) = \frac{\log\left(\frac{hypo(x_i)+1}{hypo(x_j)+1}\right)}{\log\left(\frac{1}{\max}\right)} \quad (30)$$

Is finally obtained:

$$f_{IC}(x_i, x_j) = 1 - \frac{1}{2} \left| \frac{\log\left(\frac{hypo(x_i)+1}{hypo(x_j)+1}\right)}{\log\left(\frac{1}{\max}\right)} \right| \quad (31)$$

We define the length of the shortest path between two concepts x_i and x_j by:

$$dist_{CT}(x_i, x_j) = |\zeta(x_i)\Delta\zeta(x_j)| \times f_{IC}(x_i, x_j) \quad (32)$$

$$dist_{CT}(x_i, x_j) = \left(d(x_i) + d(x_j) - 2d(x_{ij}) \right) \left(1 - \frac{1}{2} |IC(x_i) - IC(x_j)| \right) \quad (33)$$

Starting from the similarity measure of Lin [7] (20) and equation (33), we obtain our similarity measure between two concepts x_i and x_j of the hierarchy of concepts as follows:

$$sim_{CT}(x_i, x_j) = \frac{1}{1 + dist_{CT}(x_i, x_j)} \quad (34)$$

That is to say:

$$sim_{CT}(x_i, x_j) = \frac{1}{1 + (d(x_i) + d(x_j) - 2d(x_{ij})) \left(1 - \frac{1}{2} |IC(x_i) - IC(x_j)| \right)} \quad (35)$$

Or:

$$sim_{CT}(x_i, x_j) = \frac{1}{1 + (d(x_i) + d(x_j) - 2d(x_{ij})) \left(1 - \frac{1}{2} \left| \frac{\log\left(\frac{hypo(x_i)+1}{hypo(x_j)+1}\right)}{\log\left(\frac{1}{\max}\right)} \right| \right)} \quad (36)$$

B. Checking similarity properties

- sim_{CT} verifies the symmetry property:

$$\forall x_i, x_j \in \Omega = (x_i)_{i=1 \dots p}$$

$$sim_{CT}(x_i, x_j) = \frac{1}{1 + (d(x_i) + d(x_j) - 2d(x_{ij})) \left(1 - \frac{1}{2} |IC(x_i) - IC(x_j)| \right)} = sim_{CT}(x_j, x_i)$$

- sim_{CT} verifies the property of positivity:

$$\forall x_i, x_j \in \Omega = (x_i)_{i=1 \dots p}$$

$d(x_i) \geq d(x_{ij})$ and $d(x_j) \geq d(x_{ij})$ from where

$$d(x_i) + d(x_j) - 2d(x_{ij}) \geq 0$$

Otherwise, $1 \geq |IC(x_i) - IC(x_j)| \quad \forall x_i, x_j \in \Omega = (x_i)_{i=1 \dots p}$

$$\text{So, } 1 - \frac{1}{2} |IC(x_i) - IC(x_j)| \geq 0$$

The expression

$$1 + (d(x_i) + d(x_j) - 2d(x_{ij})) \left(1 - \frac{1}{2} |IC(x_i) - IC(x_j)| \right) \geq 0$$

Therefore

$$\frac{1}{1 + (d(x_i) + d(x_j) - 2d(x_{ij})) \left(1 - \frac{1}{2} |IC(x_i) - IC(x_j)| \right)} \geq 0$$

$$sim_{CT} \geq 0$$

- sim_{CT} verifies the property of maximality:

The quantity $1 + (d(x_i) + d(x_j) - 2d(x_{ij})) \left(1 - \frac{1}{2} |IC(x_i) - IC(x_j)| \right)$ reaches its minimum with $x_i = x_j$. So,

$$1 + (d(x_i) + d(x_i) - 2d(x_{ii})) \left(1 - \frac{1}{2} |IC(x_i) - IC(x_i)| \right) =$$

$$1 + (2d(x_i) - 2d(x_i)) \left(1 - \frac{1}{2} |IC(x_i) - IC(x_i)| \right) = 1 + 0 = 1$$

$$sim_{CT}(x_i, x_i) = \frac{1}{1} = 1 = \text{maximum of } sim_{CT}(x_i, x_j)$$

So, $\forall x_i, x_j \in \Omega = (x_i)_{i=1 \dots p} \quad sim_{CT}(x_i, x_i) \geq sim_{CT}(x_i, x_j)$

C. Experimentation and Evaluation

We apply here, our measure sim_{CT} of conceptual similarity in a practical case and present its assessment. We first describe the experimental data and we give the experimental results from the comparison of sim_{CT} with the similarity measure of Wu and Palmer and proxiGenea 3.

1) The experimental data

For our experiment, we use here, an ontology of social resilience [18]. For the purposes of our work, we amended and supplemented this ontology (Fig. 1) by including dimensions of social resilience [19]. For the sake of readability, we present just a part of the modified ontology.

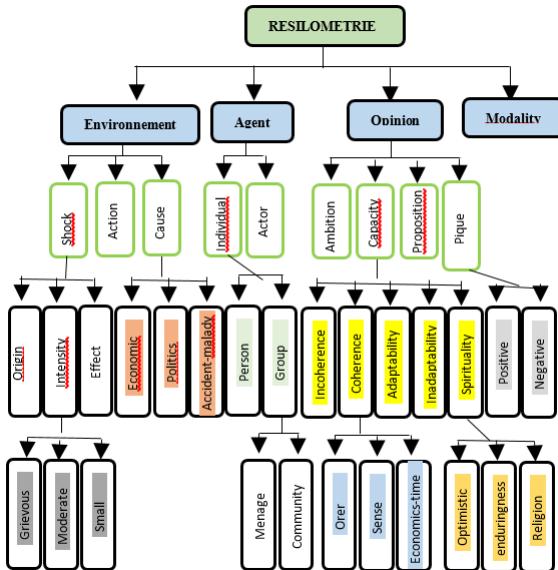


Fig. 1. Ontology of resilience processes.

We also use a simpler ontology extract (Fig. 2) similar to that used by Dudognon and al. in [2] for comparing our proposal to that of Wu and Palmer and ProxyGenea 3.

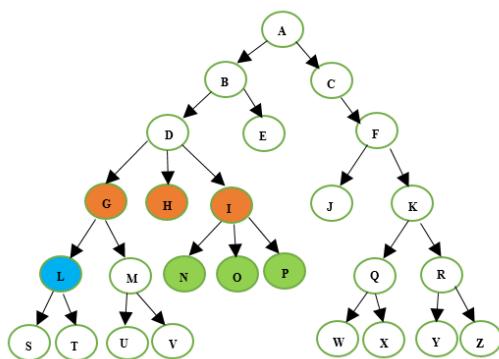


Fig. 2. Ontology extract

The objective of sim_{CT} is to distinguish the difference of similarity between concepts derived from a same hypernym or

immediate parent unlike to the proposal of Wu and Palmer as well as that of Dudognon mentioned in section 3.

Two main semantic relationships characterize our ontology namely:

- Hyperonymy: relationship between a concept1 and a concept2, more general (Capacity-coherence).

- Hyponymy: relationship between a concept1 and a more specific concept2. It is the reciprocal of the hyperonymy. This relationship may be useful in information retrieval. Indeed, if one seeks all texts dealing with capacity (resilience), it may be interesting to find those who speak of consciousness, or adaptability.

The application of our similarity measure on some concepts of Fig.1, gives the following similarity values:

- Similarity of two identical concepts (shock-shock):

$$\text{sim}_{CT}(\text{choc}, \text{choc}) = \frac{1}{1+(3+3-2\times 3)(1-0.5\times 0)} = \frac{1}{1+0} = 1$$

- Similarity of two concepts linked by the relationship "is one" (capacity - coherence):

$$\text{sim}_{CT}(\text{cap}, \text{coh}) = \frac{1}{1+(3+4-2\times 3)(1-0.5\times|-0.297|)} = 0.54$$

- Similarity of two brothers concepts (coherence-incoherence) or (coherence - spirituality):

$$\text{sim}_{CT}(\text{coh}, \text{incoh}) = \frac{1}{1+(4+4-2\times 3)(1-0.5\times|-0.375|)} = 0.38$$

$$\text{sim}_{CT}(\text{coh}, \text{spir}) = \frac{1}{1+(4+4-2\times 3)(1-0)} = 0.33$$

- Similarity of two concepts from two different taxonomic branches (grievous - religion):

$$\text{sim}_{CT}(\text{grav}, \text{rel}) = \frac{1}{1+(5+5-2\times 1)(1-0.5\times 0)} = 0.11$$

2) Comparison of conceptual similarity measures

Here, we applied the three conceptual similarity measures (sim_{CT} , proxiGenea 3 and Wu & Palmer) to the extract of simplified ontology of Fig. 2.

Table II summarizes the results obtained after application of the three measures of similarity. The aim is to show how different similarity measures take into account the different types of relationships between concepts and their relative positions in the hierarchy of concepts.

TABLE II. COMPARISON OF SEMANTIC SIMILARITY MEASURES.

N°	C ₁	C ₂	WP	Pg3	Sim _{CT}
1	A	B	0.67	0.67	0.85
2	A	C	0.67	0.67	0.77
3	B	D	0.67	0.5	0.79
4	B	E	0.67	0.33	0.35
5	D	G	0.8	0.5	0.56
6	D	H	0.8	0.5	0.28
7	D	I	0.8	0.5	0.43

8	I	N	0.85	0.5	0.30
9	I	O	0.85	0.5	0.30
10	L	S	0.88	0.5	0.30
11	B	C	0.5	0.5	0.68
12	D	E	0.5	0.33	0.32
13	G	H	0.67	0.33	0.23
14	H	I	0.67	0.33	0.20
15	N	O	0.75	0.33	0.18
16	N	P	0.75	0.33	0.18
17	O	P	0.75	0.33	0.18
18	L	M	0.75	0.33	0.26
19	S	T	0.80	0.33	0.17
20	A	A	1	1	1
21	B	B	1	1	1
22	G	K	0.16	0.16	0.29
23	L	R	0.12	0.12	0.15
24	S	Z	0.10	0.10	0.09
25	A	D	0.4	0.4	0.70
26	B	G	0.5	0.33	0.49
27	I	L	0.57	0.25	0.22
28	Q	Y	0.67	0.25	0.17
29	A	G	0.28	0.28	0.45
30	D	S	0.57	0.25	0.17

Table II presents the similarities values between concepts according to the type of relationship. Thus, lines 1 to 10 show the similarities of pairs of concepts related by subsumption relationship; Lines 11-19 show the pairs of concepts brothers ; lines 20 and 21 are the similarities values of pairs of identical concepts ; Lines 22-24 show the similarities values of concepts located on two different under taxonomic trees ; Lines 25 and 26 present the case of pairs of concepts bound by the relationship of grandfather and grand-son; Lines 27 and 28 show the similarities values of pairs of concepts linked by the uncle and nephew relationship ; Finally, lines 29 and 30 concern couples of concepts linked by the relationship of rear - grandfather and great-grand - son.

The Semantic similarity matrix of simct stemming from Table II above is:

TABLE III. MATRIX OF SEMANTIC SIMILARITY SIMCT

	A	B	C	D	E	G	H	I
A	1.00	0.52	0.53	0.35	0.50	0.29	0.40	0.31
B	0.52	1.00	0.34	0.50	0.63	0.36	0.46	0.38
C	0.53	0.34	1.00	0.25	0.34	0.20	0.27	0.22
D	0.35	0.50	0.25	1.00	0.45	0.52	0.62	0.54
E	0.50	0.63	0.34	0.45	1.00	0.32	0.25	0.29
G	0.29	0.36	0.20	0.52	0.32	1.00	0.41	0.35
H	0.40	0.46	0.27	0.62	0.25	0.41	1.00	0.38
I	0.31	0.38	0.22	0.54	0.29	0.35	0.38	1.00

The Analysis of Tables II and III allows us to observe some similarities between the three similarity measures such as the privileging subsumption relationship to sibling relationship. However, the subsumption relation is more privileged with the measures of simct and proxiGenea3 unlike that of Wu and Palmer.

All the concepts brothers which have the same number of subsumed concepts have the same Similarity value: 0.33. This is the case for example of the relationships: I-N, I-O and I-P.

Moreover, between two concepts by the sibling relationship, the closer to the father is the one who is least subsumed (which has fewer son concepts). This is the case of relationships D-G, D-H and D-I. At the level of concepts brothers, Wu and Palmer and ProxiGenea 3 gives an identical similarity value to these concepts. In practice, this is not quite realistic, in our view. Indeed, the concepts can be from the same father and not have the same characteristics. For example, in the ontology of resilience processes shown above, the "coherence" concept is semantically more similar to the concept "incoherence" than the concept "spirituality" although all from the same father. Our measure of similarity simct establishes a difference in similarity values of concepts brothers, through the calculation function of the difference in information content f_{IC} associated.

3) Evaluation of our approach

For a partition P of all the nodes in k ($k \leq n$) groups, the modularity Q is defined by:

$$Q = \sum_{C \in P} \frac{w_C}{w} - \left(\frac{D_C}{2w} \right)^2 \quad (37)$$

Where w_C is the number of links within the class C;

D_C , the sum of the degrees of all nodes of the class C;

w , the number of links in the hierarchy of concepts.

The calculation results of modularity are presented in Table IV.

TABLE IV. COMPARISON OF MODULARITY BASED ON THE NUMBER OF CLASSES.

Number of classes	Modularity		
	WP	PG	Simct
2	0.131	0.154	0.156
3	0.129	0.129	0.129
4	0.145	0.150	0.160

Looking at the graph in Fig. 3 below, we notice a superiority of our proposal in terms of clustering quality than that of Wu and Palmer and proxiGénéa3.

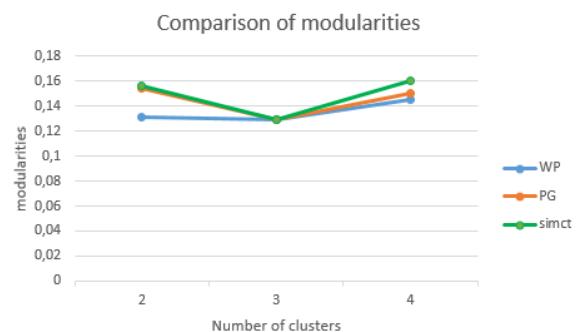


Fig. 3. Comparison of modularities

V. CONCLUSION AND OUTLOOK

In this paper, we proposed a conceptual semantic similarity measure on taxonomic data type. It can be used in many applications including automatic classification or for information retrieval (IR). Our proposal, compared to the Wu and Palmer measure and ProxiGenea 3 provides a better quality of clustering and establishes a difference in the semantic similarity between concepts brothers from the same father.

Our future work will consist initially, to apply our similarity measure on larger data to confirm the results presented in this article in a broader context. Secondly, we will consider extending this measure to other types of symbolic data.

REFERENCES

- [1] WU, Z. et PALMER, M., Verb semantics and lexical selection, Proceedings of the 23rd Annual Meetings of the Associations for Computational Linguistics, p. 133-138, 1994
- [2] Dudognon, D., Hubert, G., & Ralalason, B. J. V., Proxigénéa: Une mesure de similarité conceptuelle. In Proceedings of the Colloque Veille Stratégique Scientifique et Technologique (VSST 2010), 2010, October.
- [3] Bisson G. La similarité: une notion symbolique/numérique, In Apprentissage symbolique - numérique, éd. par Moulet B. Editions CEPADUES, pp. 169 - 201, 2000.
- [4] Celeux G., Diday E., Lechevallier Y., Govaert G. and Ralambondrainy H. Classification automatique des données, Editions Dunod, Paris, 1989.
- [5] RESNIK, P., Using information content to evaluate semantic similarity in a taxonomy, IJCAI, p. 448-453, 1995.
- [6] JIANG, J. et CONRATH, D.W., Semantic Similarity based on Corpus Statistics and Lexical Taxonomy, Proceedings of the International Conference on Research in Computational Linguistics (ROCLING), Taiwan, 1997.
- [7] LIN, D., An information-theoretic definition of similarity, Proceedings of the 15th international conference on Machine Learning, p. 296-304, 1998.
- [8] RADA, R., MILI, H., BICKNELL, E. et BLETTNER, M., Development and application of a metric on semanticnets. Systems, Man and Cybernetics, IEEE Transactions on, 19(1): p. 17-30, 1989.
- [9] LEACOCK, C., MILLER, G. A., et CHODOROW, M., Using corpus statistics and WordNet relations for sense identification, Comput. Linguist. 24, 1, 147-165, 1998
- [10] Buscaldi, D., Flores, J. J. G., Meza, I. V., & Rodriguez, I., SOPA: Random Forests Regression for the Semantic Textual Similarity task.SemEval-2015, 132, 2015.
- [11] Buscaldi, D., Le Roux, J., Flores, J. J. G., & Popescu, A., Lipn-core: Semantic text similarity using n-grams, wordnet, syntactic analysis, esa and information retrieval based features. In Second Joint Conference on Lexical and Computational Semantics (p. 63), 2013, June.
- [12] Buscaldi, D., Tournier, R., Aussenac-Gilles, N., & Mothe, J., Irit: Textual similarity combining conceptual similarity with an n-gram comparison method. In Proceedings of the First Joint Conference on Lexical and Computational Semantics-Volume 1: Proceedings of the main conference and the shared task, and Volume 2: Proceedings of the Sixth International Workshop on Semantic Evaluation (pp. 552-556). Association for Computational Linguistics, 2012, June.
- [13] Seco, N., Veale, T., & Hayes, J., An intrinsic information content metric for semantic similarity in WordNet. In ECAI (Vol. 16, p. 1089), 2004, August.
- [14] Fellbaum, C., A semantic network of english: the mother of all WordNets. In EuroWordNet: A multilingual database with lexical semantic networks (pp. 137-148). Springer Netherlands, 1998.
- [15] Deerwester, S., Dumais, S.T., Furnas, G. W., Landauer, T.K., and Harshman, R., Indexing by latent semantic analysis. JOURNAL OF THE AMERICAN SOCIETY FOR INFORMATION SCIENCE, 41(6) : 391-407, 2010, October.
- [16] Gabrilovich, E. and Markovitch, S., Computing semantic relatedness using Wikipedia-based explicit semantic analysis. In In Proceedings of the 20th International Joint Conference on Artificial Intelligence, pages 1606-1611, 2007.
- [17] Cilibra, R. L. and Vitanyi, P.M.B. , The google similarity distance. IEEE Trans. On knowl. And Data Eng., 19(3):370-383, 2007.
- [18] ACHIEPO OdilonYapo M., Les bases fondamentales de la Résilométrie, une science de modélisation de la souffrance. Journée Scientifique « Café Résilience », Février 2015.
- [19] COULIBALY Kpinna Tiekoura, Odilon Yapo M. ACHIEPO, Brou Konan Marcellin, Michel Babri. « Resilometrical modeling of interactions in social resilience dimensions ». International Journal of Computer Science Issues (IJCSI), Volume 12, Issue 4, July 2015.
- [20] Newman M.E.J., Girman M., Finding an evaluating community structure in networks.Physical Review E, 69(6), 2004.
- [21] Van Dongen S.M., Graph Clustering by Flow Simulation. PhD thesis, University of Utrecht, 2000.

AUTHORS PROFILE

Coulibaly Kpinna Tiekoura is now PhD student at the Department of Mathematics and Computer Science of National Polytechnic Institute (Yamoussoukro, Ivory Coast). He received his M.S. degree in data processing from University of Nangui Abrogba in 2013. He is a member of the international resilience research group (UMI Resilience, IRD) and is also a member of the Laboratory of Computer Sciences and Telecommunications (INP-HB) Abidjan, Ivory Coast. His research interests include the mathematical modeling, the resilience process, Multidimensional Statistics, Artificial Intelligence, Machine Learning, Data Mining and Data Science. His works are centered on clustering methods adapted to resilience process.

Brou Konan Marcellin is a Ph-D in Computer Science and Teacher researcher at the Houphouët Boigny National Polytechnic Institute (INP-HB) of Yamoussoukro (Ivory Coast). He is the Director of the Department of Mathematics and Computer Science. He is a Member of Laboratory in Computer Sciences and Telecommunications (INPHB). His interests are information systems, database and programming languages.

Odilon Yapo M. ACHIEPO is a statistician-economist Engineer (ENSEA Abidjan, Ivory Coast) and has a Master degree in Computer Science with specialization in Artificial Intelligence and Business Intelligence (Polytechnic School of Nantes, France). He is a Ph-D student in Mathematics and Information Technologies (EDP-INPHB Yamoussoukro, Ivory Coast). He is also a Teacher-researcher in University of Korhogo (Ivory Coast), International Senior-Expert Consultant, member of the international resilience research group (UMI Resilience, IRD) and is a member of the Laboratory of Computer Sciences and Telecommunications (INP-HB) Abidjan, Ivory Coast. His centers of interests are Computational Mathematics, Multidimensional Statistics, Artificial Intelligence, Machine Learning, Data Mining and Data Science. He also is the author-creator of the Resilometrics, a modeling discipline which consists on developing and applies computational models for measure, analyze and simulate social resilience process.

Babri Michel, PhD, is now Senior Lecturer in data processing. He teaches data processing and telecommunication in INP-HB. He is the Director of the Laboratory of Computer Sciences and Telecommunications (INP-HB) Abidjan, Ivory Coast. The topics of his current interest of research include distributed networks, cloud computing, convergent mobile networks, big Data and software defined networks.

Aka Boko, is a titular professor in computer sciences and physical sciences at Nangui Abrogoua University (Abidjan, Ivory Coast). He is the Director of the Department of Mathematics and Computer Sciences at that University. His interests are information systems, big data, programming languages and Artificial Intelligence.

An algorithm (COLMSTD) for detection of defects on rail and profile surfaces

İlhami Muhammed Orak
Faculty of Engineering
Karabuk University
Karabuk, Turkey (78000)

Ahmet Çelik
Tavşanlı Vocational School
Dumlupınar University
Kutahya, Turkey

Abstract—Rail or profile products are used in many fields today. The rolling process is the most important production phase of the rail and the profile product. However, undesirable defects in the surface of the product during the rolling process can occur. Identifying these defects quickly by an intelligent system using image processing algorithms will provide a major contribution in terms of time and labor. For the detection of the regions, objects and shapes on the image, several algorithms were used. In this study, we introduce a Standard Deviation based algorithm (COLMSTD) by using the pixel color values. In order to evaluate the performance of the algorithm, the result of the COLMSTD algorithm is compared with the results of Hough Transform, MSER, DFT, Watershed, Blob Detection algorithms. In this study, it was seen that each algorithm has different capability in some extend to identify the surface defects in rail or profile. However, COLMSTD algorithm achieve more accurate and successful results than the other algorithms.

Keywords- Computer vision; Image processing; Manufacturing systems; Defect detection; Hot rolling; Rail; Profile.

I. INTRODUCTION

During the rolling process, unexpected or unwanted defects on the material may be encountered. As the defects occur during the production process, the defected material has to be detected and the causes of the defect must be eliminated immediately. Offline detection of defects is extremely slow and does not have sufficient reliability. The defect inspection of the rolled products is being done on the cooling bed visually. On the other hand, the inspection of rail's inner surface defect is performed at the defect control center. The purpose of this study is to enable online detection of defects on the rolled material with respective size ranges between 0.5-2.5 cm. The detection system; we targeted should give quick results for the material rolled in about 7 m/s by processing images taken with the CMOS camera. In this rolling, crack (linear), point, or regional type of defects can be encountered on the surface of material.

These defects may not always be in uniform shapes. Therefore, detection of defects is difficult. During the rolling stage of rail or profile, since the cylinder force is applied from different directions, this can increase the defect rates. To detect the defects on all surfaces of rail or profile materials, there must be at least 8 cameras in the system. For detecting defects that occur during the rolling process, the studies were mostly related to flat rolling fields and were limited to certain types of defects. FFT feature extraction methods along side with artificial neural networks and genetic algorithms used for defect detection process [1]. Detection of defects by using background extraction method used on the obtained gray images taken with CCD

camera [2]. On the other hand, SVM (Support Vector Machine) algorithm used for defect detection and classification in real-time [3]. A parallel image processing system used to detect the defects occurring in the cold rolling process [4]. Artificial neural networks used for defect detection in cold rolling [5,6].

In this study, investigation is conducted for defect detection on rail or profile images. A new algorithm named COLMSTD is introduced. It is based on standard deviation ad uses column wise consideration. In order to evaluate its success rate, five other image processing algorithm are also used for comparison. This new algorithm shows high success rate for all type of defects. The other algorithms show success in certain types of defects, but they are insufficient in detection of all defects.

II. DEFECT DETECTION SYSTEM

Defect detection system consists of two basic parts, as shown in Fig. 1. It constitutes image acquisition as the first stage. In the first stage high resolution of CMOS camera is used to acquire images. Images are obtained from the camera in gray color with the help of the hardware structure [7]. Pixel values on the gray images are in between 0 and 255. Image qualities are in 8-byte color depths. Pixel value is obtained by taking the average of RGB (Red, Green, and Blue) color values.

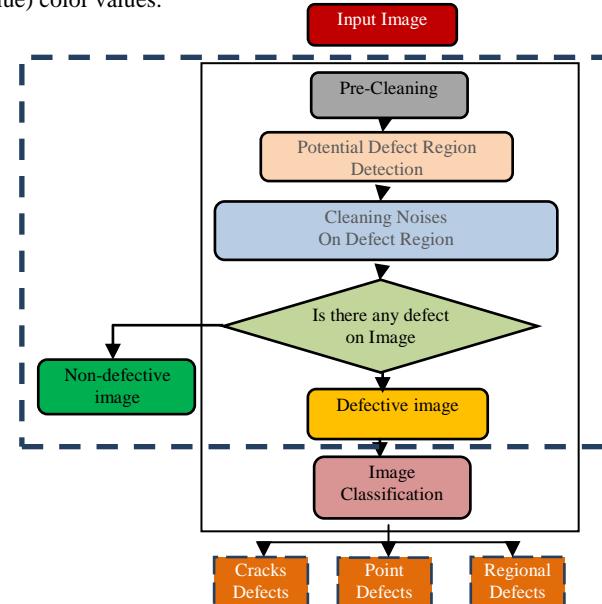


Figure 1. Defect identification system

In the next step, defect detection for obtained images is conducted. This stage covers, the detection of potential defect regions, noise removing and identifying the potential defects in the noise-cleaned image. In previous study, algorithm for the removing noise in the defective region was developed [8]. In this study, as the next step, an effective algorithm is developed for recognition of all types of defects.

The sizes of the rail images obtained by the camera are in 416x197 or 384x197 pixels. Additionally, the number of images obtained for each rail varies between 100 and 1150 depending on the rail length. In this study, the images were obtained from a prototype system used in the rail and profile mill of Kardemir Inc. The system produces colored image of a rail structure and shows the defected areas in different colors as it is displayed in Fig. 2. Surfaces of head, body and base of rail are displayed in two dimensional image. In the image, defect-free regions are displayed in green, pit regions are in blue and bump regions are in red. The results of our algorithms will be verified with the results of this system.

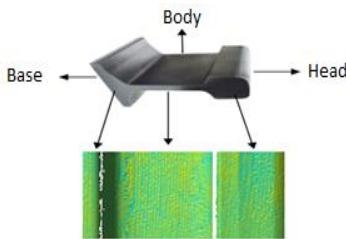
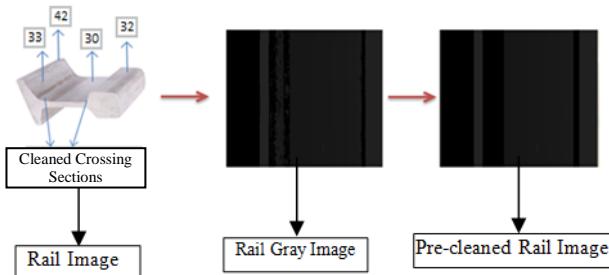


Figure 2. Rail structure and 3D rail modeling

In the prototype system, the top view of rail is obtained from the camera located in exit section of the rolling mill. As shown in Fig. 3, rail image is in gray tone. In this study, prior to applying algorithms, crossing regions of the base, body and head of the rail are cleaned in order to achieve accurate results.

Figure 3. Real and gray image of rail



III. COLMSTD ALGORITHM

In this study, we consider to introduce column-based evaluation for image processing. In column wise, pixels have similar gray values opposite to row wise where sheds occurs in different section of the rail images. The method aims to reveal defective region by using standard deviation of each column and comparing the value of pixel with the neighboring pixels. Different gray values are obtained on image depending on the shape of the product surface. The region having deviated gray value is marked as possible defected region. In this method, first of arithmetic means of all columns are calculated. The standard deviation calculated for each column could be effectively used in the separation of the regions. These regions represented with different colors if desired. Calculation of the arithmetic mean of the pixels in a column is expressed by the following equation.

$$\text{Mean}_j = \frac{1}{N} \sum_i^N P_{i,j} \rightarrow \frac{(P_{(0,j)} + P_{(1,j)} + P_{(2,j)} + \dots + P_{(N,j)})}{N} \quad (1)$$

Here $j = 0 \rightarrow M$ and N is the number of pixels on a column specifying the height of the image and M is the number of columns. $P_{i,j}$, is the gray value of each pixel.

Standard deviation is one of the most widely used statistical methods. In terms of image processing, by using this method, the pixels having different value than the average value could be identified. Standard deviation is also used in image filtering for removing unwanted pixels. Recognition of objects or regions on images can also be done by this technique [9]. Standard deviation is obtained by the following equation.

Standard Deviation is shown;

$$\sqrt{\frac{1}{N} \sum_{i=0}^N (P_{i,j} - \text{Mean}_j)^2} \quad (2)$$

Where $j \leq M$. In Fig. 4, the detection of point, crack and regional defective areas by COLMSTD algorithm are shown. It can be seen that regional and point type defects are correctly detected. The positions of the detected defects coincide with the actual position of the defects. If a smaller sensitivity coefficient (hk) is selected, the defects can be detected more precisely. The defect numbered as "1" in the Figure is a regional defect and defect sensitivity coefficient is 1.22. Line and regional defects are shown as "2" and "3" respectively. Since this algorithm is applied directly onto gray rail image without l_0 normalization, it provides time saving.

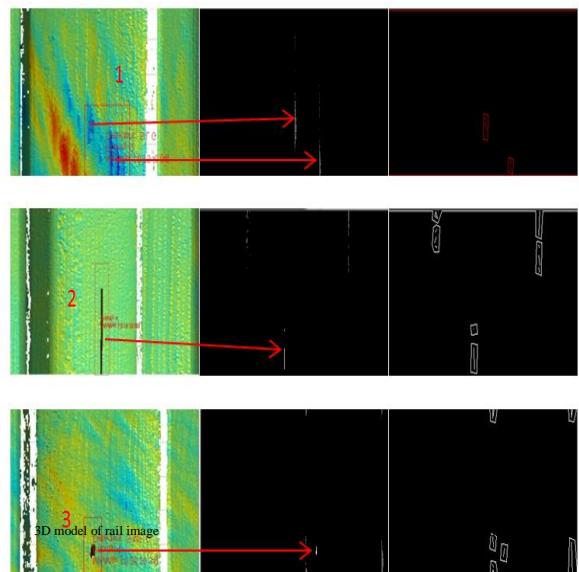


Figure 4. Defect detection capability of COLMSTD algorithm

COLMSTD image processing algorithm based on arithmetic average and standard deviation classify pixels having gray values greater than specified threshold level. Accordingly;

```

 $P_{i,j} \neq 0$ 
 $\left\{ \begin{array}{l} \text{if } |P_{i,j} - S_{Mn}| \leq StSpm \\ \{ \\ \text{Not\_defect} \rightarrow (P_{i,j} = 0) \\ \} \\ \text{elseif } |P_{i,j} - S_{Mn}| > hk (hk = 1.8) \\ \{ \\ \text{Deep\_defect} \rightarrow (P_{i,j} = 255) \\ \} \\ \text{elseif } |P_{i,j} - S_{Mn}| > hk (hk = 1.5) \\ \{ \\ \text{Medium\_depth\_defect} \rightarrow (P_{i,j} = 150) \\ \} \\ \text{else} \\ \{ \\ \text{Low\_depth\_defect} \rightarrow (P_{i,j} = 50) \\ \} \end{array} \right. \quad (3)$ 

```

Where $P_{i,j}$ is the gray value of each pixel, S_{Mn} is the mean of column and $StSpm$ is the standard deviation of column pixel values. $(P_{i,j} = 0)$, $(P_{i,j} = 255)$, $(P_{i,j} = 150)$ and $(P_{i,j} = 50)$ are results of COLMSTD algorithm.

IV. OTHERS ALGORITHMS USED FOR DEFECT DETECTION

For comparison reason, DFT, Blob Detection, MSER, Hough Transform and Watershed algorithms are considered for detection of defects on the rail or profile. Some of the algorithms cannot be efficient on the images taken directly from the camera. In this respect, Hough Transform, MSER, DFT, and Blob detection algorithms are applied after l_0 normalization process.

A. l_0 NORM (Zero Level Normalization)

In general the l_0 norm of X is defined as:

$$\|x\|_p = \sqrt[p]{\sum_i X_i^p} \quad (4)$$

Where $p \in R$. Hence, l_0 norm of X is

$$p \rightarrow \|x\|_0 = \sqrt[0]{\sum_i X_i^0} \quad (5)$$

Since there is a zeroth-power and zeroth-root in it, it is more commonly can be summarized mathematically as follows [10].

$$\|x\|_0 = \lim_{p \rightarrow 0} \|x\|_p^p = \#(i | x_i \neq 0) \quad (6)$$

This is a very simple and intuitive measure of sparsity of a vector x , counting the number of nonzero entries in a matrix. l_0 normalization process compares the differences between adjacent pixels on the image. If there are greater differences between adjacent pixels color values, l_0 norm constitutes edge in that area according to the image brightness values. l_0 normalization of image (I) can be expressed as following [11].

$$c(I) = \#\{p \mid I_p - I_{p+1} \neq 0\} \quad (7)$$

Where p is index value, I_p and I_{p+1} indicates neighbor pixel gray values. $c(I)$ parameter shows the results of l_0 norm value [11].

B. DFT (Discrete Fourier Transform)

DFT may indicate the frequency distribution of pixels on an image. Information about existence and shape of an object can be obtained according to frequency distribution. Fourier Transform generates a frequency distribution plane consisting of sinus and cosines values by using the values of the gray image. Fourier transform of two dimensional image or a matrix is expressed as [12].

$$F(x_{df}, y_{df}) = \sum_{x_{df}=0}^{M-1} \sum_{y_{df}=0}^{N-1} I(x_{image}, y_{image}) e^{-iw} \quad (8)$$

$$e^w = e^{2\Omega(\frac{x_{df} * x_{image}}{M} + \frac{y_{df} * y_{image}}{N})} \quad (9)$$

Where $I(x_{image}, y_{image})$ is an image, x_{image} and y_{image} are gray values on coordinate plane. $F(x_{df}, y_{df})$ indicates frequency plane for x_{df} and y_{df} points. M is the width of image and N is the height of image [12].

C. Blob Detector

Blob (droplet) detection algorithm is used for detection of the small region (spots) on images. In order to identify blob region, some data related to blob such as area, radius, type, center, and threshold must be calculated. In blob detection, every pixel in the image is compared with the 8 neighboring pixels and similar ones will be combined together. This method finds blob object having gray values different from the background of the image [13].

Identification of the blob can be done by filtering. The most common filter used in blob detection is LoG (Laplacian of Gaussian). Application of the LoG function to 2-dimensional image is shown as following [12-14].

$$LoG(x, y) = -\frac{1}{\Omega\sigma^2} \left[1 - \frac{x^2 + y^2}{2\Omega\sigma^2} \right] e^{-\frac{x^2 + y^2}{2\Omega\sigma^2}} \quad (10)$$

Where σ is sigma value and indicated by

$$\sigma = \frac{\text{radius}}{\sqrt{2}} \quad (11)$$

The radius value is predetermined value of blob object. $LoG(x, y)$ calculates the value of image x and y points [12].

D. MSER (Maximally Stable Extremal Regions)

Maximally Stable Extremal Region (MSER) is used to identify distinct regions in the images. MSER algorithm recognizes the regions by comparing their pixels intensities. In MSER algorithm, the bright (white) regions have maximum intensity values and the dark regions have minimum. MSER algorithm is carried out in 4 steps [15].

Pre-process: The densities of pixels are determined.

Segmentation: Image is divided into regions according to the density values.

MSER detection: Regions are labeled as Q_i according to their size.

Showing result: The defected regions are shown by determining the boundaries.

The regions with different density values on the image distinguished using the binary system. The division process is indicated by [16].

$$I_{binary} = \begin{cases} 1 & \rightarrow I_{in} \geq g \\ 0 & \rightarrow \text{otherwise} \end{cases} \quad (12)$$

Where I , g and I_{in} indicate image, defined threshold value and intensity value of a region respectively. By comparing with threshold value, results are converted to binary system. If the image density value is greater than or equal to threshold value, it takes value “1” or otherwise “0”. Intensity value, I_{in} can be calculated by dividing pixel gray values of Q_i to total number of pixels. Q_i region value is indicated as follows.

$$g \in [\min(I_{in}), \max(I_{in})] \quad (13)$$

In MSER algorithm, starting from outermost region towards innermost regions all regions are compared and Q_i regions are identified. Q_i extremal region has the following rule for maximum intensity [16].

$$Q_i \geq Q_{i-1} \quad (14)$$

The boundaries of regions are marked while considering the pixel values. Finally based on the extremal regions maximally stable extremal regions are calculated as follows [16].

$$(Q_i^g) = |Q_i^{g-\Delta}| - |Q_i^{g+\Delta}| / Q_i^g \quad (15)$$

Q_i^g , area is obtained with a threshold value for gray value (g), Δ is the stability range parameter. $Q_i^{g-\Delta}$ and $Q_i^{g+\Delta}$ extremal regions [16].

E. Hough Transform

Hough Transform is used to determine the objects, their location and their angle. This method is usually used in detection of lines in pictures. However, the generalized Hough Transform is capable of working for all type of shapes that can be expressed mathematically [17]. There are 3 main types of this method as linear, circular, and general. To identify irregular shapes, General Hough transform algorithm is used, but the features of shape and its size must be defined in advance[17,18]. On the other hand, Circular Hough Transform needs proper circle shape to be used. For that reason we will only consider Linear Hough Transform.

1) Linear Hough Transform

Linear Hough Transform converts the object-finding problem to density-finding problem by moving the information from image space to parameter space [17]. A line is generally expressed as:

$$y = ax + b \quad (16)$$

Each different (a, b) pair in parameter space represents a different line. Another method of expressing a line is:

$$x \cos \theta + y \sin \theta = \rho \quad (17)$$

Where θ can take value between 0 and 180 degrees.

Here ρ refers to normal of stated line drawn from the origin [17]. The intersection points of the lines drawn from different angles and the defined line are obtained. By connecting these intersecting points, the line is generated.

F. WATERSHED Algorithm

Watershed algorithm is one of the effective segmentation algorithms [19]. It consists of 2 main steps. First step is sorting the pixel gray values. The second step is grouping pixels by using threshold value [20]. In this method, image segmentation is based on isolating an object from the background. The regions are isolated by using the gray values and then labeled [21]. When it is applied on rail images, deviations in the value of the pixels show defective regions. The threshold T_h of image pixel value is given as [22].

$$T_h = \{p \in \text{Res}, u(p) \leq h\} \quad (18)$$

Where $u(p)$ scalar function takes h level which changes between h_{\min} and h_{\max} . Res is image resolution. Calculation of Watershed region value X_h is indicated by following equation [22].

$$\begin{cases} X_{h_{\min}} = T_{h_{\min}} \\ \forall h \in [h_{\min}, h_{\max} - 1], X_{h+1} = \min_{h+1} \cup IZ_{T_{h+1}}(X_h) \end{cases} \quad (19)$$

$IZ_{T_{h+1}}$ produces different color values for each region.

$$IZ_{T_{h+1}} = \bigcup_{i=1}^k IZ_{T_{h+1}}(X_{h_i}) \quad (20)$$

Where I indicates an image. k is the number of minima and Z is indicated as $Z \in \text{Res}$ [22].

Individual gray level value can be defined to separate the regions on the image. The determination of these gray levels can be done as Region 1: RGB(20), Region 2: RGB(40), Region 3: RGB(50), Region 4: RGB(90) and Region 5: RGB(others)

V. EVALUATION OF ALGORITHM'S RESULTS

In order to compare the performance of COLMSTD algorithm with the other image processing algorithms, all algorithms are applied on 100 defective images. Regional, point and crack type defects are distributed as 90, 8, and 2 accordingly. Table 1 shows the ability of each algorithm to detect defects and identify the type of defects. It can be seen from the table that COLMSTD algorithm reveals better results than other methods. It detects all types of defects (i.e. crack, point and regional) whereas others can detect only one or two types. With Hough Transform algorithm, the objects having predetermined shape and size can be recognized. However, the possibility of surface defects having proper shape is very limited in rail images. This algorithm remains inadequate for non-uniform shape of defects on the rail images. MSER algorithm is used to identify regions on images. However, it is concluded that clear regional differences are needed for MSER. Watershed algorithm can also differentiate a region having different colored pixels. In our study, this method is found as more useful method in detection of the regional defects. However, in detection of point or line defects, it is not successful. Blob Detection method can only be used for the detection of point defects on the image, but not for other kinds of defects. In Table 1, the values are conducted for the images having defects ranging from 0.5 cm to 2.5 cm.

TABLE I COMPARISON OF ALGORITHMS

Algorithm Name	Defect Detection	Defect Types
DFT	Available	There is little information about defect location.
BLOB Detection	Available	Point defects, small crack and regional defects.
MSER	Available	Just regional defects.
Line Hough Transform	Available	Just crack defects.
Watershed	Available	Just regional defects.
COLMSTD	Available	Regional, point and crack defects.

Table 2 shows the detection ability of the algorithms, which are applied to an image having 1 point and 1 regional defect. COLMSTD algorithm achieves the most accurate results. It seems that other algorithms attain different number of defects than the actual number of defects.

TABLE II DEFECT DETECTION CAPABILITY OF ALGORITHMS

Algorithm Name	Number of Detected Point Defects	Number of Detected Regional Defect
MSER	0	1
Line Hough Transform	0	1
Watershed	0	1
DFT	1	1
BLOB Detection	13	0
COLMSTD	1	2

The performance values obtained from the applications are seen in Table 3. The algorithms are tested on 20 defective images consisting of 2 linear defective images, 5 point defective images and 13 regional defective images. It is seen that COLMSTD is the most effective method with 85% success rate in defect detection. Although DFT algorithm achieves a close performance, the defect location information cannot be obtained. On non-defective images, it is seen that COLMSTD has the highest success rate as 90%. The second most successful method is Line Hough Transform with 85% success rate. When we consider the both cases together it is seen that COLMSTD has the highest capability in detection of defect and defect location.

In order to see the performance of COLMSTD, the most successful algorithm, on different defect types, it was tested on 100 defective images. Regional, crack and point type of defects are distributed on the images as 49, 5 and 46 respectively. Defective images are randomly selected. Point Defects that created 1-3 pixels in the horizontal or vertical, Cracks (linear) defects has 2 pixels width or height as regular or irregular line appearance. The defect is also has more than 3 pixels width and height, the pixel group has been recognized as regional defects. COLMSTD algorithm performance is evaluated based on the results obtained.

TABLE III SUCCESS RATE OF THE ALGORITHMS ON DEFECT DETECTION

Algorithm Name	Success Rate on Defective Images (%)	Success Rate on Non-Defective Images (%)
DFT	80	60
BLOB Detection	35	5
MSER	60	10
Line Hough Transform	40	85
Watershed	65	80
COLMSTD	85	90

Table 4 shows the performance of COLMSTD algorithm if sensitivity coefficient is selected as 1.22. For the images having crack defect, the performance is 100% while it becomes 92% for the images having point defects. On the other hand, for the images having regional defects, success rate is 58%. Regional defect detection success is low since there are some regional defects that cannot be detected with the sensitivity of 1.22.

TABLE IV PERFORMANCE OF COLMSTD ALGORITHM

Defect Type	Number of Defective Images Used	Defect Detection Performance (%)
Crack	5	100
Point	46	92
Regional	49	58

The effect of sensitivity coefficients in COLMSTD algorithm is also examined by selecting the sensitivity coefficient between 0.8 and 1.22. The regional defect detection performances of COLMSTD for different coefficients are shown in table 5 for 100 defective images. Success rate for regional defect varies according to the selected sensitivity. Sensitivity coefficient of 0.8 achieves 97% success rate. This indicates the ability of the method to detect even the smallest defects. While the sensitivity coefficient increase, the success rate of recognizing regional defects decrease. If the coefficient is selected as greater than 1.22, the success rate will be comparatively less.

TABLE V REGIONAL DEFECT DETECTION PERFORMANCE OF COLMSTD ALGORITHM

Sensitivity Coefficient (hk)	Accuracy on Defective Images (%)	Accuracy on Non-Defective Images (%)
0.8	97	0
1.0	94	8
1.1	74	56
1.22	58	82

Other than success rate of detection, all algorithms are evaluated in terms of execution time performance. Defect detection period of each algorithm is given in Table 6 for the types of defect that they are able to detect. It can be seen that COLMSTD algorithm detects point and crack type defects in the shortest time. Regional defect is identified most quickly by the MSER. On the other hand the performance of the DFT is the worst among all 6 algorithms in terms of computation time.

TABLE VI DEFECT DETECTION TIME OF ALGORITHMS

Algorithm Name	Crack Defect (sec)	Point Defect (sec)	Regional Defect (sec)
DFT	0,234	0,167	0,202
Blob detector	-	0.156	-
MSER	-	-	0,134
Line Hough Transform	0.195	-	-
Watershed	-	-	0,163
COLMSTD	0,109	0,074	0,203

VI. CONCLUSION

In this study, an effective algorithm is developed for defect detection on the surface of the rail or the profile material. The images are taken from the rolling process of the material. This study targets for detection of all types of defects. According to the results, COLMSTD has the ability to detect all type of defects. The other

image processing algorithms applied show limited capabilities in defect detection. Some of the algorithms applied to gray value images directly could not produce reasonable results. For that reason, L_0 normalization process is used prior to applying DFT, MSER, Blob detection and Hough transform algorithms. On the other hand, results could be directly obtained by COLMSTD and Watershed without applying L_0 normalization algorithm.

The gray images of the rail or profile have different gray values for base, body and head parts. Better quality of the gray images will increase the success rate of obtaining accurate results. Detecting defects on the surfaces of rail is very important and necessary processing step. In gray values of defective bumps and pits must be apparently different from other regions. Otherwise, there will be probably loss of defects in filtering and cleaning stages. For that reason, temperature effect on the surface of the rolled rail and oscillating movement on the rail path must be minimal. Otherwise, non-defective regions can be regarded as defective and defective ones are non-defective.

It is foreseen that by making job sharing on a parallel system, defects can be quickly identified for complete rail. This will enable the implementation of the system in real time application. Future studies will focus on performing defect detection on the parallel system and conducting performance benchmark. The eligibility of using in the mill environment will be also examined.

REFERENCES

- [1] G. Wu, H. Zhang, X. Sun, J. Xu, K. Xu, "A Bran-new Feature Extraction Method and its application to Surface Defect Recognition of Hot Rolled Strips", IEEE International Conference on Automation and Logistics, pp. 2069-2074, 2007.
[Online]. Available: <http://dx.doi.org/10.1109/ICAL.2007.4338916>
- [2] K. Xu, C. Yang, "On-line Defect Detection Algorithms for Surface Inspection of Hot Rolled Strips", IEEE International Conference on Mechanic Automation and Control Engineering (MACE), pp. 2350-2353, 2010. [Online]. Available:
<http://dx.doi.org/10.1109/MACE.2010.5535586>
- [3] H. Jia, L. Y. Murphey, J. Shi, S. Chang, "An Intelligent Real-time Vision System for Surface Defect Detection", 17th International Conference on Pattern Recognition, vol. 3, pp. 239-242, 2004.
[Online]. Available: <http://dx.doi.org/10.1109/ICPR.2004.1334512>
- [4] B. Tang, J. Kong, X. Wang, L. Chen, "Surface Inspection System of Steel Strip Based on Machine Vision", First International Workshop on Database Technology and Applications, pp. 359-362, 2009.
[Online]. Available: <http://dx.doi.org/10.1109/DBTA.2009.133>
- [5] X. Deng, X. Ye, J. Fang, C. Lin, L. Wang, "Surface Defects Inspection System Based on Machine Vision", International Conference on Electrical and Control Engineering (ICECE), pp. 2205-2208, 2010. [Online]. Available: <http://dx.doi.org/10.1109/iCECE.2010.543>
- [6] G. Kang, L. Hong, "Surface Defects Inspection of Cold Rolled Strips Based on Neural Network", Proceedings of 2005 International Conference on Machine Learning and Cybernetics, vol. 8, pp. 5034-5037, 2005. [Online]. Available:
<http://dx.doi.org/10.1109/ICMLC.2005.1527830>
- [7] M. S'anchez, V. Vidal, J. Arnal, A. Vidal, "Image Noise Removal on Heterogeneous CPU-GPU Configurations", Procedia Computer Science, vol. 29, pp. 2219-2229, 2014. [Online]. Available:
<http://dx.doi.org/10.1016/j.procs.2014.05.207>
- [8] N. Neogi, D. Mohanta, P. Dutta "Review of vision-based steel surface inspection system", Journal on Image and Video Processing (EURASIP), vol 50, 2014. [Online]. Available: <http://dx.doi.org/10.1186/1687-5281-2014-50>
- [9] H. Zhai, H. Huang, S. He, W. Liu, "Rice Paper Classification Study Based on Signal Processing and Statistical Methods in Image Texture Analysis", International Journal of Software Innovation, vol. 2, no. 3, pp. 1-14, 2014. [Online]. Available:
<http://dx.doi.org/10.4018/ijsi.2014070101>
- [10] M. Elad, "Sparse and Redundant Representations - From Theory to Applications in Signal and Image Processing", pp. 12-46, Springer Press, 2010.. [Online]. Available:
<http://dx.doi.org/10.1007/978-1-4419-7011-4>
- [11] L. Xu, C. Lu, Y. Xu, J. Jia, "Image Smoothing via L_0 Gradient Minimization", ACM Transactions on Graphics, vol. 30, no. 6, pp. 1-11, 2011. [Online]. Available: <http://dx.doi.org/10.1145/2070781.2024208>
- [12] L. Shapiro, G. Stockman, "Computer Vision", pp. 160-200, Prentice Hall Press, 2001.
- [13] F. Wang, R. Xiangshi, L. Zhen, "A Robust Blob Recognition and Tracking Method in Vision-based Multitouch Technique", International Symposium on Parallel and Distributed Processing with Applications (ISPA), pp. 971-974, 2008.
[Online]. Available: <http://dx.doi.org/10.1109/ISPA.2008.129>
- [14] D. Ravipati, P. Karreddi, A. Patlola, "Real-time Gesture Recognition and Robot control through Blob Tracking", IEEE Students' Conference on Electrical, Electronics and Computer Science (SCEECS), pp. 1-5, 2014. [Online]. Available:
<http://dx.doi.org/10.1109/SCEECS.2014.6804526>
- [15] F. Kristensen, J. W. MacLean, "Real-Time Extraction of Maximally Stable Extremal Regions on an FPGA", IEEE International Symposium on Circuits and Systems, pp. 165-168, 2007.
[Online]. Available: <http://dx.doi.org/10.1109/ISCAS.2007.378247>
- [16] M. Donoser, H. Bischof, "Efficient Maximally Stable Extremal Region (MSER) Tracking," IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR), pp. 553-560, 2006. [Online]. Available: <http://dx.doi.org/10.1109/CVPR.2006.107>
- [17] A. Herout, M. Dubská, J. Havel, "Real-Time Detection of Lines and Grids By PC lines and Other Aproaches", pp. 3-54, Springer Press, 2013. [Online]. Available: <http://dx.doi.org/10.1007/978-1-4471-4414-4>
- [18] D. H A. Ballard, "Generalizing The Hough Transform to Detect Arbitrary Shapes", Pattern Recognition, vol. 13, no. 2, pp. 111-122, 1981. [Online]. Available:
[http://dx.doi.org/10.1016/0031-3203\(81\)90009-1](http://dx.doi.org/10.1016/0031-3203(81)90009-1)
- [19] G. Bradski, A. Kaehler, "Learning OpenCV Computer Vision with the OpenCV library", pp. 295-297, O'Reilly Media Press, 2008.
- [20] H. Sun, J. Yang, M. Ren, "A fast watershed algorithm based on chain code and its application in image segmentation", Pattern Recognition Letters, vol. 26, no. 9, pp. 1266-1274, 2005. [Online]. Available: <http://dx.doi.org/10.1016/j.patrec.2004.11.007>
- [21] J.B.T.M. Roerdink, A. Meijster, "The Watershed Transform: Definitions, Algorithms and Parallelization Strategies", Fundamenta Informaticae, vol. 41, no. 1-2, pp. 187-228, 2000. [Online]. Available: <http://dx.doi.org/10.3233/FI-2000-411207>
- [22] L. J. Belaid, W. Mourou, "Image Segmentation: A Watershed Transformation Algorithm", Image Analysis & Stereology, vol. 28, no. 2, pp. 93-102, 2009. [Online]. Available:
<http://dx.doi.org/10.5566/ias.v28.p93-102>

Investigating the opportunities of using mobile learning by young children in Bulgaria

Radoslava Kraleva[#], Aleksandar Stoimenovski[#], Dafina Kostadinova^{*}, Velin Kralev[#]

[#] Department of Informatics, South West University "Neofit Rilski", Blagoevgrad, Bulgaria

^{*} Department of Germanic and Romance Studies, South West University "Neofit Rilski", Blagoevgrad, Bulgaria

Abstract – This paper provides an analysis of literature related to the use of mobile devices in teaching young children. For this purpose, the most popular mobile operating systems in Bulgaria are considered and the functionality of the existing mobile applications with Bulgarian interface is discussed. The results of a survey of parents' views regarding the mobile devices as a learning tool are presented and the ensuing conclusions are provided.

Keywords – Mobile learning, Mobile learning application, Analysis of the parents' opinion

I. INTRODUCTION

Mobile technologies have significantly changed the life of modern society. Nowadays, most people have not only a phone, but most often they use a smart phone, a tablet and computer as well. These devices are considered as mobile devices¹ and portable devices². Mobile devices most often have their own mobile operating system approaching closer to the operating system³ desktop and portable computing devices.

These lightweight, comfortable and compact mobile devices are attractive to children. They use them for gaming, watching movies, listening to music, chatting with friends and communicating with the global world. However, all these features are controlled only by a few taps. There is no need to use any additional keyboard or mouse. Children grow up with all these devices around them and acquire their usage before they have started to speak or walk.

The rapid development of hardware and software technologies is a prerequisite for many new ways of using them in modern life [1]. This resulted in adopting a new concept in training called ubiquitous learning (U-learning) which combines traditional classroom training and the possibility of

access to educational resources on the Web anytime and anywhere [2], [3], [4]. A number of scientists, psychologists, educators and software developers focused their attention on this new kind of education for children based on applications for mobile and portable devices [5].

On this background the main goal of this study is to research and analyze the usage of mobile devices in the education of young children in Bulgaria. The tasks of this study are:

- To review the most commonly used mobile operating systems in Bulgaria, as well as the possibility of using the existing applications with interface in the Bulgarian language in the training of young children;
- To make an overview of the scientific publications on the topic related to the use of mobile learning;
- To analyze the opinions of parents regarding the use of applications for mobile devices in the education of their children in Bulgaria.

II. APPLICATIONS FOR MOBILE DEVICES WITH BULGARIAN INTERFACE FOR CHILDREN

There are three competing mobile operating systems, Android of Google Inc., Windows Phone and iOS of Microsoft to Apple (Fig. 1) on the Bulgarian markets. Every day users around the world download thousands of apps from the market of these operating systems. Developers rapidly create new and new applications that are added to various markets to meet the needs of consumers.

According to the statistics provided by Microsoft last year [7], there were 669,000 applications in the Windows Store and hundreds of new ones were added every day. This is a small number compared to the markets of Google and Apple.

¹ *Mobile devices* – These are all wireless devices with their own operating system, and using Wi-Fi, 3G or 4G internet connection.

² *Portable devices* – These are laptops, notebooks, netbooks, ultrabook.

³ *Mobile operating systems* – Operating systems for mobile devices.

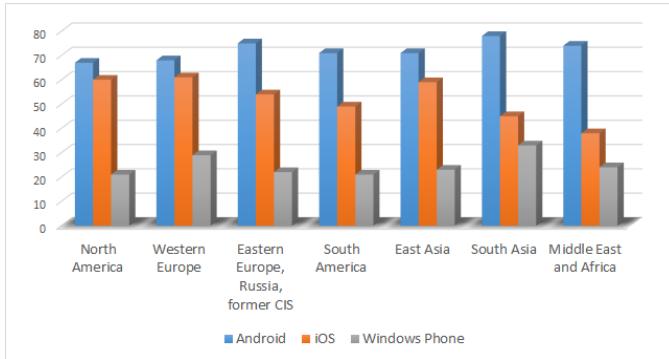


Figure 1. Selected mobile platforms used by app developers worldwide as of 1st quarter 2014, by region [6]

The statistics provided by Gartner Inc. [8] reveals that a large proportion of the downloaded applications belongs to the applications for free downloads versus paid applications (Fig. 2).

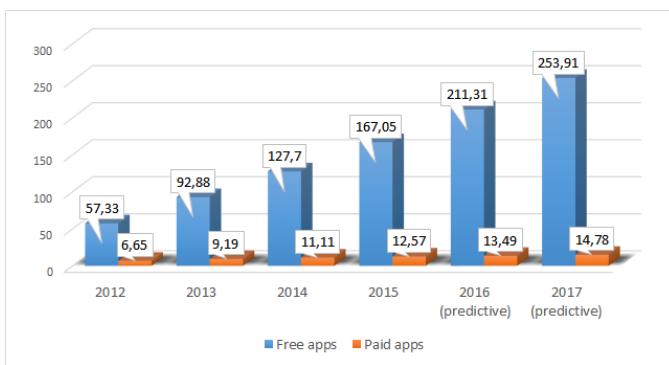


Figure 2. The number of downloaded free and paid mobile applications for the period 2012 to 2017 (2017 is predictive) according to Gartner [8]

As it can be seen from the diagram (Fig. 2), most companies and independent developers and users rely on free apps. Often to achieve higher profits other techniques are applied such as adding unwanted ads to free applications, additional modules for which the consumer must pay. In most cases, all applications require a continuous connection to the Internet.

Most downloaded mobile applications refer to games or some other kind of entertainment. Small is the share of software for learning. And even less of it can be used safely by young children, as most of the free applications include pop-up ads or paid modules.

Some of the applications that could be used in teaching young children and are available at Google Play are: "Kids Numbers and Math FREE" (free; studying numbers, counting to 20, addition, subtraction; aged 4 to 6 years); "Number Games: Math for Kids" (Free; Studying objects, shapes, time, numbers, multiplication, division, addition and subtraction; Aged 6 to 10 years); „Baby Puzzles“ (Free; Recognition of shapes and developing fine motor skills; Aged 0 to 3 years); "LetterSchool free - write abc" (Free; Studying writing uppercase and lowercase letters and numbers up to 10; Aged 0 to 6 years); "Game Kids free 3" (Free; Studying objects,

numbers and letters connecting the dots, development of memory and logic; Aged 0 to 6 years) and many others.

Many of these applications are free for download, but the modules providing more features are paid. In the above applications the problem that appears is that there is no support for the Bulgarian language and some games require the assistance of the parent. In other applications, the child is not able to use them at all since a good command of English is needed.

However, applications in the Bulgarian language were also found on Google Play such as „Букви, цифри, цветове Безплатно“ /Letters, figures, colors Free/ (Free; learning letters, numbers and colors; Aged 0 to 6 years), „БГ Срички“ /BG Syllables/ (Free; Studying writing and pronunciation of Bulgarian words; Aged 2 to 8 years), „Уча АБВ“ /Learn ABC/ (Paid; Study the style of writing Bulgarian letters; Aged 2 to 8 years); „БГ Буквар“ /BG Primer/ (Free; Learning the letters; Aged 0 to 6 years), and others.

In these applications what is considered as a problem is the presence of unwanted ads and limited functionality compared to alternative applications in English. Many of parents' comments regarding the applications are negative and disapproving, which leads to bad rating of the applications.

On the same date in Apple's App Store a number of applications of the type listed above were found; they had the problem of language and ads. Here applications with support for Bulgarian language that can be used in teaching children at an early age were discovered, too. Such are the „Буквите“ /The letters/ (Paid; Pronunciation and spelling of words; Aged 0 to 6 years), „Мозайка“ /Mosaic/, „Българските букви и цифри“ /The Bulgarian letters and numbers/ (Free; Knowledge of letters, numbers and colors; Aged 0 to 6 years), „Букви с витамини“ /Alphabet of vitamins/ (Paid; Pronunciation and writing of letters; Aged 0 to 6 years) and others. No applications associated with the development of mathematical knowledge in children with Bulgarian language interface were found.

Some applications were found in Windows Store which can be used in the training of young children. Such are the "Kids Play & Learn" (Free; Learning the colors, objects, numbers, sounds, time, mathematics, puzzles and languages; Suitable for all ages), "Kids Play Math" (Free; Studying of the numbers and simple math with addition, subtraction, multiplication and division; Aged 0 to 12 years), "Baby Play & Learn" (Paid; Promotes the study of flowers, animals, fruits and objects; Aged 0 to 3 years), "MeSchoolTeacher" (Free; Studying of the numbers, letters and objects; Aged 0 to 17 years), "Kids Preschool Learning Games" (Paid; Studying of the mathematics, numbers, letters, words, objects; Ages 3 to 6 years) and many more. All reviewed applications are supported mainly in English (United States); some of them use several languages, German, Spanish, Russian, but these applications do not support the Bulgarian language.

The wide variety of different and no so much different applications in the stores of Android, Apple and Microsoft lead to the unpleasant trend presented in [9], according to which

more and more children in the US spend more time playing on a mobile device, instead of doing some sport or reading books.

As a result of the research presented in this section, it can be concluded that there are still problems related to the quality development of applications for mobile learning. Moreover, in most cases, developers seek quick profits by relying on advertisers or paid modules.

III. TEACHING TO STUDENTS THROUGH MOBILE DEVICES

Over the past few years there has been an increasing interest in the application of non-standard approaches to teaching. Such approaches are based on the use of mobile applications for science learning. Detailed analysis of the design, feasibility and the results achieved by students, when using mobile learning (M-learning,) is presented in [10]. The authors of this paper would recommend more research on mobile learning applications, e.g., using them with more varied science topics and diverse audiences.

In [11] a survey based on more than 110 references in regard to the benefits of using various mobile devices such as laptops, mobile phones and other in the learning process has been done. Based on this, a number of conclusions have been drawn. This paper does not provide any survey of parents of young children who are going to use such devices in their future learning and for various types of entertainment as well.

In [12] the application Mobile Plant Learning Systems is presented; it is used in elementary schools in Taiwan. This software is related to learning in an elementary-school-level botany course, in particular, the classification and detailed information of the different types of plants. The access to the information is through Wi-Fi, and the mobile operating system used is Microsoft Windows Mobile 5.0 Pocket PC Phone Edition. This application is installed on personal digital assistants (PDAs) and the access to the necessary training materials is at any time, regardless of the location of students and teachers. In [12] the effectiveness of the mobile learning is investigated, a survey to obtain feedback from students has been done as well.

Another mobile learning application "ThinknLearn", assisting students in high school to create hypotheses is presented in [13]. Positive results from its practical use in obtaining new knowledge and stimulating deductive thinking in students are observed.

In [14] the opinion of students from preschool to 12th grade (3 to 18 years old) and their parents of the use of mobile devices in the course of their studies is discussed. The data of 2392 parents and 4164 children are processed; children are categorized by gender and age.

In [15] the effects of m-learning, by tracking the development of cognitive skills of young children using the mobile application "Jungle Adventure", for Android and iOS is presented. The working languages of this application are 4 (English, French, German and Spanish). A survey was conducted among 56 children aged 2 to 4 years through the analysis of an independent psychologist. They had to fill in a

survey at the beginning of the experiment and every day for three weeks after using the app for about 7.5 minutes. The results showed that about 38% of children have improved cognitive knowledge of colors, letters, objects.

As a result of this study, which cannot be exhaustive enough, it can be concluded that at present very few studies related to young children and their achievements when learning with mobile technologies (M-learning) are available. As a matter of fact, such a study has never been done before in Bulgaria. Therefore, we can say that this is an interesting problem area that is to be analyzed and developed.

IV. RESEARCH AND ANALYSIS OF THE PARENTS' OPINION

Studying the parents' opinion in Bulgaria is important to determine the possibility of implementing mobile learning from early childhood.

Similar analysis of the parents' opinion in the USA, who have at least one child in preschool, is made in [9]. Also, the quality of the education received in the target group, consisting of 90 children, aged 3 to 7 years is evaluated.

From the above mentioned sources one can conclude that the role of parents in the education of children and the successful use of applications for mobile devices in this process are closely related. Therefore, the study of parents' attitudes in Bulgaria on this important issue is of great significance.

To examine the opinion of parents of children under the age of 10 a questionnaire has been developed. It consists of 17 questions: 2 of them are free response, all the others are closed.

The opinion of 50 parents of 64 children, of which 76% have one child, 20% have two children, and the remaining 4% have more than 2 children, is investigated.

The age of their children is shown in Figure 3. As it can be seen from the diagram, most of them are at the age of 4 to 7 years (65%). 16 % of all children are 1 to 2 years of age. There are no children with special educational needs among them.

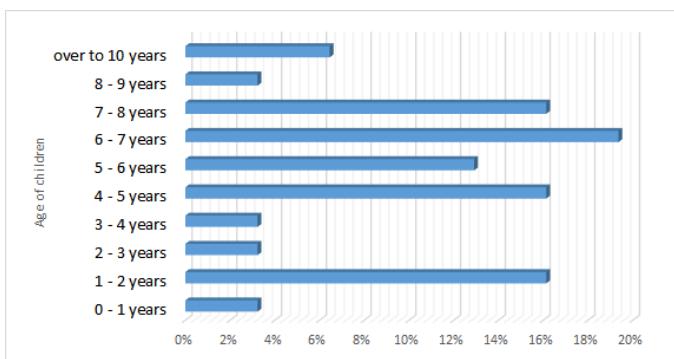


Figure 3. Age of the children of the surveyed parents

In Bulgaria some parents of children aged 0 – 2 years prefer to look after them on their own not using the service of the nursery schools; other parents decide that their children would not attend the afternoon classes of the preschool. It should be noted that full-time education in elementary school in Bulgaria is not mandatory. Only 24% of the children of the surveyed

parents do not attend any school, because this category includes the children up to age 2 whose parents raise and educate them at home. 24% of children attend school half-day, and 52% - an all-day school.

All interviewed parents confirmed that they devote time for further training of their children at home in order to enhance and consolidate the knowledge instructed at school.

This result points to the fact that parents are an essential part of the learning process of children and the development of any innovative training tools must be presented to a wide range of parents or they can even participate in their preparation and creation.

Like the parents from the surveyed literature from different parts of the world, all parents surveyed in Bulgaria allow their children to use computer devices, including mobile devices, regardless of the age of their children.

The period of time that children can use these devices authorized by the surveyed parents is different (Fig. 4). 64% of parents agree that the optimum time is within two hours per day and 20% of them believe that the best period of time should be reduced to one hour a day.

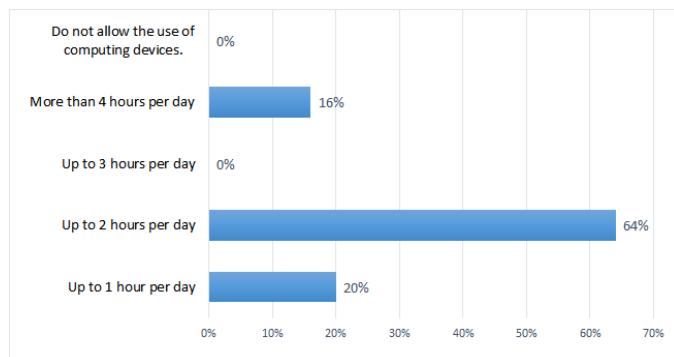


Figure 4. The period of time during which children can use the computer device

Most of the families in our survey have different computing devices. This can be seen from the diagram shown in Figure 5 which shows the type of different devices parents allow their children to use. The results here are slightly different from those reported at the beginning of the section.

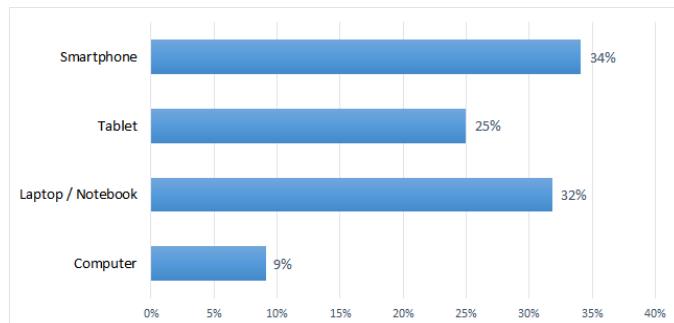


Figure 5. The types of computing devices that children can use

This is due to the fact that in Bulgaria, not every child has its own smartphone or tablet, and in most cases he/she uses

their parents' devices. The same is true for desktops or portable devices. This is due to the great parental caution related to the safety of children using different computing devices and growing up in good health.

According to the survey of the parents' opinion, 42% of the children use the computer gaming devices, 33% for education and 25% for access to multimedia information such as pictures, music and video (Fig. 6).

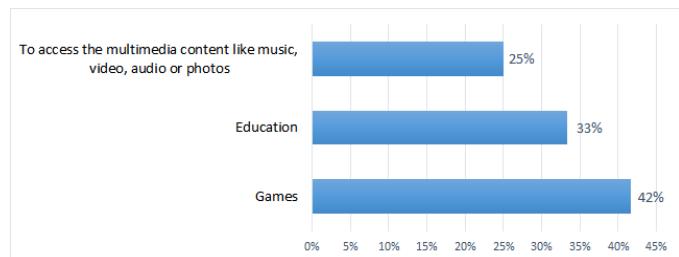


Figure 6. Activities for which children most often use computing devices

The operating systems of computing devices that children use are as follows: Android (46%) of Google, Windows (43%) of Microsoft and iOS (11%) of Apple. In this way it is easier to gauge consumer preferences and accordingly, for which operating system an application for mobile learning of young children with interface in Bulgarian to be developed.

The opinion of parents on the applications available for free download in stores on Google, Microsoft and Apple has been investigated. Some parents have responded with more than one answer. The results are rather varied (Fig. 7). The greatest dissatisfaction among the 32% of parents caused the presence of pop-up ads that appear during the use of the application. One solution to this problem is the development of applications without access to the Internet. According to 29% of the parents, another drawback is the lack of support for Bulgarian language in most of the available applications.

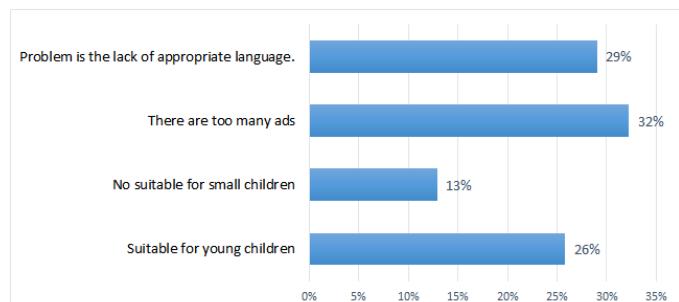


Figure 7. Opinion on the interface and functionality of applications available for free download in stores on Google Play (Google), Windows Store (Microsoft) and App Store (Apple) for the education of young children in Bulgarian

An interesting trend in the responses (Figure 6.5) is observed: 26% of the parents believe that there are mobile applications suitable for young children. These parents claim that their children must learn the English language in their early childhood and use it. This is supported by the results obtained here regarding language of the interface their children use. The

parents have found that 79% of the applications are in English, 14% in Bulgarian and 7% in other languages.

Furthermore, 92% of all surveyed parents support the idea of using mobile learning in the Bulgarian language, and 64% of them express their positive comments and recommendations. Some of these comments are presented in Table 1.

TABLE I. COMMENTS OF PARENTS ON THE USE OF MOBILE LEARNING IN BULGARIAN

	Comments of parents
1	"It will greatly help in the learning process."
2	"Great idea!"
3	"I agree that it is necessary to have such software!"
4	"The idea is good and it will be something new and interesting for children."
5	"Modern education needs of such software for mobile learning."
6	"Such software is absolutely essential!"

As a result of the present research we may firmly state that 64% of the parents support the education of children by using mobile learning and would be happy to use them in their daily routines. This will ensure complete use of the mobile devices that are up to date and can easily be updated and provide additional knowledge for children. Furthermore, the training will not depend on the location, light, and body position. In this way more freedom of learning is provided and the stress of school and conventional learning can be avoided.

V. CONCLUSION

In this paper we have reviewed the available applications for mobile devices connected to the educational process of young children. We have classified their functionality and user interface. An analysis of the current literature sources related to the use of mobile devices in teaching young children has been made. A questionnaire survey of parents' opinions concerning the use of applications for mobile phones as a tool for mobile learning has been supplied. The obtained results have been duly presented, analyzed and summarized.

Modern technologies are the tool with the help of which products related to e-learning, M-learning and U-learning are developed. They are a requirement and of great benefit to overcome the barrier of time and space related to knowledge providers and to increase the access to current information. Sometimes the way of providing knowledge depends on the curricula and the different ways of building a mobile learning system. Therefore, when building such systems one should

seek to disregard the influence of the technology used on the quality accessible presentation of the targeted educational material. Furthermore, any such system must provide a safe and secure environment for children.

REFERENCES

- [1] Z. Cheng, S. Shengguo, M. Kansen, T. Huang, T. and H. Aiguo, "A personalized ubiquitous education support environment by comparing learning instructional", in proceedings of 19th international conference on advanced information networking and applications (AINA 2005), pp. 567–573, Los Alamitos, CA: IEEE Computer Society, 2005
- [2] Y. M. Huang, Y. L. Jeng and T. C. Huang, "An educational mobile blogging system for supporting collaborative learning", journal of Educational Technology and Society, vol. 12, issue 2, pp. 163–175, 2009
- [3] M. Virvou, E. Alepis, "Mobile educational features in authoring tools for personalized tutoring", Computers and Education, vol. 44 (1), pp. 53–68, 2005
- [4] Y. E. Hashim, A. Osman, A. El-Gelany Mobile Technology and Education: Theoretical Study, International Research Journal of Computer Science, issue 02, vol. 3, 2016
- [5] M. F. Lin, C. P. Fulford, C. P. Ho, R. Iyoda, & L. K. Ackerman, Possibilities and challenges in mobile learning for K-12 teachers: a pilot retrospective survey study. In Proceedings of the seventh IEEE international conference on wireless, mobile and ubiquitous technology in education (WMUTE'12), Takamatsu, Kagawa, Japan: IEEE Computer Society, pp. 132–136, 2012
- [6] Statista, "Selected mobile platforms used by app developers worldwide as of 1st quarter 2014", <http://www.statista.com/>
- [7] Microsoft, <http://news.microsoft.com/bythenumbers/store-downloads> [accessed Desember 5, 2015]
- [8] Gartner, Inc., <http://www.gartner.com/technology/home.jsp> [accessed October 2, 2015]
- [9] C. Chiong, C. Shuler, "Learning: Is there an app for that? Investigations of young children's usage and learning with mobile devices and apps", New York: The Joan Ganz Cooney Center at Sesame Workshop, 2010
- [10] J. M. Zydney, Z. Warner, "Mobile apps for science learning: Review of research", journal of Computers and Education, vol. 94, pp. 1-17, 2016
- [11] Y. T. Sung, K. E. Chang, T. C. Liu "The Effects of Integrating Mobile Devices with Teaching and Learning on Students' Learning Performance: A Meta-Analysis and Research Synthesis", International Journal Computers and Education, Elsevier, 2015
- [12] Y. M. Huang, Y. T. Lin, S. C. Cheng "Effectiveness of a Mobile Plant Learning System in a science curriculum in Taiwanese elementary education", International Journal Computers and Education, 54, Elsevier, pp. 47-58, 2010
- [13] S. Ahmed, D. Parsons, "Abductive science inquiry using mobile devices in the classroom", journal Computers and Education, Elsevier, pp. 62-72, 2013
- [14] Grunwald Associates LLC, "Living and Learning with Mobile Devices: What Parents Think About Mobile Devices for Early Childhood and K-12 Learning", 2013, https://www.corp.att.com/edu/docs/mobile_kids.pdf [Accessed April 6, 2016]
- [15] EmeeYou, "White Paper", 2012, http://www.emeyou.com/wp-content/uploads/2012/11/emeeyou_white_paper_04112012.pdf [accessed February 29, 2016]

Conducting multi-class security metrics from Enterprise Architect class diagram

Osamah S. Mohammed

Dept. of Software Engineering

College of Computer Sc. & Math, University of Mosul.
Mosul, Iraq.

Dujan B. Taha

Dept. of Software Engineering

College of Computer Sc. & Math, University of Mosul.
Mosul, Iraq.

Abstract— Developers often neglect security until the end of developing the software just after coding, and any change in the code with respect to security may lead to change in the software code, this consumes time and cost depending on the software size. Applying security on a software late in its SDLC may result in many security flaws, some of them can involve serious architectural issues. Applying security metrics on design phase can reveal the security level and fix vulnerabilities of a software earlier in the project. In this work, security metrics has been discussed, and conducting these metrics from Enterprise Architect class diagram using a proposed CASE tool.

Keywords-Software Engineering; Security metrics; Enterprise architect; Class diagram; SDLC; Design phase

I. INTRODUCTION

Software that does not exhibit a high quality is easier to hack, and as a consequence, low-quality software can indirectly increase the security risk with all of its attendant costs and problems. To build a secure system, we must focus on quality, and that focus must begin during design [1]. As Willoughby said “You must think about security, reliability, availability, dependability at the beginning, in the design, architecture, test and coding phases, all through the software life cycle” [2]. Applying security in the design phase of SDLC can reduce a large number of defects and security vulnerabilities before coding. Most security vulnerabilities result from flaws that are introduced in the software during design and development. Therefore, to significantly reduce software vulnerabilities, the overall defect content of software must be reduced. Security must be designed and built into a system from the ground up. According to the CERT Coordination Center (CERT/CC) of the SEI, more than 90% of reported security incidents are the result of exploits against defects in the design or development flaws [3]. Metrics help the developers to manage the software as well as the software development process. Metrics can help to detect and analyze the software functionality and correct them during the software development process.

In this work, we discuss the security metrics that is applied on design phase of the software life cycle which will help in identifying potential security flaws and how it could help reducing them before start coding the software. This will help reducing the total amount of time and cost spent on managing and applying security later on the project.

A proposed CASE tool has been used to conduct the security metrics from a class diagram designed using Enterprise Architect.

II. BACKGROUND

Security metrics are being widely used to measure the security level and try to fix any vulnerabilities, but most of these metrics were used at source coding which is considered late in the SDLC. Ram and Alagarsamy proposed a set of security metrics which can measure the method level security through the source code [4]. I. Chowdhury, B. Chan, and M. Zulkernine proposed a code-level security metrics which can be used to suggest the level of security of a code segment [5]. Alshammari proposed a set of security metrics which can assess the security level and reveal security vulnerabilities from a class diagram in design phase of the software development life cycle [6]. Assessing security metrics and fixing security vulnerabilities at design phase will decrease a large amount of security flaws which may appear while coding or after deployment of the software. It measures any potential information flow between objects instantiated the design's classes [6]. To measure the security metrics for a class diagram, some additional annotations are required to help express information flow between methods and attributes in a given class or to express information flow between the classes through class diagram relations. For this metric, UMLsec and SPRAK's annotation are used to express this information flow. UMLsec annotations consist of using ‘secrecy’ label as a stereotype for each confidential attribute in a class, and ‘critical’ label as a stereotype for each class containing at least one confidential attribute in a class diagram [7]. SPARK is programming language, which can be defined as “a programming language designed for security-critical code in which the programmer may annotate subroutines with the intended data flow between variables and parameters” [8]. ‘derives from’ block is used as one of the SPARK’s annotations which explains how the flow of values are going from methods and attributes, and show which variable are being accessed or mutated in each method [8]. Using this block will help these metrics to detect information flow between different classes and between methods and attributes.

Enterprise Architect (EA) is a UML CASE tool used for analysis and design of a software. It's used to cover all aspects of software including business, systems modeling and design, [9]. Designing automated security metrics tool is relatively easy, because EA can export a diagram as an (.XML) file which can be easily interpreted for use of automated processing on that diagram. The XML file contains all the details needed to elicit and calculate security metrics using XML file parser. A sample XML file is shown in Figure 1, Class Diagram XML Structure., exported from a class diagram from EA.

```
<UML:Class name="Session" xml:id="E4ID_08913F48_991E_45e4_B66D_C6371A4C8F80" visibility="public" namespace="EAPK_2EB8C8A8_950F_437b_A0EF_B0AAEAE8349" isRoot="false" isLeaf="false" isAbstract="false" isActive="false">
    <UML:ModelElement.stereotype>
        <UML:TaggedValue tag="specification" value="true1"/>
    </UML:ModelElement.stereotype>
    <UML:ModelElement.taggedvalue>
        <UML:TaggedValue tag="isSpecification" value="false"/>
        <UML:TaggedValue tag="e_stereotype" value="class"/>
        <UML:TaggedValue tag="e_type" value="0"/>
        <UML:TaggedValue tag="version" value="1.0"/>
        <UML:TaggedValue tag="package" value="EAPK_2EB8C8A8_950F_437b_A0EF_B0AAEAE8349"/>
        <UML:TaggedValue tag="date_created" value="2016-03-01 14:17:55"/>
        <UML:TaggedValue tag="date_modified" value="2016-03-18 18:27:02"/>
        <UML:TaggedValue tag="genotype" value="true2"/>
        <UML:TaggedValue tag="tagged" value="0"/>
        <UML:TaggedValue tag="package_name" value="Diagram OO D 1"/>
        <UML:TaggedValue tag="phase" value="1.0"/>
        <UML:TaggedValue tag="author" value="Osama"/>
        <UML:TaggedValue tag="complexity" value="1"/>
        <UML:TaggedValue tag="status" value="Proposed"/>
    </UML:ModelElement.taggedvalue>
</UML:Class>
```

Figure 1, Class Diagram XML Structure.

III. SECURITY METRICS

Security metrics for multi-class design aim to assess the information-flow security of an object-oriented design. It uses five properties of the design of an object-oriented program which is: composition, coupling, extensibility, inheritance, and design size. These metrics measure potential information flow between objects derived from its class diagram according to security design principles of reducing attack surface and the least privilege [6].

A. Composite-Part Critical Classes (CPCC):

This metric is defined as “The ratio of the number of critical composite-part classes to the total number of critical classes in a design” [6]. This metric is expressed as:

$$CPCC(D) = 1 - \left(\frac{|CP|}{|CC|} \right) \quad (1)$$

Where CP is the number of composite-part critical classes in design D and CC is the total number of critical classes in the same design.

B. Critical Classes Coupling (CCC)

This metric is defined as “The ratio of the number of all classes' links with classified attributes to the total number of possible links with classified attributes in a given design” [6]. This metric is expressed as:

$$CCC(D) = \frac{\sum_{j=1}^{ca} \alpha(CA_j)}{(|C| - 1) \times |CA|} \quad (2)$$

Where $\alpha(CA_j)$ is the number of classes which may interact with classified attribute CA_j in design D, C is the number of classes, and CA is the total number of classified attributes in the same design.

C. Critical Classes Extensibility (CCE)

This metric is defined as “The ratio of the number of the non-finalized critical classes in a design to the total number of the critical classes in that design” [6]. It can be expressed as:

$$ECC(D) = \frac{|ECC|}{|CC|} \quad (3)$$

Where ECC is the number of critical extensible classes and CC is the total number of critical classes in the design.

D. Classified Method Extensibility (CME)

This metric is defined as “The ratio of the number of the non-finalized classified methods in a design to the total number of classified methods in that design” [6]. It's expressed as:

$$CME(D) = \frac{|ECM|}{|CM|} \quad (4)$$

Where ECM is the number of extensible classified methods in design D and CM is the number of classified methods in the same design.

E. Critical Superclasses Proportion (CSP)

This metric can be defined as “The ratio of the number of critical Superclasses to the total number of critical classes in an inheritance hierarchy” [6]. Its equation is as follow:

$$CSP(H) = \frac{|CSC|}{|CC|} \quad (5)$$

Where CSC is the number of critical superclasses in design D and CC is the number of critical classes in a hierarchy located in the same design.

F. Critical Superclasses Inheritance (CSI)

This metric is defined as “The ratio of the sum of classes which inherit from each critical superclasses to the number of possible inheritances from all critical classes in a class hierarchy” [6]. This metric is expressed as:

$$CSI(H) = \frac{\sum_{k=1}^{csc} \beta(CSC_k)}{(|C| - 1) \times |CC|} \quad (6)$$

Where $\beta(CSC_k)$ is the number of classes which may inherit from the critical superclass CSC_k , C is the number of classes, and CC is the number of critical classes in a hierarchy located in the design.

G. Classified Methods Inheritance (CMI)

This metric is defined as “The ratio of the number of classified methods which can be inherited in a hierarchy to the total number of classified methods in that hierarchy” [6]. It's expressed as:

$$CMI(H) = \frac{|MI|}{|CM|} \quad (7)$$

Where MI is the number of classified methods which could be inherited in the hierarchy, and CM is the number of classified methods in the same hierarchy.

H. Classified Attributes Inheritance (CAI)

This metric is defined as “The ratio of the number of classified attributes which can be inherited in a hierarchy to the total number of classified attributes in that hierarchy” [6]. It’s expressed as:

$$CAI(H) = \frac{|AI|}{|CA|} \quad (8)$$

Where AI is the number of classified attributes which could be inherited in the hierarchy, and CA is the number of classified attributes in the same hierarchy.

I. Critical Design Proportion (CDP)

This metric measures the impact of the size of a certain design size. Its defined as “The ratio of the number of critical classes to the total number of classes on a design” [6]. It’s expressed as:

$$CDP(D) = \frac{|CC|}{|C|} \quad (9)$$

Where C is the number of classes and CC is the number of classes in the same design.

IV. PROPOSED CASE TOOL

The proposed tool is a webapp CASE tool used to calculate specific-class and multi-class security metrics, which can be accessed with any device which contains an internet connection and a web browser. Users can register and access the functionalities of this tool, such as: uploading an XML file exported from EA to process and save the results into the database; and viewing the results of the diagrams. This tool can process a class diagram exported from EA as an XML file, and the class diagram has to be annotated with UMLsec and SPARK’s annotations. The architecture of this tool is shown in Figure 2. New users can register and login as a regular user, the user can view the last uploaded diagrams metrics which consist of design security metrics and specific class metrics as shown in Figure 3 and Figure 4. A user can design a class diagram with different variation of a class, the tool will help the user to calculate, view, and easily compare these classes to select the most secure class. The use of this tool can reduce the total cost of a project by reducing the number of vulnerabilities discovered in the design phase, which reduces a large number of potential security vulnerabilities and flaws that may be discovered late in the project.

V. CASE STUDY

In this case study, different variation of a class diagram has been designed for a webapp user information system. As shown in Figure 6, this system is responsible for managing the access and storing information of a user to the system. A user can log-in the system as a regular user or as an admin. Each user has a confidential data in its class such as the password,

sault of the password and the database connection. The session class is concerned about managing each user’s session which has confidential data in it such as sessionId, sessionHash and mysql.

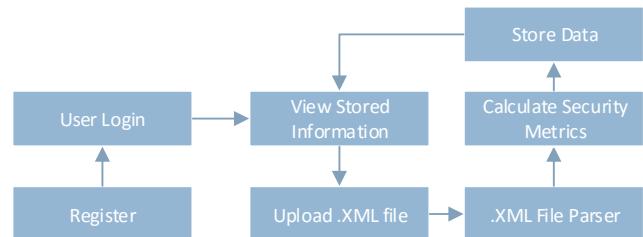


Figure 2, Proposed tool Architecture.

No.	Diagram Name	Class count	CPCC	CCC	CCE	CME	CDP	Details	Actions
1	Design 1	5	0.67	0.071	1	1	0.6		
2	Design 2	6	0.75	0.044	1	1	0.67		
3	Design 3	4	1	0.056	1	1	0.75		
4	Design 4	3	1	0	0	0	0.33		

Figure 3, Proposed tool Main Page.

- Design 2						
Diagram Name	CPCC	CCC	CCE	CME	CDP	
Design 2	0.75	0.044	1	1	0.67	

You have 4 Classes.							
No.	Class Name	CIDA	CCDA	COA	CMIAI	CAAI	CAIW
1	MySQL	0	0	1	0	1	1
2	Person	0	0	0.33	0.67	0.6	1
3	Session	0	0	1	0.5	0.33	1
4	User	0	0	1	0.67	0.27	0.45

No.	Hierarchy Top Level Class Name	CSP	CSI	CMI	CAI
1	User	0.5	0.5	0.25	0.6

Figure 4, Specific Design Results.

Upload your diagram

Please note that the diagram must follow the standards UMLsec and Spark’s annotations.
You can follow this [guide](#).

Fill the form

Please select your diagram XML file.

Select file

Save results in database?

upload

Figure 5, Upload Form.

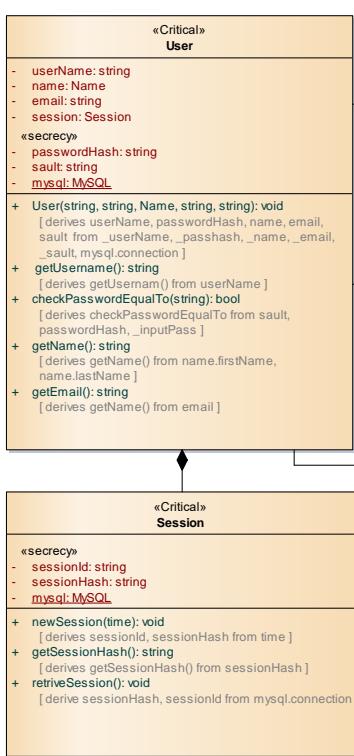


Figure 6, Webapp User Information System Design 1.

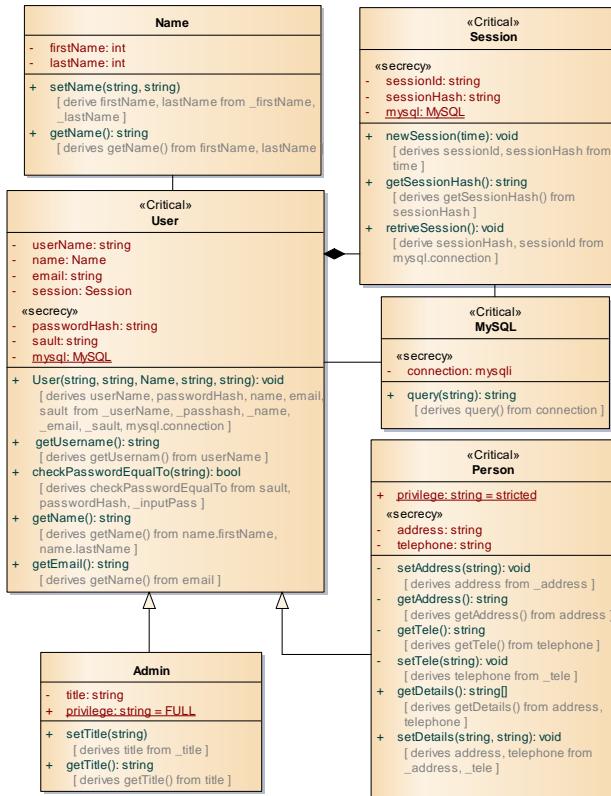


Figure 7, Webapp User Information System Design 2

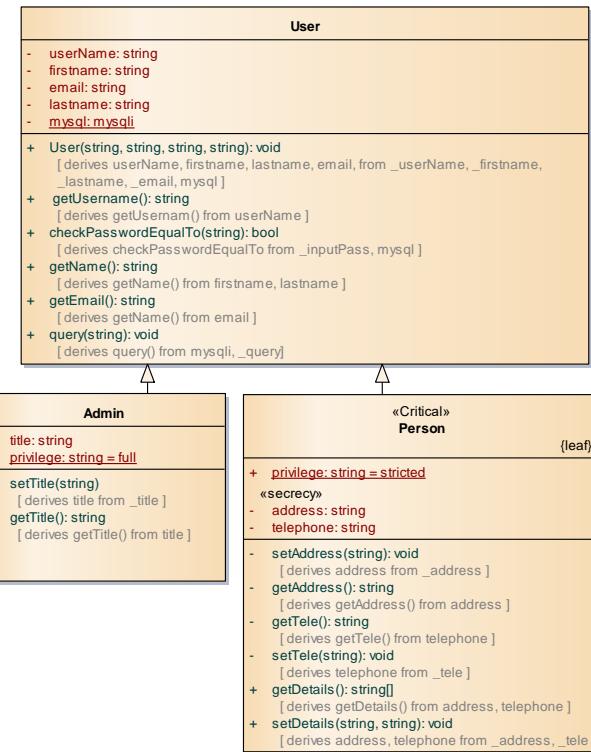


Figure 8, Webapp User Information System Design 4.

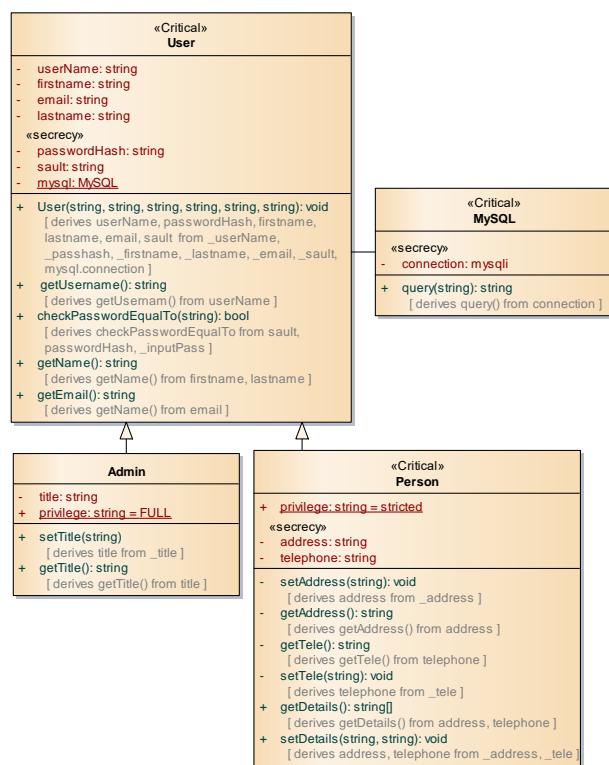


Figure 9, Webapp User Information System Design 3.

Table 1, Design Security Metrics Results.

Metric Name	Design 1	Design 2	Design 3	Design 4
CPCC	0.67	0.75	1	1
CCC	0.071	0.044	0.056	0
CCE	1	1	1	0
CME	1	1	1	0
CSP	0	0.5	0.5	0
CSI	0	0.5	0.5	0
CMI	0	0.25	0.25	0
CAI	0	0.6	0.6	0
CDP	0.6	0.67	0.75	0.33

A different variation of the same diagram has been designed for calculating security metrics and determine which design has the most security. Figure 7 shows the User class that has two subclasses which is Admin and Person. Person class is critical since it has confidential attributes (address, telephone).

Figure 8 shows the diagram which is similar to Figure 7, but it doesn't have Session class, and Figure 9 shows the diagram with only User class along with its subclasses (Admin, Person). Security metrics will help choosing the best diagram with regards to security.

VI. RESULTS AND CONCLUSION

Results shown in Table 1 are conducted using the proposed CASE tool. The result shows the security metrics from designs shown in Figures 6-9 where the lower value of the metric result is considered more secure design. Regarding composite part critical class metric (CPCC), Design 1 is the most secure one since it uses the composite part class to store classified data rather than storing them in the main class which can be exposed to the public.

Critical classes coupling metric (CCC) used to minimize the use of classified attributes through coupling. Design 4 is the most secure design because it doesn't use any coupling between their classes. With respect to critical class extensibility metric (CCE), design 4 is the most secure design because the critical class Person is labeled as a leaf, which means no class can extend from this critical class. In consequence, it's the most secure class according to this metric. In critical methods extensibility metric (CME), design 4 is the most secure design because its classified methods are considered ‘final’ and it can't be extensible because the class is labeled as a leaf which affect the class and its attributes and methods.

Critical superclasses proportion metric (CSP) measures superclasses ratio in a hierarchy, design 1 and design 4 are considered secure designs because they don't have a superclass labeled as a critical class. The lower number of the critical superclasses classes in a design would minimize the value of this metric which result a more secure design.

According to critical superclasses inheritance metric (CSI) result, design 1 and design 4 are the most secure designs since they both doesn't have a critical superclass. Same result obtained when conducting classified methods inheritance

metric (CMI) and classified attributes inheritance metric (CAI) since those metrics depend on critical superclasses to measure the security of an inheritance and both design 1 and design 2 has no critical superclasses on them.

Critical design proportion metric (CDP) measures the size of a design with respect to security and design 4 is the most secure design according to this metric since it has less critical classes than the total number of classes in that design.

After calculating the metrics result, design 4 can be considered as the most secure design since most of the results have the lowest value compared to other designs results except CPCC metric, which is considered as the most insecure class for composition because it doesn't use composite part class to store its classified attributes.

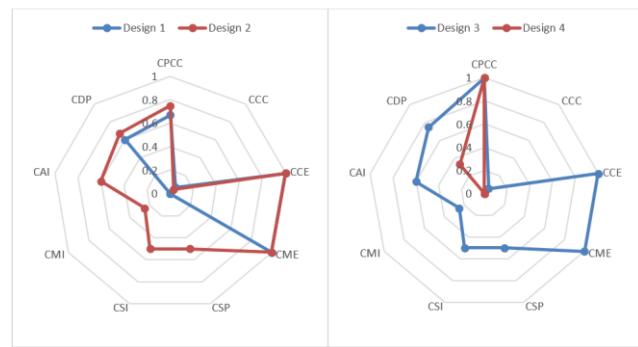


Figure 10, Results Comparison.

Security flaws can be expensive especially for large software products, and fixing these flaws is hard may take long time, and it may increase the total cost of project.

The use of these security metrics in earlier phase of the software development life cycle can decrease a large amount of security flaws and vulnerabilities which may be discovered later in coding or after deployment.

One way of using this metrics is designing software by several developers, compare and promote the best design according to the metrics results. One developer can use these metrics to avoid some design flaws and make the design more secure according to the results of these metrics.

VII. REFERENCES

- [1] Roger S. Pressman, *Software Engineering A practitioner's approach 7th Edition*. 2010.
- [2] M. Willoughby, “Q&A: Quality software means more secure software,” 2005. [Online]. Available: <http://www.computerworld.com/article/2563708/security/q-a--quality-software-means-more-secure-software.html>.
- [3] N. R. Mead and G. McGraw, “A portal for software security,” *IEEE Secur. Priv.*, vol. 3, no. 4, pp. 75–79, 2005.
- [4] S. R. K. T, “A Method Level Security Metrics Suite for Java Programs,” vol. 3, no. 6, pp. 1991–1996, 2012.
- [5] I. Chowdhury, B. Chan, and M. Zulkernine, “Security metrics for source code structures,” *Proc. fourth Int.*

- Work. Softw. Eng. Secur. Syst., no. October, pp. 57–64, 2008.
- [6] B. Alshammari, C. Fidge, and D. Corney, “Security metrics for object-oriented designs,” *Proc. Aust. Softw. Eng. Conf. ASWEC*, pp. 55–64, 2010.
- [7] J. Jürjens, “UMLsec: Extending UML for secure systems development,” *Proc. 5th Int. Conf. Unified Model. Lang.*, pp. 412–425, 2002.
- [8] J. Barnes, *High Integrity Software: The SPARK Approach to Safety and Security*. Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc., 2003.
- [9] G. Spark, D. O ’bryan, S. Mcneilly, N. Capey, J. Redfern, B. Maxwell, V. Kumar, H. Britten, and S.

Meagher, “Enterprise Architect User Guide,” p. 2888, 2012.

AUTHORS PROFILE

Dr. Dujan B. Taha (Assistant Prof.) is currently a lecturer at Mosul University, College of Computer Science and Mathematics / Software Engineering Department. She received B.Sc. degree in Computer Science / University of Mosul in 1991, M.Sc. degree / University of Mosul in 1996 and Ph.D. degree / University of Mosul in 2005. Her research interests are in information and network security, Software Engineering, Image processing and pattern recognition.

Osama S. Mohammed is currently an M.Sc. student in Software Engineering Department / Collage of Computer Science and Mathematics / University of Mosul.

Data Traffic Optimization in Different Backoff Algorithms for IEEE 802.15.4/Zigbee Networks

*Muneer Bani Yassein, Maged Refat Fakirah
Faculty of Computer and Information Technology
Jordan University of Science and Technology
Irbid, Jordan, *Corresponding Author

Qusai Abuein, Mohammed Shatnawi, Laith Bani Yaseen
Jordan University of Science and Technology
Irbid, Jordan

Abstract—Zigbee/IEEE 802.15.4 is a short range wireless communication standard designed for home monitoring, health care, and industrial applications. In this paper, the impact of data traffic load and two data traffic types, namely, Constant Bit Rate (CBR) and Variable Bit Rate (VBR) are studied by considering Binary Exponential Backoff Algorithm (BEB), Linear Backoff Algorithm and Fibonacci Backoff Algorithm (FIB). The efficiency of these algorithms is extensively evaluated by modifying the number of CBR or VBR packets sent from the nodes to the PAN coordinator. The obtained results demonstrate that using the VBR data traffic increases the throughput and decreases the end to end delay, while adopting the CBR data traffic decreases the total energy consumption of a small scale network.

Keywords—IEEE 802.15.4/ZigBee; backoff ; BEB; Linear; FIB; data traffic load; VBR; CBR

I. INTRODUCTION

Zigbee/IEEE 802.15.4 is a standard based on faint data rate and faint amount of power that are frequently used in wireless sensor networks (WSN). Conventional wireless networks are recommended to use Zigbee to connect wireless sensor networks used in home monitoring, health care, commercial and industrial systems [8].

Networks that use Zigbee can contain either a limited number of nodes co-located in a small space or thousands of nodes spread across a wide workspace area [8]. In large scale deployment, the reliability and the energy consumption are among the key issues to overcome [11].

The Zigbee standard supports the MAC and physical layers [9]. The MAC layer operates in two modes: beacon enabled and beaconless.

The PAN coordinator, in beacon mode, sends regularly beacon messages to synchronize them and allocate the guaranteed transmission period for each node (GTS). A super-frame message is sent between every two successive beacon messages, where the interval between these beacons determines the length of the super-frame [10]. As Figure 1 illustrates, this super-frame message is partitioned into 16 robust time slots in addition to an optional amount of idle

time, to allow nodes to sleep if the sleep mode is activated [8].

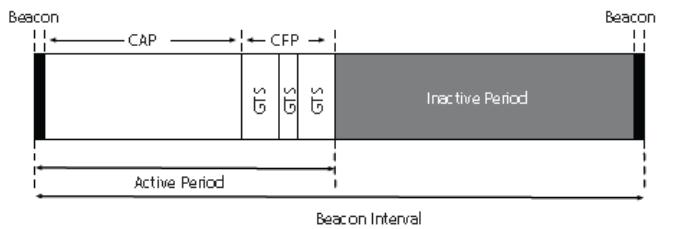


Figure 1. The structure of super-frame message(adapted from [10]).

Furthermore, the beacon enabled mode has two channel access techniques. Contention Access Period (CAP) and Contention Free Period (CFP), which allow the PAN to allocate a time slot called Guaranteed Time Slot (GTS) for every node in the network. On the other hand, in CAP channel access, every node has to wait in order to send its data during the same channel via a technique called Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) [2].

In beacon enabled mode, each node has to use the CSMA/CA technique with all other nodes in the network while attending to access the channel, while it has to use the un-slotted CSMA/CA in beaconless mode. In both modes the nodes should wait for a random amount of time called Binary Exponential Backoff period (BEB) before starting to send their data to decrease the probability of collisions over the transmitting channel. This period vary according to a range of [0, 2BE-1]. Unfortunately, following this rule is not sufficient to prevent collisions in which different nodes may choose the same backoff time [12].

In this paper, we studied the impact of Constant Bit Rate (CBR) and Variable Bit Rate (VBR) under three backoff algorithms (BEB, Linear Backoff algorithm and Fibonacci backoff algorithm (FIB)) on the overall performance of Zigbee/IEEE 802.15.4 standard. The network performance is studied based using three measurement metrics: throughput, average end to end delay and total energy consumption.

The rest of the paper is organized as the critically reviews the related work are discussed in section I. The advantages

and limitations of proposed solutions to avoid the problem identified in the natural BEB algorithm is presented in section II. Section III presents the simulation study. Section IV discusses the results. Eventually, conclusion and future work is presented in section V.

II. RELATED WORK

Several researches were conducted to improve the overall network performance of ZigBee standard under well-known metrics.

Bani Yassien, et al. [1] have suggested a new backoff technique called Fibonacci Backoff technique (FIB) that introduces an incremental Backoff period that should be considered by the nodes before sending their data. The proposed technique avoids collisions caused by transmitting in the same time, based on the following formula:

$$F(x) = F(x-2) + F(x-1), \text{ where } x >= 0, F(0)=0 \text{ and } F(1)=1 \quad (1)$$

The authors of [1] compared the results with a conventional technique called Binary Exponential Backoff (BEB). Their experiments were performed using Qualnet 5.2 simulator based on a star topology with nine nodes. The simulation is performed using two phases. Six nodes out of nine send the data using VBR application in the first phase. In the second phase, three nodes out of the nine send data. The authors evaluated the performance of the network based on three metrics (e.g. average end to end delay, total energy consumption, throughput). The results show that (FIB) outperforms the (BEB) in both phases with different Fibonacci series equal to 4, 5, 6, and 7. However, the Fibonacci series should be chosen carefully depending on the traffic rate and density of the network. Small networks with frequent packet transmission should choose small Fibonacci series or operate using the original BEB algorithm, while large scale networks and infrequent packets should choose large Fibonacci series such as 10 numbers of the Fibonacci series.

In [2], Khamayseh et al, have suggested a new linear Backoff technique that concerns with computing the Backoff period that should be considered from the nodes before sending its data to avoid collisions based on the following formula:

$$BT = \text{random}(1, \text{Mul} * BE) \quad (2)$$

The results of the suggested technique were compared with the original technique called (BEB) that depends on the binary exponential function to compute the Backoff period of time. The experiments were performed using Qualnet 5.2 simulator based on a star topology with 16 nodes. The authors of [2] evaluated the performance of the network based on several metrics including average end to end delay, total energy consumption, throughput, idle mode, delivery ratio, transmit mode and receive mode. The results show that the linear Backoff technique outperforms the conventional (BEB) technique.

Rohm and Goyal [3] have investigated the effect of macMaxCSMA, macMinBE and macMaxBE values on the

beaconless Zigbee network efficiency according to various traffic loads generated by the nodes. During their simulation the authors guaranteed all the nodes are visible to each other and covered by the radio range, where the number of used nodes varies between 10 and 60 nodes leading to 10 – 300 overall packets per second. The authors used packet latency and packet loss probability metrics to evaluate the performance of the network. Furthermore, they produced a dynamic Backoff algorithm to adjust the macMaxCSMA, macMinBE and macMaxBE automatically to increase the throughput and to reduce the packet loss. This proposed algorithm was able to be adapted quickly according to the network traffic load.

In [4] Momani et al. proposed a new increment technique to prevent transmissions from being failed as well as to select a convenient Backoff period by sliding the connection window. The new algorithm increases the delivery ratio of packets while it raises the end to end delay as a result of using large Backoff periods. The simulation was conducted on 1000*1000 network area using GloMoSim simulator with a 30, 60, 100 nodes consecutively, and using CBR data application type to generate 10 packets per second. The metrics used to evaluate the performance of the proposed contribution are data delivery ratio, end to end delay and network overhead. The results show that moving the contention window (CW) to the right of the past transmissions can increase the efficiency of the algorithm than the original (BEB) algorithm with 7.1%, Pessimistic Linear Exponential Backoff algorithm (PLEB) with 19%, and Smart Adaptive Backoff algorithm (SABA) with 16.5%.

III. METHODOLOGY

This research paper studies the impact of the data traffic load and type on the network performance using a Fibonacci Backoff algorithm (FIB), Linear algorithm, and the original Binary Exponential Backoff algorithm (BEB). The efficiency of these algorithms is comparing by considering different traffic loads and two kinds of traffic types (i.e. CBR, and VBR).

A. Data Traffic Types

Data traffic type can be defined as a data source or traffic flow generator [6]. Two kinds of data traffic types are used in this work:

1) *Constant Bit Rate (CBR)*: It is not an on/off traffic rather it depends on generating a constant amount of data output during each time period, in which the CBR can be used to gather the features of all available capacities [6][7].

2) *Variable Bit Rate (VBR)*: It is an on/off traffic used in encoding videos or sounds because it depends on a variable amount of data output during each time slice. It needs high storage because it supports high bit rate [6][7].

B. Simulation Setup And Scenarios

The simulation used eight reduced function devices (RDF) with a full function device (FFD) that acts as a PAN coordinator for them following a star topology placement

model. The simulation area is 80*80 meters with a simulation time of 1000 seconds as explained in table I.

Two scenarios are conducted to estimate the impact of the data traffic type upon the three studied algorithms. The first scenario generates VBR traffic from each node to the PAN coordinator with different amount of data traffic loads that can be adjusted by changing the number of nodes that send traffic per each experiment in the range of 1 to 8. In other words, the number of nodes that send traffic differs from one experiment to another during the range between 1 and 8 as illustrated in Figure 2.

The second scenario differs from the first one. In this case the nodes generate CBR traffic and the generated traffic amount varied from 50 KB/s to 400 KB/s based on the number of sending nodes during the experiment as shown in Figure 3.

TABLE I. PARAMETERS USED IN THE SIMULATION OF THE SCENARIO.

Parameter	Value
Simulator	QualNet 5.2
Radio Type& MAC model	IEEE 802.15.4
Area (Terrain)	80 m * 80 m
Number of nodes	9
Topology	Star
Simulation time	1000 s
Packet rate	50 kbps
Start time	10 Seconds
End time	0 Seconds
Interval	1 Second
Energy model	MICAZ
Antenna Height	0.08
Antenna Model	Omnidirectional
Data Traffic Type	VBR, CBR
Channel Access Mode	CSMA
BO and SO	4, 2 respectively
Routing Protocol	AODV

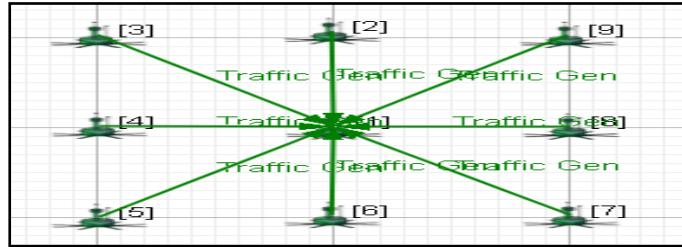


Figure 2. 9 nodes (star topology) with 8 VBR traffic type implemented by QualNet simulator.

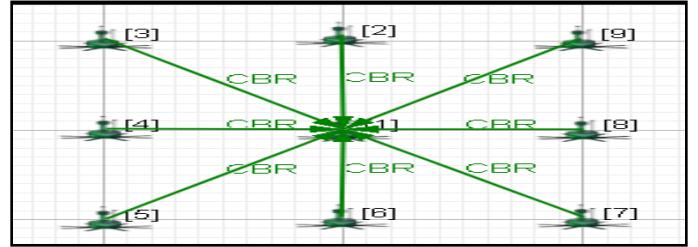


Figure 3. 9 nodes (star topology) with 8 CBR traffic type implemented by QualNet simulator.

IV. RESULTS DISCUSSION

This section describes in detail the results obtained from the experiment by categorizing the results into three groups according to the metrics used in the efficiency estimation of the investigated algorithms. This can present a clear and meaningful understanding of the results gained. For this procedure three metrics were used as follows:

1) *Throughput*: It refers to the amount of data frames that are successfully gone during the PAN in a specific period of time [9]. According to the Figures 4, 5, and 6, it is obvious that using the VBR data traffic type increases the performance of the network for all investigated algorithms under different traffic loads by increasing the throughput compared to the other used traffic type (i.e.CBR). Also, increasing the number of nodes that send packets to the PAN coordinator to increase the amount of traffic load can affect the throughput positively as well.

Figures 4, 5, and 6 show that the maximum throughput values, which can be gained from using a VBR type are: 1891.60 Bits/S from the FIB algorithm, 1898.60 Bits/S from the Linear algorithm, and 2066.80 Bits/S from the BEB algorithm. On the other hand, the maximum throughputs gained from using CBR are 401.20 Bits/S, 511.20 Bits/S and 470.60 Bits/S consecutively.

2) *Average End to End Delay*: The average time disbursed by the packet to reach the PAN coordinator from the source node [8]. The results in Figures 7, 8, and 9 state that using the VBR data traffic type increases the performance of all investigated algorithms by decreasing the average end to end delay compared to the other used traffic type called CBR.

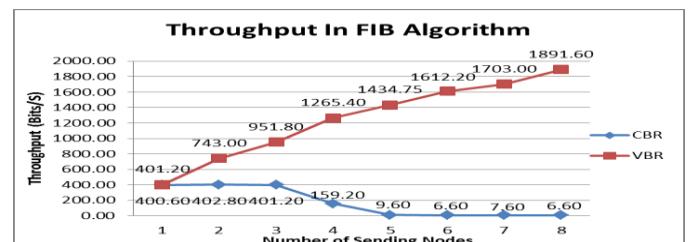


Figure 4. Throughput performance of FIB algorithm using CBR & VBR traffic types under different traffic loads.

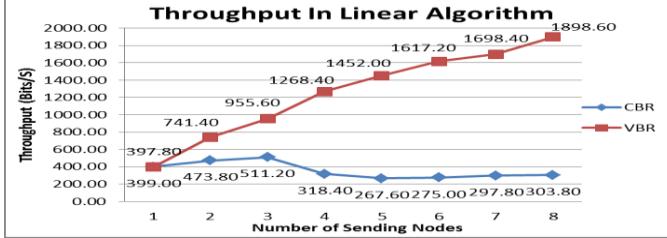


Figure 5. Throughput performance of Linear algorithm using CBR & VBR traffic types under different traffic loads.

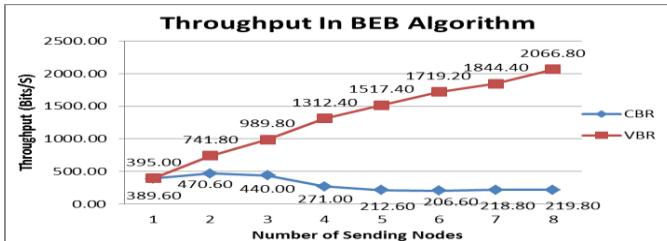


Figure 6. Throughput performance of BEB algorithm using CBR & VBR traffic types under different traffic loads.

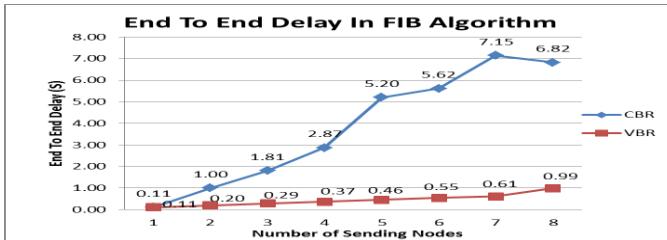


Figure 7. Average end to end delay in FIB algorithm using VBR & CBR traffic types under different traffic loads.

Furthermore, increasing the amount of traffic load by increasing the number of nodes that send packets to the PAN coordinator affects negatively on the average end to end delay in all investigated algorithms. This can happen because the average end to end delay becomes greater with each increase in the amount of data traffic load.



Figure 8. Average end to end delay in Linear algorithm using VBR & CBR traffic types under different traffic loads.

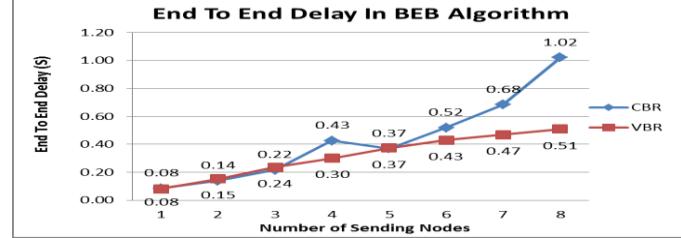


Figure 9. Average end to end delay in BEB algorithm using VBR & CBR traffic types under different traffic loads.

3) *Total energy consumption:* The total sum of the energy consumed in the transmitting mode, receiving mode, idle mode, and sleeping mode [8]. It is measured in mWh unit and the greater the active period, the greater the energy consumption [9]. Figures 10, 11, and 12 give a clear indication about the best data traffic type that can be used to enhance the performance of the network by decreasing the Total Energy Consumption (i.e. CBR in the all studied algorithms).

In addition, the results that are shown in the same graphs, one can observe that the results vary in FIB algorithm according to the change in the number of nodes that send traffic to the PAN coordinator (i.e. the best amount of nodes that give best values is one and three with 28.44 mWh and 25.51 mWh consequently). However, increasing the amount of traffic load affects negatively on the performance of the network in both Linear and BEB algorithms because the Total Energy Consumption increases.

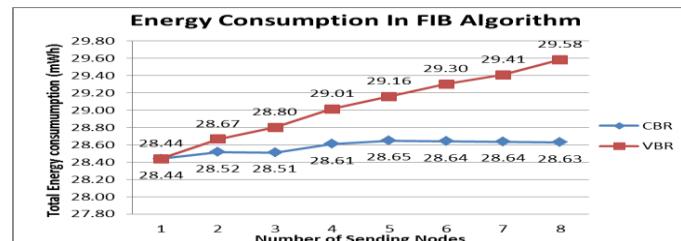


Figure 10. Total Energy Consumption in FIB algorithm using VBR & CBR traffic types under different traffic loads.

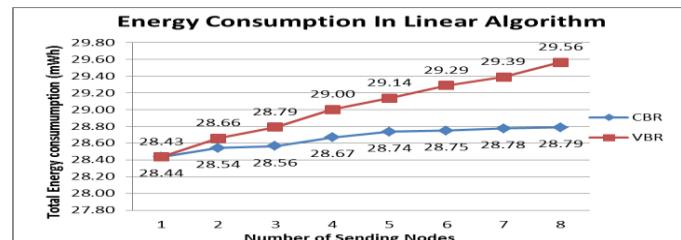


Figure 11. Total Energy Consumption in Linear algorithm using VBR & CBR traffic types under different traffic loads.

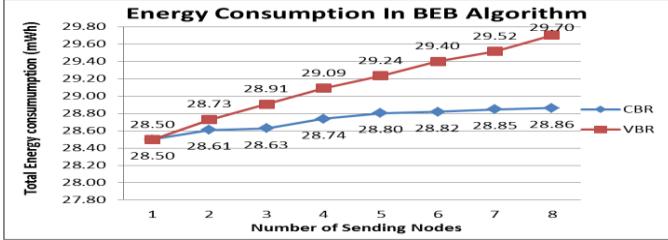


Figure 12. Total Energy Consumption in BEB algorithm using VBR & CBR traffic types under different traffic loads.

V. CONCLUSION AND FUTURE WORK

This research paper studied the impact of two kinds of data traffic generators which are CBR and VBR on three algorithms (e.g. FIB, Linear, and BEB) under different traffic loads. The QualNet 5.2 simulator is used to estimate the network performance by measuring the throughput, end to end delay and total energy consumption. From the simulation result, we conclude that using VBR traffic generator increases the performance of the network for all studied algorithms by increasing the throughput and decreasing the end to end delay, in spite of it consumes more energy. Furthermore, the end to end delay and the total energy consumption become worse by increasing the amount of traffic load, while that affects the throughput positively.

This work might be extended in the future by increasing the number of nodes that send packets during the simulation time. This is done trying to get more accurate and significant results about the impact of the data traffic load on the network. In addition, increasing the number of nodes might be a good indication of deciding whether the amount of traffic load is high or low. New algorithms can be developed, such as combination between the FIB and linear algorithms in which each node adaptive its Backoff behavior to work as a linear algorithm when low traffic load is transmitted, and the node uses the FIB algorithm when the traffic load is high.

REFERENCES

- [1] B. Y. Muneer, S. Marwa, M. Wail, and K. Yaser, "Fibonacci backoff algorithm for IEEE 802.15. 4/ZigBee," Network Protocols & Algorithms 4, no. 3, pp. 62-78, 2012.
- [2] K. Yaser, M. Wail, J. Reem, and H. Rana, "Improved backoff technique for ZigBee networks," 3rd International Conference on Computer Modelling and Simulation, Brno, Czech Republic, 2012.
- [3] D Rohm and M Goyal, "Dynamic backoff for IEEE 802.15.4 beaconless networks," IEEE Mini-Grants (National Science Foundation under Grant No. 0442313), University of Wisconsin Milwaukee, Milwaukee, WI 53201, 2009.
- [4] M. Ahmad, A. E. Ahmad, B. Y. Muneer, D. Omar, M. Saher, and M. Wail. "Intelligent paging backoff algorithm for ieee 802.11 mac protocol." Network Protocols and Algorithms 4, no. 2, 2012 , pp. 108-123,
- [5] "http://web.scalable-networks.com/content/qualnet," last accessed on 19/09/2015.
- [6] M. Shubhangi, X. D. Ashish, and A. K. Jaiswal, "Effect of mobility and different data traffic in wireless Ad-hoc network through QualNet," International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-5, pp. 364-368, June 2013.

- [7] "http://en.wikipedia.org/wiki/Variable_bitrate", last accessed on 19/09/2015.
- [8] B. Y. Muneer, K. Yaser, R. F. Maged, and A. A. M. Ghassan, "Optimization in backoff technique for IEEE 802.15.4/ ZigBee networks," The tenth International Conference on Wireless and Mobile Communications (ICWMC), pp. 124-128, Seville, Spain, June 2014.
- [9] K. Wook and A. Sun-Shin, "Differential dynamic traffic control for IEEE 802.15.4 networks," Journal of information science and engineering 26, pp. 255-266, 2010.
- [10] M. F. Laura, F. Michael, F. Viktoria, and G. Mesut, "Modes of inter-network interaction in beacon-enabled IEEE 802.15.4 networks," Ad Hoc Networking Workshop (MED-HOC-NET), 14th Annual Mediterranean. IEEE, 2015.
- [11] Tytgat, Lieven, Y. Opher, P. Sofie, M. Ingrid, and D. Piet, "Analysis and experimental verification of frequency-based interference avoidance mechanisms in IEEE 802.15. 4," Networking, IEEE/ACM Transactions on 23.2, pp. 369-382, 2015.
- [12] K. Mounib , G. Mouhcine, and T. M. Hussein, "A survey of beacon-enabled IEEE 802.15. 4 MAC protocols in wireless sensor networks," Communications Surveys & Tutorials, IEEE 16.2, pp. 856-876, 2014.

A Novel Polygon Cipher Technique using hybrid key Scheme

Shadi R. Masadeh

Faculty of Information Technology
Isra University
Amman, Jordan

Hamza A. A. Al_Sewadi

King Hussein Faculty of Computing
Prince Sumaya for Technology
Amman, Jordan

Abstract— Due to the narrow key space and frequency analysis weakness, classical cipher techniques are not suitable for most today's information communication. On the other hand, modern standardize ciphers are far more secure and widely used for such communication. However, they are so complicated in implementation and may not be suitable for less sophisticated applications. This paper suggests a novel symmetric cipher method based on polygon scheme that shows superior security as compared with classical methods by having wide key space and strength against frequency analysis attack and yet it is simpler than modern ciphers.

Keywords- *information security, encryption/decryption, secret key, symmetric cryptography, asymmetric key implementation.*

I. INTRODUCTION

The ever increasing uses of digital computer systems for information storage and digital communication for transmission have led to the problem of vulnerability of information breach. For this reason, so many information security algorithms are needed and are developed and practically implemented. Basically they rely of encryption of the information. Hence, both classical and modern encryption techniques are widely in use today for solving information security problems against adversary attacks. The notorious modern techniques whether, symmetric such as DES, 3DES or AES and asymmetric such as RSA, [1]-[2], are very good examples of actual cryptosystem that are practically and effectively used for encryption/decryption of information. They are so complicated but they proved their strength and have been in use for some time. However, for some less sophisticated applications, some classical encryption techniques might still be useful, such as new variants of Playfair cipher, see Goyal et. al. [4] and Kumar et. al. [5]. Some interesting and recently developed versions of Playfair cipher variants shall be discussed in this work and will be compared with the proposed ciphering method. This paper suggests a new encryption/decryption algorithm that implements a polygon shape diagram. It incorporates more characters and follows completely different procedure for building the encryption/decryption table, password usage and implementation process.

After, the brief introduction in section 1, section 2 lists important related works. Then a detailed explanation of the proposed polygon cipher cryptosystem scheme is included in

section 3. Section 4 includes the implementation of the algorithm and comparison with some similar techniques. Finally section 5 concludes the paper.

The preparation of manuscripts which are to be reproduced by photo-offset requires special care. Papers submitted in a technically unsuitable form will be returned for retyping, or canceled if the volume cannot otherwise be finished on time.

II. RELATED WORK

Classical techniques in the security field had been studies for long time; however they are still under consideration by various researchers. This section considers the most relevant ones to the proposed work.

Playfair cipher variants were suggested and experimented with by many researchers. They have added so many enhancements to the original cipher suggested and used practically for some time, even in world wars I and II.

Murali and Senthilkumar [6], used the random number methods in the Palyfair cipher method in order to enhance the security features of transmission over unsecured channels. The random numbers is transmitted to the receiver instead of alphabetic characters.

Sastray et. al. [7] considered the 7 bits ASCII characters representation for the plaintext message characters denoted by codes from 0 to 127. Shanon's concept of confusion and diffusion was achieved by suitable variation in the traditional Playfair rules together with modification in the substitution tables.

Babu et. al. [8] implemented a 6x6 matrix in their work instead of 5x5. They added the numbers in their cipher, but still they didn't care about lowercase letters, white space and other printable characters.

Rahmani et. al. [9] introduced the extension of Vigenère Cipher based on the Alpha-Qwerty Cipher and reverse Alpha-Qwerty Ciphers and their method works on set of 92 alphabetic by inserting digits and special characters to existing vigenere cipher method. Comparison of extension of Vigenère Cipher with the original vigenere cipher showed that the cipher text is less understandable and difficult to break. Moreover, frequency analysis attack failed when implemented on the original Vigenère cipher.

Kaur et. al. [10] suggested 3D-Playfair Cipher ($4 \times 4 \times 4$ Playfair cipher) that works on trigraph rather than using digraph which eliminates a diagram and its reverse will encode in a similar way. They enhanced security for the data that consist of alphabets, numerals and special characters via its transmission. Also, high rates of confusion and diffusion has been achieved as the method provided $64 \times 16 \times 4 = 4096$ possible trigraphs. Their 3D-Playfair matrix included 64 characters, which resulted in character frequency of occurrence of $1/16 * 1/4$ (i.e. $1/64 = 0.0156$).

Hamad et. al. [11] proposed an extended version of Polyfair method for ciphering digital image securely. They built a 16×16 secret key to be used for generating a mask that is subsequently XOR'ed with the scrambled image. Their experimental results showed a wide key space that makes it hard for the hackers to execute a frequency analysis attack on the pixel digraphs.

Kartha and Paul [12] listed a cryptanalysis review for Polyfair method and some of its recent modifications. Also they pointed out the primary weakness of Vigenère cipher which is the repeating nature of its key.

Ali and Sarhan [13] combined an advanced encryption algorithm with stream cipher method in order to enhance the security of Vigenere method. This is due to the fact that the stream cipher uses binary form instead of characters, which makes it relatively harder to break by using frequency analysis attack.

III. THE PROPOSED POLYGON CIPHER SCHEME

The proposed cryptographic scheme is designed to include the set of alphabet characters (i.e. a - z), numerals (i.e. 0 - 9), and some of the special characters (namely; !, @, #, \$, %, ^, &, *, /, -, +, space[Δ]). A bi-square shape inside a circle as that of Fig. 1 is implemented to accommodate this character set. These characters are allocated to the angles formed by the squares intersections according to a pre-defined order as will be described latter in this section.

The scheme is a symmetric system with the secret key consisting of two parameters; namely the angle and the rotation of the character set template. Therefore each character of the message will be replaced by the character position after the implementation of the secret key. In the following, a detailed description is included for producing the character set template, key implementation, encryption process and decryption process.

A. Character set template

Two equal squares are uniformly intersected inside a circle produce eight intersection points on the radii (i.e. -1 to -8) forming six angles at each point, allowing for 48 angles. The angles at these intersections may be utilized to accommodate the alphabet characters, numerals, and the selected special characters starting from the first angle on radius (-1) in a clockwise sequence then continuing in anticlockwise to radius (-2) then (-3) and so on until radius (-8). The 8 radii form angles at the center of the circle numbered -1, -2, ..., -8 to represent the angle values $\pi/8$, $3\pi/8$, $5\pi/8$, $7\pi/8$, $9\pi/8$, $11\pi/8$,

$13\pi/8$, $15\pi/8$, respectively. The (-) sign used here represents anticlockwise direction while (+) sign will be used for clockwise direction. The resulting character set template which can be called the default template is illustrated in Fig. 1. It must be noted here that the (Δ) character is used to represent the space.

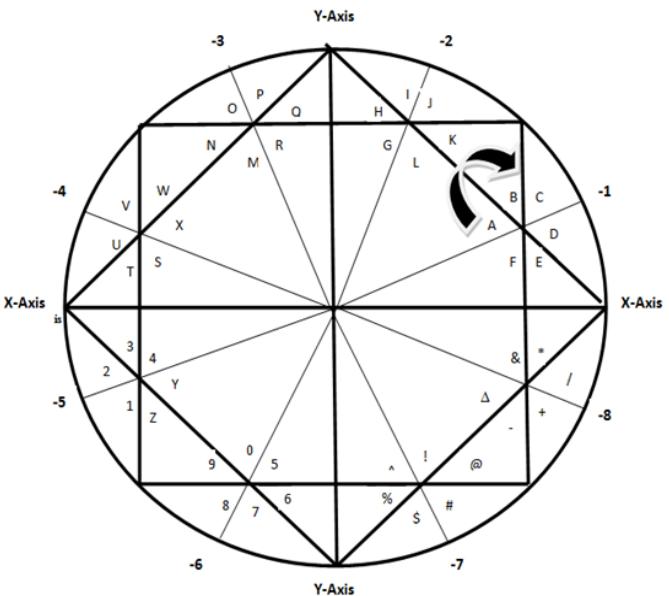


Figure 1. The default character set template

The information of Fig. 1 can be expressed clearly in the default matrix that consists of 8×6 entries, representing the 8 groups of 6 characters each. Then a 7th column is added that points to the angle of each group resulting into an 8×7 matrix as shown in table I.

TABLE I. DEFAULT CHARACTER SET TABLE.

	0	1	2	3	4	5	Angle
0	A	B	C	D	E	F	-1
1	G	H	I	J	K	L	-2
2	M	N	O	P	Q	R	-3
3	S	T	U	V	W	X	-4
4	Y	Z	1	2	3	4	-5
5	5	6	7	8	9	0	-6
6	!	@	#	\$	%	^	-7
7	&	*	/	+	-	Δ	-8

B. Key implementation:

The secret key is designed to consist of two parts separated by comma; a chosen number of the character set followed by an angle with a rotation direction, as shown in the following example. Let the key be as given in (1) below.

$$\text{key} = \text{"CRYPTOGRAPHY, +2"} \quad (1)$$

The first part of the key is used to construct the character set template after dropping any repeated characters, i.e. only "CRYPTOGAH" is taken in this example, and the second part is used to rotate this template (i.e. "+2" means angle $3\pi/8$ anticlockwise). After writing these characters in sequence in fresh template of Fig. 1 starting from the first position, the remaining characters are used to complete the template. Then

the character set template is rotated according to the second part of the key, for this example it will be as shown in Fig. 2. The content of this template of Fig. 2 can be translated into an 8x7 matrix. See the matrix of table II after omitting the column containing the default angle. This table is now ready to be used for encryption or decryption of messages.

It must be noted that Fig. 1 is included for clarification of the idea of construction table II and obviously it is not required to be drawn each time.

TABLE II. THE EXAMPLE ENCRYPTION/DECRYPTION CHARACTERS SET

	0	1	2	3	4	5	Angle	Key angle
0	C	R	Y	P	T	O	-1	-3
1	G	A	H	B	D	E	-2	-4
2	F	I	J	K	L	M	-3	-5
3	N	Q	S	U	V	W	-4	-6
4	X	Z	1	2	3	4	-5	-7
5	5	6	7	8	9	0	-6	-8
6	!	@	#	\$	%	^	-7	-1
7	&	*	/	+	-	Δ	-8	-2

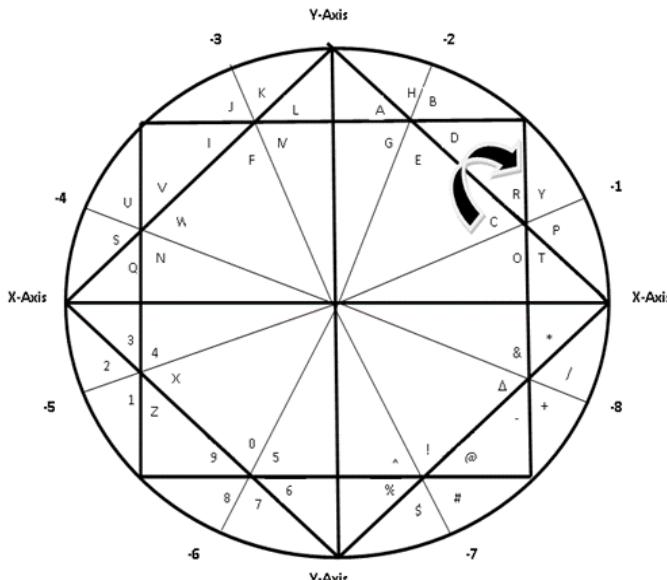


Figure 2. The character set template for the example key

C. Encryption procedure, E

To encrypt a message by the proposed scheme, the encryption/decryption character set matrix for the secret key is used. Each character of the message is replaced by three parameters; the raw number, the column number, and the angle of rotation. Therefore, the cipher text string consists of group's blocks with four parameters, namely; three values and a sign (e.g. [2, 5, -5]). These values stand for raw number, column number, rotation direction and angle number, respectively, as will be seen in the next section.

D. Decryption procedure, D

As the receiver knows the secret key, he/she first constructs the encryption set matrix, table II. Then decryption is performed by inverting the encryption process, i.e. treating

elements of C one-by-one into the matrix to recover the original message.

E. The overall cryptosystem Scheme

The proposed cryptosystem is a hybrid of stream cipher and block cipher. It assumes the division of each message M into blocks M_1, M_2, \dots, M_n . The elements of each block are enciphered with the same key, but different blocks use different keys. Each block, M_i is encrypted with a session key K_i ($i = 1, 2, \dots, n$) that is enciphered with the receiver's public key. They are concatenated with each other and transmitted to the recipient, as shown in Fig. 3.

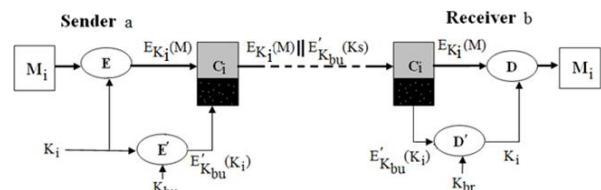


Figure 3. The proposed cryptosystem scheme.

On the other side, the receiver uses his/her own private key to get the session key recovered first and then use it recover the original message block. It must be noted that the algorithms E and D are the proposed encryption and decryption algorithms, respectively, proposed in this paper, while E' and D' are any other public-key algorithms such as RSA or PGP.

In order to enhance the security of this cryptosystem, different sub-keys generation is done by successive encryption using the receiver's public key, see Fig. 4-a, but on the receiver side it is achieved by decrypting the concatenated ciphered sub-keys by the receiver's private key, as shown in Fig. 4-b.

On the sender side, the sub-keys generation is done by successive encryption using the receiver's public key, see Fig. 4-a, but on the receiver side it is achieved by decrypting the concatenated ciphered sub-keys by the receiver's private key, as shown in Fig. 4-b.

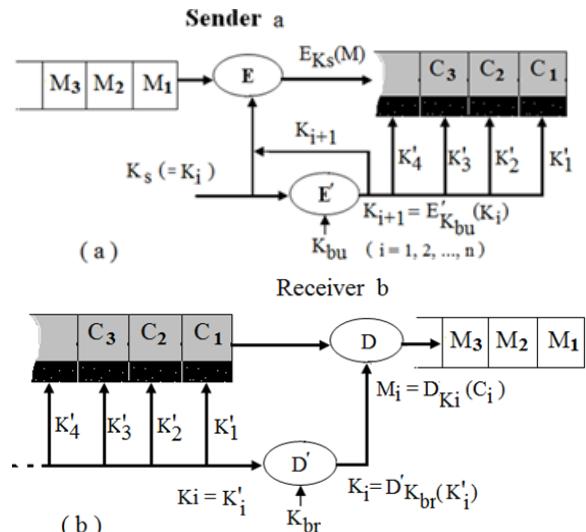


Figure 4. The overall cryptosystem processes.

IV. RESULTS AND DISCUSSION

The algorithm of section 3 is programmed to accept a keyword first in order to generate the character set template, from which, the character set table is produced. For example if the key of equation (1) [i.e. key = "CRYPTOGRAPHY, +2"] is used in the polygon of Fig. 1, it will produce the polygon of Fig. 2, from which table II is obtained that shall be used for encryption and decryption.

For example if the message to be encrypted by the above key is given in (2).

$$M = \text{"museum\#245 is closed"} \quad (2)$$

Then the resulting ciphertext message C, after using the character set table becomes as shown by (3).

$$C = "[2,5,-5],[3,3,-6],[3,2,-6],[1,5,-4],[3,3,-6],[2,5,-5],[6,2,-1],[4,3,-7],[4,5,-7],[5,0,-8],[7,5,-2],[2,1,-5],[3,2,-6],[7,5,-2],[0,0,-3],[2,4,-5],[0,5,-3],[3,2,-6],[1,5,-4],[1,4,-4]" \quad (3)$$

This ciphertext C consists of numbers only and can then be transmitted safely to the recipient.

For the decryption of this message in inverse of the encryption process is followed. Therefore, as the same character set table will be obtained if the same key of equation (1) is used, then the resulting message will be the original message M.

In order to check for the security strength of the polygon cipher scheme, the number of characters involved, and key space complexity which are crucial for brute force attack may be considered. Likewise, the probability of frequency analysis which is the study of the frequency of occurrence for letters or groups of letters in a ciphertext, Harrison et.al. [14] must be considered. Hence, a comparison of the key space, Number of characters and the vulnerability for frequency analysis attack is calculated and listed in table III.

The probability of frequency analysis for the characters and letters occurrence in the text involved in this study is calculated according to the following equation, (4).

$$P = (n / N) \quad (4)$$

Where, P is the probability of occurrence, n is the number of characters, and N is the number of possible diagrams.

TABLE III. COMPARISON OF POLYGON CIPHER WITH OTHER SCHEMES

Cipher Method	Key space	Number of characters	frequency (probability)
Playfair	25!	26	0.038
Vigeneer	26*26	26	1
Babu et. al.	36!	36	0.028
Verma et. al.	64!	64	0.016
Polygon (Proposed)	48!*8*2	48	0.000325

Table III, shows that the key space and the frequency analysis probability for the proposed polygon cipher is far more superior to all the considered methods, however, Verma method uses more characters than the proposed polygon cipher at the price of increase vulnerability. As far as the key space

concerned, polygon cipher has better range compared with Vigeneere, Buba and all Playfair variants.

In the proposed scheme, the security strength of the polygon cipher is enhanced by adding other algorithms such as PGP or RSA resulting into a hyper cryptosystem to be used for multiple key secure information exchange. That was achieved by dividing the message into segments, then encrypting the first segment with the seed key, and then generating sub-keys for successive message segments.

V. CONCLUSION

The polygon shape offers lots of angles and interconnections that are utilized in this work to accommodate more characters to be used for secure text communication. It also offers some other degrees of freedom such as angle and rotation directions. These features were utilized in this work to present the new ciphering technique that resulted into a stronger cryptosystem than notoriously known classic systems such as Playfair, Veginere, Verma, etc.

The polygon cipher has a wide key space and excellent character frequency of occurrence that would prove useful for some less complicated applications that prefer avoiding the modern and sophisticated cryptographic algorithms.

The inclusion of PGP or RSA algorithms with the polygon cipher technique for multiple key transmissions gives the method an added value to be used as a hybrid of stream cipher and block cipher for secure communication.

REFERENCES

- [1] W. Stallings, "Cryptography and Network Security: Principle and Practice, 5/E, Pearson Education, (2011).
- [2] V. Verma, D. Kaur D., Singh R. K. and Kaur A.: 3D- Playfair cipher with additional bitwise operation, In Control Computing Communication & Materials (ICCCCM), 2013 International Conference on IEEE, (2013), 1-6, (August 2013).
- [3] Yan, Song Y.: Primality Testing and Integer Factorization in Public-Key Cryptography, Springer, (2009).
- [4] P. Goyal , G. Sharma and Kushwah S|. S.: Network Security: A Survey Paper on Playfair Cipher and its Variants, International Journal of Urban Design for Ubiquitous Computing Vol. 3, No.1, 1-6, (2015), <http://dx.doi.org/10.14257/ijuduc.2015.3.1.01>.
- [5] M. Kumar, Reena Mishra R., Pandey R. K. and Singh P.: Comparing Classical Encryption With Modern Techniques", proceedings of SJSET, Vol. 1, No. 1,(2010).
- [6] P. Murali, and Senthilkumar G: A Modified Version of Playfair Cipher using Linear Feedback Shift Register, International Journal of Computer Science and Network Security (IJCSNS), Vol.8, No.12, December (2008).
- [7] U. Sastry, Shankar N. R., and Bhavani S. D.: A Modified Playfair Cipher Involving Interweaving and Iteration, International Journal of Computer Theory and Engineering, Vol. 1, No. 5, 1793-8201, (December 2009).
- [8] K. R. Babu, Kumar U., Babu A. V., Aditya I. V. N. S., and Komuraiah P.: An Extension to Traditional Playfair Cryptographic Method, International Journal of Computer Applications (IJCA), Vol.17, No.5, (March 2011).
- [9] M. K. I. Rahmani, Wadhwa N. and Malhotra V.: Alpha-Qwerty Cipher: An Extended Vigenere Cipher, Advanced Computing: An International Journal (ACIJ), Vol.3, No.3, (May 2012).

- [10] A. Kaur, Verma H. K., Singh R. K.: 3D (4 x 4 x 4) Playfair Cipher, International Journal of Computer Applications, Vol. 51, No. 2, (August 2012).
- [11] S. Hamad, Khalifa A., Elhadad A., Rida S. Z.: A Modi_ed Playfair Cipher for Encrypting Digital Images, Journal of Communications & Computer Engineering, Vol. 3, No. 2, 1-9, (2013).
- [12] R. S. Kartha, and Paul V.: Survey: Recent Modifications in Vigenere Cipher, Journal of Computer Engineering (IOSR-JCE), Vol. 16, No. 2, Ver. IX, 49-53, (Mar-Apr. 2014).
- [13] F. M. S. Ali, and Sarhan F. H.: Enhancing Security of Vigenere Cipher by Stream Cipher, International Journal of Computer Applications (IJCA) Vo. 100, No. 1, (August 2014).
- [14] K. Harrison, Munro B. and Spiller T.: Security through uncertainty, P Laboratories, (February 2007).

AUTHORS PROFILE



Shadi R. Masadeh: received a BSc degree in Computer Science and Computer Information System in 2000 and MSc degree in Information Technology in 2003, with a Thesis titled "A Mathematical Approach for Ciphering and Deciphering Techniques". After that, I received PhD from department of Computer Information System in 2009 with a Thesis titled "A New Embedded Method for Encryption/Decryption Technique Using Self Approach". My research interests including E-learning Management, Encryption and Decryption Systems, Networking and Wireless security. Currently, I'm working at Isra University in Computer Networks Department.



Hamza A. A. Al_Sewadi is currently a professor at King Hussein Faculty of Computing Science, Prince Sumaya University for Technology, Jordan. He is graduated from Basrah University (Iraq), then M.Sc. and Ph.D. degrees, respectively from University of London (UK). Previously he worked at Isra University and Zarqa University (Jordan), Aizu University (Japan), and Basrah University (Iraq). His research interests include Cryptography, Steganography, Watermarking, Information and Computer Network Security, Artificial Intelligence and Neural Networks.

An Efficient Method to diagnose the treatment of Breast Cancer using Multi-Classifiers

J. Umamaheswari

Computer science dept. Majmaah University
Al- Majmaah, Saudi arabia

Jabeen Sultana, Ruhi Fatima

Computer science dept. Majmaah University
Al- Majmaah, Saudi arabia

Abstract— Knowledge discovery in the form of rule extraction proposed to extract rules from classification datasets by giving data set to Decision Trees (DT), NBTREE, KNN and 10-fold Cross Validation performed, resulting the tree or a model from which rules are extracted and measured on different parameters taken from root node to leaf node .

Keywords- Transparent; Opaque; Knowledge discovery; rule extraction

I. INTRODUCTION

Data Mining and Machine Learning techniques extract knowledge from large data bases. The knowledge gained is difficult to interpret and it is not in human comprehensible form. Hence rule extraction is performed to interpret the knowledge gained from different machine learning techniques. For real world classification problems, datasets are large in size. For mining the knowledge from those databases, learning takes more time by the standard Machine Learning Techniques [5] and further the knowledge acquired by these techniques remains hidden and inaccessible. Therefore Knowledge discovery in the form of rule extraction is proposed here to extract rules from classification datasets and giving data set to Decision Trees (DT), Naïve base (NB)TREE, KNN and 10-fold Cross Validation is performed resulting in the tree or a model from which rules are extracted and measured on parameters like Accuracy, Specificity, Sensitivity, Number of rules, Conditions per rule, and Comprehensibility. The rule extraction techniques are applied, rules are taken from root node to leaf node in the case of DT and NB. In KNN accuracy, RMSE (root mean square error), Sensitivity and Specificity are determined.

Rule Extraction is very much necessary in crucial decision making processes in Medical Field, Banking Sector, and Time Series analysis. Making decisions involves keeping in mind a lot of things pertaining to any related field. In the following literature related to the current topic of rule extraction from data is reviewed. Meticulous, a survey of two papers taken- one on active learning and rule extraction and the other on Multiple Kernel based support vector machine (SVM) and rule extraction.

II. RULE EXTRACTION TECHNIQUES

Based on the type of internal model learned using machine learning techniques and how well the model is used by rule extractors to extract rules, rule extraction techniques are classified into three categories [9,1]

1. Decompositional Approach
2. Pedagogical Approach
3. Eclectic or Hybrid Approach

II.1. Decompositional Approach

A decompositional approach deals directly with the internal workings of the black-box classifier utilized for learning the model. For example, in the case of support vector machine (SVM), hyperplane model learned by SVM is considered by the decompositional approach. Rule extraction is done by utilizing the SVM's support vectors, separating hyper plane and symbolic rules are extracted from the trained network. The rules extracted are in human comprehensible rules format [1]. Nunez et al. [7] proposed a decompositional rule extraction approach where prototypes extracted from k-means clustering algorithm are combined with support vectors from SVM and then rules are extracted. k-means clustering algorithm used to determine prototype vectors for each input class. An ellipsoid is defined in the input space combining these prototypes with support vectors and mapped to if-then rules. The disadvantage of this algorithm is the construction of hyper rectangles based on the number of support vectors. RulExtSVM, Hyper rectangle Rules Extraction (HRE), Fuzzy Rule Extraction (FREx) approach are some of the algorithms used in this approach.

II.2. Pedagogical Approach

A pedagogical approach does not consider the internal workings but looks at the model learned by the classifier indirectly without peeping into the black box. These algorithms directly extract rules that relate the inputs and outputs of the trained classifier. For example, in the case of SVM, predicted class labels of SVM are given to rule extraction approaches. The main idea behind these techniques

is that the knowledge gathered by the trained model is modeled better by taking the predictions of the trained classifier than going to the original data set [12]. Trepan and REX are some of the pedagogical approaches used for rule extraction from ANNs [4].

II.3.Eclectic or Hybrid Approach

Eclectic approach deals with the rule extraction techniques that incorporate the elements of both the decompositional and pedagogical approaches. For example, SVM model using training set and used to predict the output class labels for training instances and support vectors. Then, decision tree is generated for generating rules from this set of labeled data [1]. Thus, both decompositional features (support vectors) as well as pedagogical features (using SVM to re-label the training instances) are used in this eclectic or hybrid approach.

III. DECOMPOSITIONAL RULE EXTRACTION FROM SVM BY ACTIVE LEARNING BASED APPROACH

A decomposition data mining approach is applied to extract knowledge from a data set, enhances the computational complexity and robustness of knowledge extraction from large data sets resulting in good decision making. The extracted knowledge is used for prediction purposes [16].

Decompositional rule extraction from SVM by active learning based approach (ALBA) was proposed by Martens et al [3]. In this paper, various benchmark data sets like Body fat, Boston Housing, Forest Fires were considered. Martens et al [3] proposed ALBA based approach to extract rules for classification problems. ALBA was specifically proposed to extract comprehensible rules from opaque model such as SVM. Rule extraction from SVM is done by generation of synthetic data near support vectors and so indirectly near the separating hyperplane. Active learning corresponds to generation of synthetic instances. Synthetic data is considered apart from the training set and actual target values are compared with predictions. Rules are generated by applying decision tree (DT), Classification and Regression Tree (CART) etc ability to generate transparent models for regression.

SVM performs classification task and achieves best performance by modelling non-linearity's. The resulting non-linear models are black-box models. However, SVM can also be used for regression problems which appropriate rule extraction methods need to be employed to extract regression rules using ALBA and efficiency can be measured by using root mean square error (RMSE). Active learning focuses on rule induction techniques and discovers discrimination rules, whereas performance is measured in terms of prediction accuracy. ALBA is applied on public datasets and it is

possible to construct comprehensible rules for these datasets. The main steps observed in this approach are

1. Taking data set and running SVM on it and extracting Support Vectors
2. Calculating distance from SVs to training data
3. Generating synthetic or artificial data around the SVs (Learning Step)
4. Labeling the synthetic as well as training datasets using the trained SVM model
5. Generating rules by rule extractors using the re-labeled training and synthetic datasets.

Considering SVM and the original rule extraction approaches in a novel framework using the terms such as *transparent* and *opaque* to categorize the various ways of extracting rules from data .

IV. MK-SVM SCHEME FOR FEATURE SELECTION AND RULE EXTRACTION FROM GENE EXPRESSION DATA OF CANCER TISSUE

The main Obstacle of SVM cannot deliver successful explanation of the computed solutions and present the extracted knowledge in a user-understandable form. Further, there are many parameters that need optimisation in SVM. Parameters such as the type of kernel to be used, Polynomial, Gaussian etc and the kernel parameters such as the degree of polynomial or the centre and width of the Gaussian etc need to be exhaustively searched while developing an accurate SVM model for the given data.

The main characteristic of gene expression data is that it contains a large number of gene expression values . Many genes are highly correlated which leads to redundancy in the data. Hence feature selection has to be performed prior to the implementation of a classification or clustering algorithm [20]. In filter-based method, the data's are pre-processed whereas features are selected using a quality metric, independent of the classifier. Feature selection using wrapper approaches is intimately tied to the classifier. Since wrapper methods are wrapped tightly around a classifier, huge computation time is required and hence are used less.

Multiple Kernel learning (MKL) scheme is proposed because it takes multiple kernels to replace the single fixed kernel by providing more flexibility and chance to choose a suitable kernel to make feature selection and rule extraction in the framework of SVM.

1. The proposed MK-scheme for feature selection and rule extraction is developed.
3. Experimental Results and analysis on two public gene expression datasets, colon tumour dataset and leukaemia dataset.

Efficiency of rules is measured by different parameters like no of rules, conditions per rule, comprehensibility. When rules

need to be learned from datasets, one can use classifiers such as Decision Tree (DT) that directly yield rules, i.e., the knowledge discovered is *transparent* to the user. Alternatively, classifiers such as support vector machine (SVM) can be used that do not directly give set of rules, i.e., the knowledge discovered is *opaque* to the user. Thus knowledge extraction in the form of rules from the given dataset can be viewed as belonging to two categories within the proposed framework, that of *transparent* and *opaque* approaches. Earlier researchers have not viewed the task of knowledge discovery from data in this way and we propose to compare the rules extracted using these two approaches on various parameters such as accuracy, rule comprehensibility, fidelity etc. Proposed to use 10-fold cross validation in all these experiments.

The experiments carried out on selected benchmark datasets taken from the UCI machine learning dataset repository. Firstly proposed the framework for knowledge discovery yielding two approaches i.e., Transparent approach and Opaque approach and secondly various rule extraction techniques such as Decision Trees, Naive-Bayes Tree, Rough Sets and DENFIS (Dynamic Evolving Neuro Fuzzy Inference System) are applied on various benchmark datasets and the results are calculated , evaluated against various rule such as parameters like comprehensibility, sensitivity, specificity and fidelity etc.

V. METHODS AND PROPOSED APPROACHES

The framework depicted in Fig 1 summarizes the proposed framework for comparing knowledge discovery approaches. In both transparent and opaque approaches, different rule induction techniques are used and rules discovered thus are evaluated on different parameters such as fidelity, accuracy, specificity, sensitivity and comprehensibility. Experiments are carried out on different benchmark data sets.

V.1. Decision Tree

This section describes the development of decision trees (DT) for classification tasks. These trees are constructed beginning with the root of the tree and proceeding down to its leaf nodes. Decision tree implementation using J48 algorithm is employed in the experiments reported here. This is available in WEKA, a popular data mining tool. Compared to classifiers such as neural networks and SVM, the knowledge discovered by DT is represented in rules that can be easily understood by humans and also can be used in database query tools such MYSQL for retrieving records falling in a given category. In decision making systems DT is widely accepted and used because of its human understandable structure.

A rule in a DT is obtained by starting at the root of the tree and traversing till leaf node. Class label for a test item is obtained from a decision tree by starting at the root of the tree

and moving through it until a leaf node, which provides the classification of the instance [2].

After obtaining rules the no of antecedents existing in a particular rule is calculated and comprehensibility is measured by calculating the number of rules and the number of antecedents per rule.

In Fig 2, an example decision tree for WBC(WISCONSIN BREAST CANCER) dataset is shown. This tree has 3 leaf nodes and each node has antecedents per rule that are nothing but conditions per rule. From root node to leaf node, each rule is formed. WEKA data mining tool is used in the construction of DT.

2.NBTREE

Naïve Bayes decision tree (NBTREE) is almost similar to DT except at the leaves Naïve-Bayes classifiers exist instead of storing a single class label. NBTREE is a hybrid of decision tree classifiers and Naïve-Bayes classifiers [12]. Bayes rule is used to compute the probabilities of each class using given instances. It requires estimation of conditional probabilities for each attribute value at the given label. Classification at leaf nodes is done by NB classifiers. Compared to DT, in NBTREE probabilities exist at each node and all the sum of the probabilities will be not more than unity [14].

Say, if there are three nodes and probability of a is 0.5, then the probabilities of the remaining two nodes will be, $b = 0.2$ and $c = 0.3$. Sum all the probabilities, it will be equal to 1, but not exceeding 1. The following fig 3 shows an example NBTREE for IRIS dataset generated in WEKA. WEKA is used in the construction of NBTREE.

3.KNN

K nearest neighbors that stores all available cases and classifies new cases based on a similarity measure. This algorithm is a supervised learning algorithm, where the destination is known, but the path to the destination is not.

4. Proposed Approaches

There are two different approaches proposed for Knowledge Discovery in the form of extraction of rules here:

1. Transparent approach
2. Opaque approach

In each approach, four rule induction techniques used to extract rules from the data

4.1. Transparent Approach

Transparent approach is one where the knowledge extracted from the data is transparent to the user. Typically, the classifiers used here for knowledge discovery directly make the knowledge accessible in the form of rules directly.

The Proposed Transparent Approach has the following three important phases:

1. The first phase is to train the classifier using dataset and obtain suitable rules from the given decision system, namely, DTREE, NBTREE, and KNN.
2. The second phase is to evaluate training rules on test set and
3. The third phase measures the efficiency of rules using different rule quality criteria like accuracy, comprehensibility, specificity, sensitivity, number of rules and conditions per rule.

A more comprehensive list of rule evaluation parameters is given below:

1. Accuracy
2. Number of rules
3. Antecedents per rule
4. Comprehensibility
5. Fidelity
6. Sensitivity
7. Specificity

TP^A	C^{AB}	E^{AC}
e^{BA}	T^{PB}	e^{BC}
e^{CA}	e^{CB}	T^{PC}

The parameters for rule evaluation are explained in detail here. Accuracy of a classifier on a given test set is the percentage of test instances that are correctly classified by a classifier.

1. Accuracy of a classifier on a given test set is the percentage of test instances that are correctly classified by a classifier.

$$\text{Accuracy} = \frac{\text{Number of correctly classified instances by rules}}{\text{Total number of instances in test data}} * 100$$

2. Numbers of rules are nothing but the total number of leaf nodes obtained in a tree or all the leaves representing rules.

$$\text{No of rules} = \text{no of leaf nodes}$$

3. Antecedents (number of conditions) per rule represent the number of conditions obtained in each rule. It is denoted as a pair, indicating the number of conditions and the number of rules.

$$\text{Antecedents per rule} = \text{no of conditions / no of rules}$$

4. Comprehensibility of a rule set is determined by measuring the size of the rule set (in terms of number of rules) and the number of antecedents per rule (the average number of antecedents per rule). The sum of number of rules and the antecedents per rule is equal to Comprehensibility. The lower the number, the better is the comprehensibility.

$$\text{Comprehensibility} = \text{Total No of rules} + \text{No of Antecedents per rule}$$

5. Sensitivity is calculated from Confusion Matrix obtained in the model.

Confusion Matrix:

It is dependent on the class labels, here comparison is done between the actual class labels and the predicted class labels by the classifiers. The following describes the case when we deal with two-class classification problem [2].

The generated confusion matrix is $2 * 2$ matrixes.

TP	FN
FP	TN

Sensitivity (TP) and Specificity (TN) are calculated as follows:

$$TP = (TP / TP + FN) * 100$$

$$TN = (TN / TN + FP) * 100$$

Three-class classification problem [13], with generated in order of matrix $3 * 3$ matrix and calculation of various measures are as shown below.

$$TP = TP^A + TP^B + TP^C$$

$$TN = TN^A + TN^B + TN^C$$

Where,

$$TP^A = TP^A / TP^A + FN^A$$

$$TP^B = TP^B / TP^B + FN^B$$

$$TP^C = TP^C / TP^C + FN^C$$

And,

$$TN^A = T^{PB} + T^{PC} + e^{BC} + e^{CB}$$

$$TN^B = T^{BC} + T^{PC} + e^{AC} + e^{CA}$$

$$TN^C = T^{PB} + T^{PC} + e^{BA} + e^{AB}$$

Taking this $3 * 3$ matrix into consideration sensitivity and specificity is calculated as follows

$$TP = (TP / TP + FN) * 100$$

$$TN = (TN / TN + FP) * 100$$

Sensitivity is the proportion of the positive instances that are correctly identified.

$$\text{Sensitivity} = \frac{\text{No of Positive instances Correctly Classified as Positive by Rules}}{\text{Total number of positive instances in Test data}} * 100$$

$$TP = (TP / TP + FN) * 100$$

$$\text{Specificity} = \frac{\text{No of Negative instances Correctly Classified as Negative by Rules}}{\text{Total number of negative instances in Test data}} * 100$$

$$TN = (TN / TN + FP) * 100$$

Thus all the rules are evaluated by calculating these terms. Data sets with attributes and class labels in arff file format (.arff), or (.csv) file formats are taken and applied, then 10-fold cross-validation is performed using rule extractors like DT to get results such as accuracy, confusion matrix with a DT.

4.2. Opaque Approach

Opaque approach is an approach in which the knowledge discovered by the machine learning technique is invisible to the user and to extract elements from the classifier for knowledge extraction. Consider decompositional approach where internal model acquired by the classifier is utilized for knowledge extraction. Using SVM as a classifier, vectors are extracted and inserted to rule extractors like DT, NBTREE. The extracted rules then represent the knowledge discovered by SVM and will be in human comprehensible form. Thus the knowledge embedded in classifiers such as SVM, remaining opaque to the user, and is made transparent by processing via rule induction methods.

SVM, being the high performance yielding machine learning technique, yet fails to make the knowledge learnt by it available in a human comprehensible form. In avoidance, opaque models converted into transparent models by rule extraction.

The Proposed Opaque Approach to Knowledge Discovery has three important phases:

1. The first phase is to insert the original dataset to SVM and obtain Support Vectors and form a data set using support vectors.
2. The second phase is to insert the dataset to rule extractors and suitable rules are obtained from decision systems such as DT, NBTREE, RSES and KNN.
3. The third phase is to evaluate rules and find the efficiency of rules using different rule quality criteria like accuracy, comprehensibility, specificity, sensitivity, No of rules and conditions per rule. Thus rule evaluation follows the same procedure as in the transparent case.

Benchmark classification datasets from UCI repository [18], BC and WBC used. WEKA is used in the construction of J48 i.e., DT, NBTREE and KNN [19]. Support Vectors are obtained using SVM in Rapid Miner [13].

VI.EXPERIMENTATION AND RESULTS

The proposed comparative analysis for knowledge discovery using transparent and opaque approaches is very novel. All the rule extraction techniques used in transparent approach are measured and compared with those used in the opaque approach. Rule extraction is done by two approaches, i.e., with and without using SVM, whereas Rule extraction is done on two datasets, namely, BC and WBC using three different algorithms

DT, NBTREE, and KNN. Comparison is done between these two approaches of knowledge discovery and best rule extraction approach and technique are identified.

VII.DESCRIPTION OF DATASETS USED IN THE PROPOSED APPROACHES

Datasets namely BC and WBC are taken as text files and loaded into excel sheet and converted into (.CSV) file format. And also ARFF format files are prepared using notepad and saving them in (.arff) format for using in WEKA to work with DT NBTREE and KNN modules therein. Now 10-fold cross validation is done and rules are obtained. In Table 1 shown below, various features of the three classification datasets such as instances, attributes, and class labels

TABLE-1

Dataset	No of Instances	Attributes	Decision Classes
BC (Breast Cancer)	286	9	2
WBC (Breast Cancer)	699	10	2

On each dataset 10-fold cross validation is applied and DT, NBTREE, and KNN are constructed, whereas the rules are extracted. BC has a total of 86 instances with nine attributes and 2 class labels. It is a 2-class classification problem. WBC has 699 instances with 10 attributes and 2 classes. It is a 2-class classification problem.

Firstly, original data sets are inserted to SVM implemented in Rapid Miner tool and then support vectors are obtained. The process of making input files for WEKA tool is as described. The only difference here in opaque case is that additionally, support vectors as well as the corresponding class labels are also extracted.

For each dataset, support vectors are extracted and used as training sets for rule extractors such as, DT, NBTREE, RSES and DENFIS. Then validation of rules is done on test set, computing measures such as accuracy, sensitivity, specificity, and comprehensibility. As mentioned, the transparent approach measure Fidelity which is irrelevant as rules are obtained directly from the classifier itself. So, fidelity values are shown only for the opaque case. The results obtained by following different rule extractors are described in the tables below and comparison for each rule extractor is done on these two data sets using transparent and opaque approaches.

VIII. RESULTS ANALYSIS OF WBC DATASET

The following tables summarize a comparative analysis between transparent and opaque approaches of knowledge discovery using different rule extractor techniques on BC and WBC datasets.

IX. RULE EXTRACTION USING DTREE

DT	WBC	SV-WBC
10-fold Accuracy	93.99%	92.98%
Sensitivity	93.47%	84.61%
Specificity	95.5	58.8
Number of Rules	20	4
Conditions per Rule	118/20	9/4
Comprehensibility	26	6

By comparing overall results between the two approaches, accuracy of DT in transparent approach is 93.99% compared to a comparable value of 92.98% for the opaque approach. Also, sensitivity and specificity are good in transparent approach and comprehensibility good in opaque approach compared to transparent approach.

X. RULE EXTRACTION USING NBTREE

NBTREE	WBC	SV-WBC
10-fold Accuracy	95.85%	94.76%
Sensitivity	95.7	88.46
Specificity	96.6	96.59
Number of Rules	10	2
Conditions per Rule	37/10	4/2
Comprehensibility	5	4

The accuracy is very high in transparent approach and RMS error is very high for opaque approach.

XI. RULE EXTRACTION USING DTREE

DT	WBC	SV-WBC
10-fold Accuracy	75.17%	75.08%
Sensitivity	0.32	0.06
Specificity	0.06	0.67
Number of Rules	3	3
Conditions per Rule	5	5
Comprehensibility	8	8

By comparing overall results between the two approaches, accuracy of DT in transparent approach is high 75.17% compared to a comparable value of 75.08% for the opaque approach. Also, sensitivity and specificity are good in transparent approach and comprehensibility is good in opaque approach compared to transparent approach.

XII. RULE EXTRACTION USING NBTREE

NBTREE	WBC	SV-WBC
10-fold Accuracy	74.12%	74.03%
Sensitivity	0.28	0.92
Specificity	0.06	0.69
Number of Rules	10	3
Conditions per Rule	42	5
Comprehensibility	52	8

By comparing overall results between the two approaches, accuracy of NBTREE in transparent approach 74.12% and is comparable (74.03%) to that obtained in opaque approach. Also, sensitivity and specificity is good in transparent approach and comprehensibility is found to be good in opaque approach compared to transparent approach.

XIII. RULE EXTRACTION USING KNN

KNN	WBC	SV-WBC
10-fold Accuracy	63.63	65.26
RMSE	0.53	0.53
Sensitivity	0.38	0.80
Specificity	0.34	0.71

The accuracy is high in opaque approach and RMS error is same in both approaches.

XIV. RESULTS

Two approaches such as transparent and opaque compared. In the transparent approach classifiers that yield rules directly from data are used and in the opaque approach, the knowledge gained, by a black-box classifier like SVM, is extracted by rule induction techniques. Two UCI machine learning benchmark datasets, namely, WBC and BC datasets are used in all the experiments. Three

rule induction methods, namely, DT, NBTREE, and KNN.

Overall, measures such as classification accuracy, sensitivity and specificity, transparent approaches are superior. DT and NBTREE appear to give good or comparable results across the two knowledge discovery approaches. The accuracy results of the K-Nearest Neighbor (KNN) are poor for the BC datasets, however DT consistently yields fewer rules and hence comprehensibility of rules works out to be superior.

From the results, the process of extracting the knowledge acquired by black-box classifiers like SVM has a loss of accuracy, sensitivity and specificity. Although SVM is generally a superior classifier compared to DT and NBTREE, while making the knowledge acquired by SVM transparent, acquire loss of accuracy. Thus it is better to use the transparent rule induction methods such as DT and NBTREE as efficient methods directly for knowledge discovery.

XV. CONCLUSION AND FUTURE WORK

In this paper, Two benchmark datasets from UCI machine learning repository are utilized namely, BC and WBC datasets. The black-box classifier chosen is the support vector machine (SVM). Three rule induction methods belonging to different categories of computational intelligence techniques namely, inductive learning method such as DT, probabilistic method such as Naïve Bayes Decision Tree (NBTREE), and Nearest Neighbor (KNN) are taken for experiments of both the approaches. In the opaque case, SVM is used as a pre-processor only, where only the support vectors are used further for rule extraction. Ten-fold cross-validation (CV) is performed on both the approaches. Evaluation of the rules extracted is done using measures such as ten-fold cross-validation accuracy, sensitivity, specificity, total number of rules extracted, number of conditions per rule, comprehensibility.

Results indicate that transparent approach yielded good performance overall the datasets in terms of classification accuracy, sensitivity and specificity. The DT and NBTREE rule extraction techniques gave superior performance when used in the transparent mode than combined with a black-box model as in the opaque approach. Although the SVM is a superior classifier as a standalone technique, in the process of making the hidden knowledge transparent there seems to be loss of accuracy. Also, KNN did well as standalone methods rather when combined with SVM. Thus transparent approach to knowledge discovery from data is recommended over opaque approach.

The scope of future work for this paper is improving rule extraction part and accuracy in opaque approach. A good selection of rules can increase the performance even greater. By using Rough Sets algorithms like LEM2 can be used for obtaining best possible rules in RSES and DT,

NBTREE in WEKA. Filtering of rules can also be improved by selecting rules from each decision class instead of taking rules with greater support.

References

- [1] Andrew Kusiak. Decomposition in Data Mining: An Industrial Case Study in IEEE Transactions On Electronics Packaging Manufacturing, Vol. 23, No. 4, 87-97, 2000.
- [2] Confusion Matrix
<http://www.compumine.com/web/public/newsletter/20071/precision-recall>
- [3] David Martens, Bart Baesens, and Tony Van Gestel. Decompositional Rule Extraction from Support Vector Machines by Active Learning. IEEE Transactions On Knowledge And Data Engineering, Vol. 21, No. 2, 352-358, 2009.
- [4] H. Nunez, C. Angulo, and A. Catala. Rule Extraction from Support Vector Machines. In Proceedings of European Symposium On Artificial Neural Networks (ESANN '02), pp. 107-112, 2002.
- [5] Jiawei Han, Micheline Kamber, Data Mining Concepts and Techniques. Morgan Kaufman Publishers, 2001.
- [6] M.A.H. Farquad, V. Ravi and S. Bapi Raju, "Rule Extraction using Support Vector Machine Based Hybrid Classifier", TENCON-2008, IEEE Region 10 Conference, Hyderabad, India, November 19-21, 2008.
- [7] M. A. H. Farquad. Rule Extraction from Support Vector Machine. PhD Dissertation, Department of Computer and Information Sciences, University of Hyderabad, Hyderabad, India, 2010.
- [8] M. W. Craven. Extracting Comprehensible Models from Trained Neural Networks, PhD thesis, Department of Computer Science, University of Wisconsin-Madison, USA, 1996.
- [9] Nahla Barakat and Joachim Diederich. Learning-based rule-extraction from support vector machines: Performance on benchmark datasets. In Proceedings of the conference on Neuro-Computing and Evolving Intelligence, Knowledge Engineering and Discovery Research Institute (KEDRI), Auckland, New Zealand, 13-15, 2004.
- [10] Payam Refaeilzadeh, Lei Tang, Huan Liu. Cross Validation. In Encyclopedia of Database Systems, 532-538, Springer, U.S, 2009.
- [11] <http://rapid-i.com/content/view/26/84/lang.en>
- [12] Ron Kohavi. Scaling Up the Accuracy of Naïve-Bayes

Classifiers: a Decision Tree Hybrid. In Proceedings of KDD-96, Portland, USA, 202-207, 1996.

- [13] R. Quinlan. Induction of decision trees. Machine Learning, vol. 1, 81-106, 1986.
- [14] UCI Machine Learning Repository, <http://archive.ics.uci.edu/ml/>
- [15] WEKA <http://www.cs.waikato.ac.nz/ml/weka>
- [16] Zhenyu Chen, Jianping Li, Liwei Wei, "A multiple kernel Support Vector Machine scheme for feature selection and rule extraction from gene expression data of cancer tissues", Artificial Intelligence in Medicine, vol. 41, 161–175, 2007

XVI. FIGURES AND TABLES

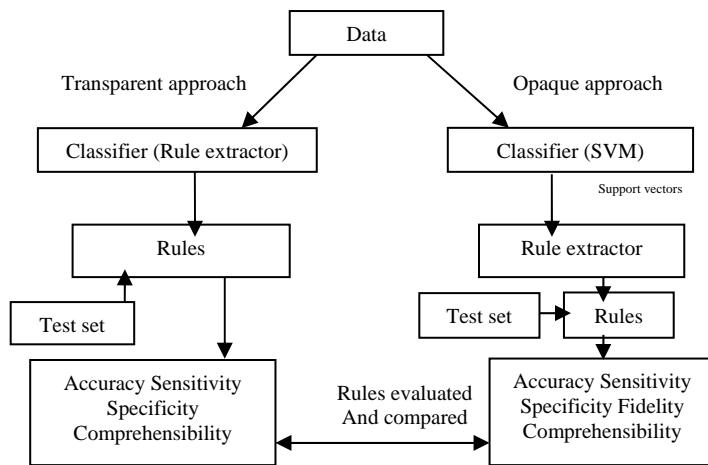


Fig 1: Flow Chart representing the proposed approaches.

SV-WBC: This is the DT we obtained in Opaque approach for WBC dataset.

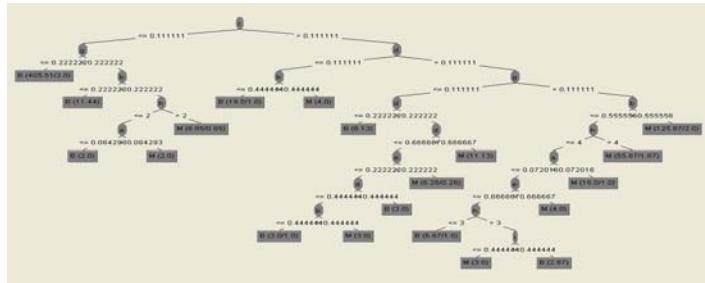


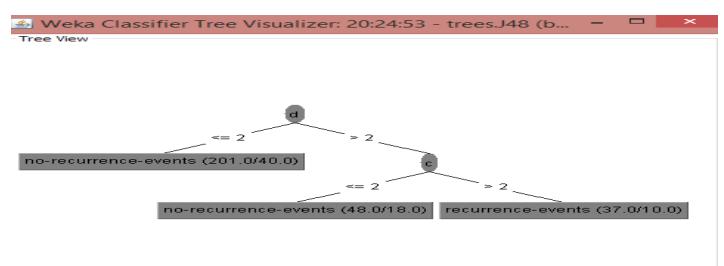
Figure A.5 DT in Transparent Approach for WBC



Figure A.6 DT for WBC in Opaque Approach

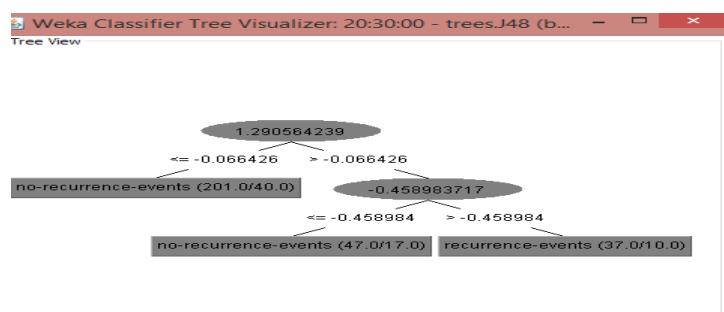
BC:

BC:Transparent approach



BC: Opaque approach

Opaque approach



NBTREE Rules

Rules obtained from NBTREE are presented below in a tree format. Each Rule is calculated from root node to leaf node. All the following NBTREES are obtained from the WEKA tool.

WBC

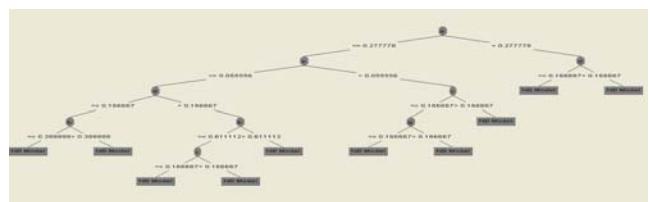


Figure B.5 NBTREE for WBC using transparent Approach

SV-WBC

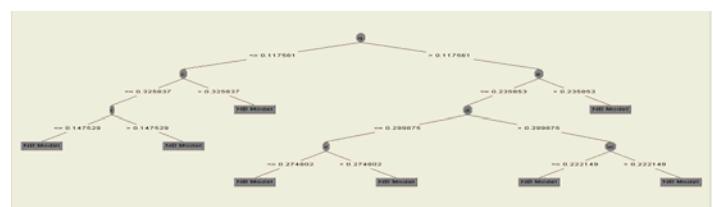
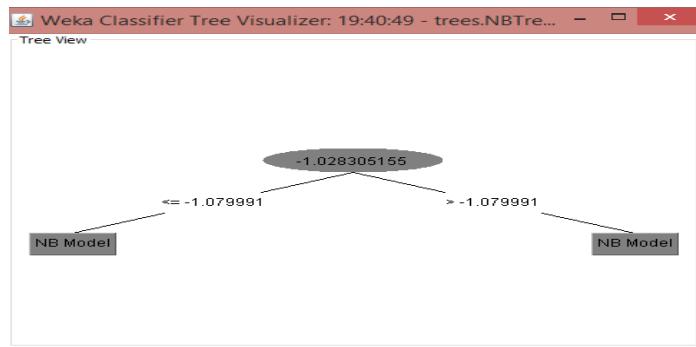


Figure B.6 representing NBTREE for WBC using Opaque Approach

BC



AUTHORS PROFILE

1.Dr.Umamaheswari

Faculty,Computer Science department ,
Majmaah University
Saudi arabia

2.Mrs. Jabeen Sultana

Faculty,Computer Science department ,
Majmaah University
Saudi arabia

3.Mrs.Ruhi Fatima

Faculty,Computer Science department ,
Majmaah University
Saudi arabia

A STUDY ON OPTIMIZING THE EFFICIENCY OF LOCATION AIDED ROUTING PROTOCOL (LAR)

Priyanka Kehar

Lovely Faculty of Technology and Sciences
Lovely professional University
Phagwara, India

Pushpendra Kumar Pateriya

Lovely Faculty of Technology and Sciences
Lovely Professional University
Phagwara, India

Abstract-The improvised network is an arrangement less network consisting of portable nodes. VANETs is the recently developed technique to achieve traffic safety and efficiency through inter vehicle communication, where routing protocol plays a vital role. Inefficient path establishment and network congestion both bring the severe degradation in network throughput and performance. Routing throughput and enactment is largely reliant on the stability and availability of the wireless link which makes it a very pivotal factor, that can't be ignored in order to obtain proper performance and throughput measurement in vehicular improvised network. As vehicle nodes have higher mobility due to which some prediction based techniques were proposed in previous times for path establishment. Among the proposed prediction based techniques, location aided routing protocol influence real time vehicular information to generate path between source and destination, with high possibility of network connectivity among them. The main feature of optimized LAR is: minimize the delay, minimize the fuel consumption, and maximize the throughput.

Keywords-Road Side Unit (RSU); Location Aided Protocol (LAR); Internet Service Provider (ISP); Intelligent Transport Service (ITS).

I. INTRODUCTION

VANETs present a quickly rising, testing class of MANETs. VANET is portrayed by a high hub versatility and restricted level of flexibility in the portability design. Henceforth, Ad-hoc convention adjust consistently to the temperamental conditions, whence developing exertion in the advancement of correspondence conventions which are particular to vehicular systems [1]. VANETs are led with moving vehicles and roadside foundation in view of high portability and persistent topological changes happen. VANETS is a self-coordinated and self composable remote

correspondence system, where vertices incorporate themselves either as customer or server for correspondence [8]. Author explained packet drop ratio increases due to low success ratio at destination side [21]. VANETs are relied upon to bolster a huge requested exhibit of segments of migrant circulated application that range from ready scattering of activity and dissemination of records [22]. In TABLE 1 we have shown a brief layered view of vehicular architecture that where it works, what is the scope of this improvised network and how it communicates.

TABLE 1: LAYERED VIEW OF VEHICULAR NETWORK

Vehicular Network	Application Type	Safety Intelligent transportation Comfort applications
	QoS	Non real time Soft real time Hard real time
	Scope	Wide area Local area
	Network Type	Ad-hoc Infrastructure based
	Communication Type	V2V V2I

Based on unique characteristics, the vehicular communication has been categorized into two parts:

- 1) Vehicle to Vehicle communication (V2V)
- 2) Vehicle to Infrastructure communication (V2I) [8].

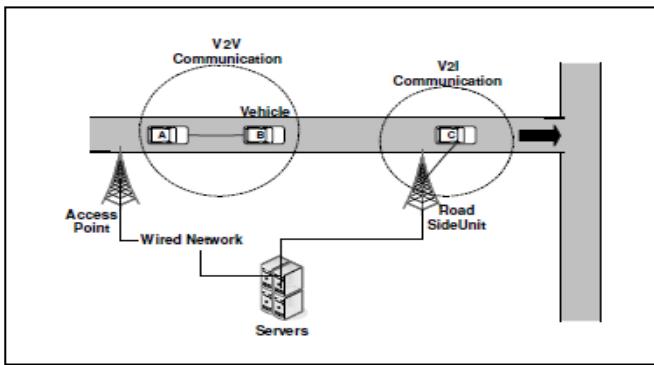


Figure 1. Communication Architecture

As shown in Figure 1, when the vehicles are speaking with the road side unit (RSU) or transmitting the messages with the side framework then this procedure is known as V2I. Then again when vehicles are transmitting information with each other are known as V2V. This V2V correspondence requires some exceptional equipment in the autos like actuator.

In this paper, we have discussed about the LAR protocol, its shortcomings and proposed a novel technique to overcome the problem of Broadcasting in LAR protocol. After that we compare the novel technique with the existing LAR protocol graphically and observe the throughput of the network and delay in transmitting a message.

The rest of the paper follows the process like this. In section II we describe literature survey. In Section III LAR protocol is reviewed. In section IV Proposed technique is being defined. In section V Algorithm is being defined and experimental results are described in section VI. In section VII Conclusion and Future scope is presented followed by the References in section VIII.

A. Challenges

It is vital to specify the important challenges in VANET:

- **Signal fading and distortions:** Objects like different vehicles or structures go about as impediments between two conveying vehicles which is one of the test that can influence the effectiveness of VANET.
- **Bandwidth limitations:** Nonappearance of a focal organizer that controls the correspondences amongst hubs, and which has the obligation of dealing with the data transmission and conflict operation.
- **Connectivity:** Owing from the high portability and fast changes of topology, which prompt an incessant discontinuity in systems, the time length required to lengthen the life of the connection correspondence ought to be to the extent that this would be possible.
- **Small effective diameter:** Owing to the small effective network diameter of a VANET, that leads to a weak connectivity in the communication between nodes.

- **Routing protocol:** In view of the high versatility of hubs and fast changes of topology, outlining an effective directing convention that can convey a parcel in a base timeframe with few dropped bundles is thought to be a basic test in VANET.

II. LITERATURE REVIEW

To optimize the efficiency of the LAR protocol first of all we need to know some of the things that is being reviewed:

A. Performance of AODV and OLSR

It is suggested that vehicular improvised system is scientific classification class of MANETs that honest to goodness remote correspondence among all the different vehicles. In the VANET steering convention and other capability must be obliged to vehicular particular capacities and necessities. In the former examination directing execution is exceptionally depending on the accessibility and steadiness of the remote connections. In the directing calculation that have been examined as of now are contrasted in the previous faking and the correlation that are finished by stochastic motion. In the examination they measure the execution of AODV and OLSR in a citified diagram. It likewise ponders the distinctive conventions under the assorted measurements like vertex portability and vehicle smallness with various movement [1]. [24] Thinks about the execution of the steering conventions in vehicular system environment. The goal of this work is to evaluate the pertinence of these conventions in various vehicular activity situations. Both the position-based and topology-based steering conventions have been considered for the study. The topology-based conventions AODV and DSR and position-based convention LAR are assessed in city and interstate situations. Furthermore, the position based directing convention gives preferable execution over topology based steering conventions regarding bundle conveyance proportion, throughput, and end-to-end delay for both the vehicular activity situations.

B. Vertex Mobility

By resources and investigation, the primary occasion of calculation on system steering from base up proposition has been supported by consolidated conduct of social bugs, for example, honey bees and ants. This session of bio-propelled directing calculations includes a similarly colossal number of calculations usually created in a year ago and fundamentally empowered by insect province conduct. It clarifies the generally held off occurrence of swarm knowledge calculation for steering [5]. The vehicles are the vertices of the system. VANETs gives the practical as an ITS. In fuel system engineering and vertex portability highlight separate VANET from rest of the improvised system. The charge adjustment in topology diminish the steering strong period. Directing is the confound assignment in improvised system [11].

C. Locating the Destination

In VANETs to begin the correspondence area based administration, the situating vertex ought to be found. It had been intended for citified zone topology which utilize vertices

data like separation of crossing point essential issue and speed in picking stable server for area, in this the formation of majority area server will be performed by fundamental server of that area by delegating other found vertices at the convergence relying upon their portability heading. The majority is being utilized to spread burden on numerous servers with the end goal of adaptation to internal failure. Additionally, the forecast calculation is utilized to permeate the clamor information and bring for the exact area of destination and conquer the issue of non-current information put away in gathered framework. It lessens the overhead and end to end postponement of steering bundle [13].

D. Overcrowded Traffic

Here every one of the gadgets transmit the information with the use of radio gadgets. Vehicle congestion is ruminating as deferral while venture. Congestion of activity can be figured utilizing different traditions like television of information bundles, extent of parcel supplied and extent of movement hive off. The feigning show case the space of vehicle congestion [12].

E. Packet Delivery Ratio

Scrimpy forwarding nodes and overcrowding network both demean the working of routing in VANETs. So an accommodative methodology in light of the gathering of two circumstance and use the strategy to the LAR convention to keep it from corruption has been created. In this versatile procedure MADM plan has been proposed to suit control capacities for message transmission. Trial examination and recreation working show that this technique can propel the bundle conveyance proportion (PDR) of LAR convention productively [14]. OLSR utilizes the capability of flooding for looking the destination which make the overheads. To subdue the problem, we use the MPR (Multi Point Relay) which helps to decrease the number of messages broadcasted during this proficiency [18].

III. LAR PROTOCOL

Location Aided Routing (LAR) protocol is position based routing protocol. It is on demand routing protocol which is similar to Dynamic Source Routing (DSR) protocol. To improve performance of routing protocols for VANET, we show how a route discovery protocol based on flooding can be improved.

LAR limits the search for a new route to a smaller request zone, thereby resulting in *reduced* signaling traffic. LAR defines two concepts: (a) expected zone, and (b) request zone. However, LAR makes several assumptions. First, it assumes that the sender has advanced knowledge of the destination location and velocity. Based on the location and velocity, the expected zone can be defined. The request zone, however, is the smallest rectangle that includes the location of the sender and the expected zone. With LAR, the sender explicitly specifies the request zone in its route request message. Node that receive the request message but do not fall within the request zone discard the packet. This, therefore, acts as a limiting boundary on the propagation of the route request

message [23]. This is known as the LAR1 scheme. The other scheme is to consider a route that has a shorter physical distance from the source to the destination node. In Figure 2 we have described how the LAR routing protocol works.

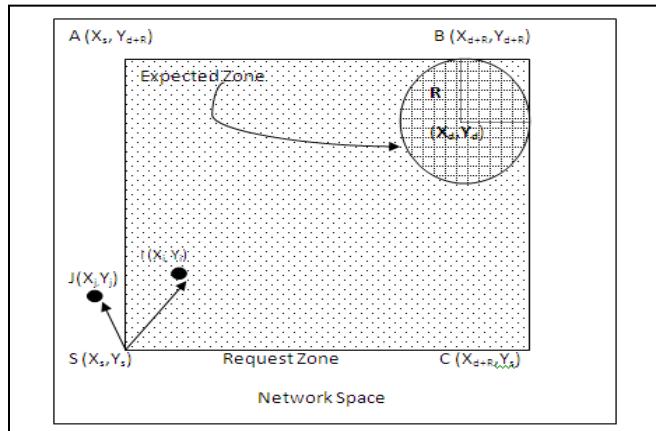


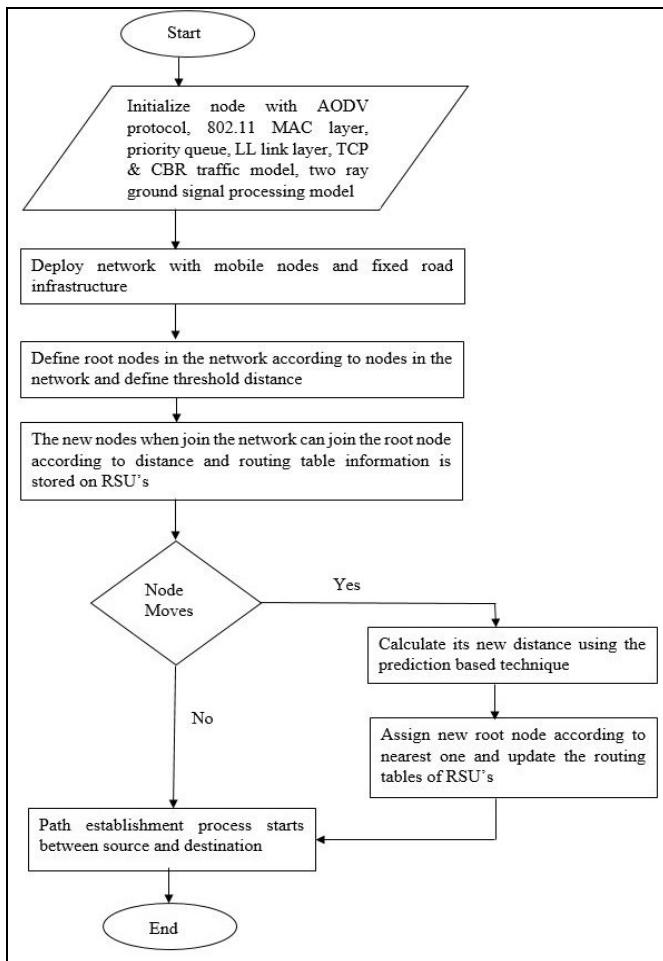
Figure 2. LAR Routing Protocol [23]

IV. PROPOSED TECHNIQUE

In the vehicular adhoc network, vehicle to vehicle and vehicle to infrastructure communication is available for communication. To vehicle to vehicle communication is available to exchange important information between vehicles. To establish path between various vehicles various routing protocols had been proposed which are of reactive and proactive type. The reactive routing protocols had remarkable performance in VANETS which use the broadcasting technique for path establishment. The broadcasting technique will increase delay in the network and network resource consumption increase at steady rate. To reduce delay in the network, the technique of multicasting has been proposed. The following are various assumptions of the proposed technique

- The network will be deployed with the fixed number of nodes and roads structure already defined
- Every node is responsible to maintain the table of its adjacent nodes
- Some nodes in the network are predefined as root nodes for multicasting nodes

In the proposed technique, in whole network we define some nodes which are root nodes, under these root nodes we will defines the leaf nodes. The leaf node comes under which root that will be decided by prediction based technique for multicasting. In Flow Chart we have defined the step wise procedure about our work that how we have proceeded in it.



Flow Chart: Way of Processing

V. ALGORITHM

Input: Road Side Units, Smart Cars

Output: Message passes from Source to Destination through Multicasting

1. Set M Mobile Node's
 2. Set S sender and R receiver
 3. Node Routing = AODV
 4. Set Route
 5. **If** (route from S to R found)
 6. Check number of route;
 7. **If** (route greater than equal 1) //means alternative route exist in network
 8. Find nearest neighboring nodes
 9. Create path through root nodes
 10. Send route acknowledge of establishment through root node
- 11. Else**
12. Root unreachable

13. End if
14. End if
15. New root node formation;
16. Source node start sending data to destination through root node
17. Increment-Q;
18. Store incoming data;
19. Receiver receives data from I node;
20. Send ACK to sender S;

VI. EXPERIMENTAL RESULTS

The examination work has been executed utilizing NS2. There are reproductions of TCP and UDP, some of MAC layer conventions, different steering and multicast conventions over both wired and remote system and so forth. What's more, the after effects of examination of both the systems utilizing different parameters are given in TABLE 2.

TABLE 2: SIMULATION PARAMETERS

Network Simulator	NS-2 Version 2.35
Window Size	800 X 800
Number of Mobile Nodes	35
Signal Processing Model	Two Ray Ground
Transmission Range	18m
MAC Layer	802.11
Link Bandwidth	2.4 GHz
Routing Protocol	AODV
Traffic Model	TCP, CBR
Maximum Node Speed	200 m/s



Figure 3. Fuel Emission

Here, in this Figure 3, x-axis denotes the time and y-axis denotes the number of packets loss. Red line indicates that old technique consumes more fuel and green line indicates consume less fuel in proposed technique. So, new technique is better than existing technique.



Figure 5. Throughput Comparison Graph

In Figure 5, red line indicates throughput of old technique and green line indicates throughput of proposed technique which is less than old technique. Here, x-axis denotes the time and y-axis denotes the energy in joules. The existing scenario where broadcasting is used have throughput 60 packets and in the proposed scenario throughput is 65 packets. So, proposed technique shows better results.

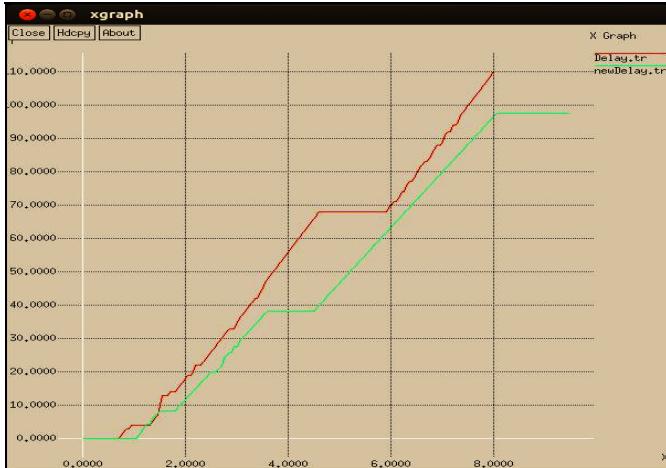


Figure 4. Comparison Graph of Delay

In Figure 4, red line indicates delay of old technique. Green line indicates the delay of new technique. Here, x-axis denotes the time and y-axis denotes the number of packets. In the broadcasting scenario delay is 10 packets and in the proposed scenario delay is 9 packets. From the above graph, it proves that proposed technique is better than the existing one.

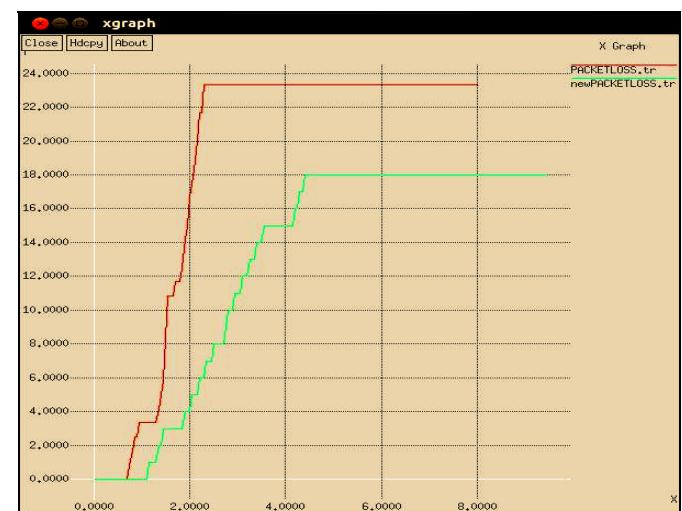


Figure 6. Comparison of Packet Loss

In Figure 6, red line indicates packet loss of old technique. Green line indicates the packet loss of new technique. Here, x-axis denotes the time and y-axis denotes the number of packets. In the existing scenario packet loss is 23 packets and in the proposed scenario packet loss is 18 packets. From the above graph, it proves that proposed technique is better than the existing one.

VII. CONCLUSION AND FUTURE SCOPE

In this research, location aided routing protocol has been chosen for routing. The whole network is divided into probability zones. Due to broadcasting, network resources are wasted and network becomes inefficient. Inefficient network decreases the performance and throughput of the network and also delay in communication increases respectively. To defeat this, issue a proposed strategy will be utilized based after multicasting and enhance effectiveness of the system. In proposed system, tree based multicasting plan will be utilized to expand the execution of the system.

NS2 reproduction instrument is utilized for the usage of both the strategies. Toward the end, there will be examination of both the methods and the outcomes are investigated graphically. The parameters utilized for execution correlation are throughput, defer and fuel discharge. It has been watched that the multicasting strategy indicates preferable results over the broadcasting technique.

Position based steering convention like LAR convention, requires data about the physical position of the taking an interest hub, have not been concentrated on that much and require more consideration. As in this examination, multicasting tree upkeep system is proposed in LAR convention. Whatever other strategy will likewise be proposed in future work. Some different parameters can likewise be utilized for the execution correlation as a part without bounds.

VIII. REFERENCES

- [1] Jerome Haerri Institut Eur'ecomz Department of Mobile Communications B.P. 193 06904, Sophia Antipolis, France," Performance Comparison of AODV and OLSR in VANETs Urban Environments under Realistic Mobility Patterns" (2005) p1-8.
- [2] Vasundhara Uchhula Dharamsinh Desai University Nadiad, Gujarat, India," Comparison of different Ant Colony Based Routing Algorithms" (2006) p1-5.
- [3] Jason J. Haas and Yih-Chun Hu University of Illinois at Urbana-Champaign Urbana, Illinois, U.S.A," Real-World VANET Security Protocol Performance" (2007) p1-7.
- [4] Josiane Nzouonta, Neeraj Rajgure, Guling Wang, Member, IEEE, and Cristian Borcea, Member IEEE," VANET Routing on City Roads using Real-Time Vehicular Traffic Information" (2008) p1-18.
- [5] Muddassar Farooq and Gianni A. Di Caro Next Generation Intelligent Networks Research Center National University of Computer and Emerging Sciences (NUCES) Islamabad, Pakistan," Routing Protocols for Next Generation Networks Inspired by Collective Behaviors of Insect Societies: An Overview" (2008) p1-60.
- [6] Caelos de morais cordeiro and dharma p.agrawal," mobile ad-hoc networking" p 61-63, IIESE, Vol. 3, issue 2, (2009).
- [7] Bilal Mustafa Umar Waqas Raja School of Computing Blekinge Institute of Technology Box 520 SE – 372 25 Ronneby Sweden," Issues of Routing in VANET"(2010).
- [8] Vishnu Kumar Sharma1 and Dr. Sarita Singh Bhaduria Department of CSE, JUET, India," Congestion and Power Control Technique Based on Mobile Agent and Effect of Varying Rates in MANET" (2011).
- [9] Rakesh Kumar, Mayank Dave department of IT, M.M. University, Mullana, Haryana, India , "A Comparative Study of Various Routing Protocols in VANET"(2011) p643-648.
- [10] Reena Dadhich Department of MCA, Govt. College of Engineering, Ajmer, India, "Mobility Simulation of Reactive Routing Protocols for Vehicular Ad-hoc Networks" (2011).
- [11] Aswathy M and Tripti Department of Computer Science & Engineering, Rajagiri School of Engineering & Technology, Rajagiri valley, Cochin, India," a cluster based enhancement to AODV for inter-vehicular communication in VANET"(2012) p41-50.
- [12] PATIL V.P.Smt. Indira Gandhi college of Engineering, New Mumbai, INDIA,"Vanet Based Traffic Management System Development and Testing Using AODV Routing Protocol" (2012) 1682-1689.
- [13] Salim M.Zaki, M.A.ngadi,Maznah Kamat," A location based routing predicton service protocol for vanet city environment"(2012).
- [14] N. Brahmi, M. Boussedjra, J. Mouzna, and M. Bayart, "Road connectivity-based routing for vehicular ad hoc networks," 2010 International Conference on Advanced Technologies for Communication (ATC), pp. 255–259, October 2010.
- [15] M. Ayaida, M. Barhoumi, H. Fouchal, Y. Ghamri- Doudane, and L. Afifl, "PHRLS: A movement- prediction-based joint routing and Hierarchical Location Service for VANETs," 2013 IEEE Int. Conf. Commun., pp. 1424–1428, 2013.
- [16] X. Du, D. Wu, W. Liu, and Y. Fang, "Multiclass routing and medium access control for heterogeneous mobile ad hoc networks," IEEE Transactions on Vehicular Technology, vol. 55, no. 1, pp. 270–277, January 2006.
- [17] T. G. Basavaraju, S. K. Sarkar, C. Puttamadappa, and M. A. Gautham, "Ecarp: An efficient congestion adaptive routing protocol for mobile ad hoc networks," 2006 6th International Conference on ITS Telecommunications Proceedings, pp. 715–718, June 2006.
- [18] S. Sekhon and D. Kumar, "Optimizing the Ad-hoc Applications in Vehicular Network : A Study," vol. 3, no. 6, pp. 2406–2408, 2014.
- [19] R. Kumar and M. Dave, "A Review of Various VANET Data Dissemination Protocols," vol. 5, no. 3, pp.27–44, 2012.
- [20] J. Meng, H. Wu, H. Tang, and X. Qian, "An Adaptive Strategy for Location-Aided Routing Protocol in Vehicular Ad Hoc Networks," 2013.
- [21] N.D.M. Nuri and H. Hasbullah, " Stratery for efficient routing in VANET", 2010 International Symposium in Information Technology (ITSIM), Kuala Lumpur, pp. 903-908, June 2010.
- [22] S. Dashtinezhad, T. Nadeem, B. Dorohonceanu, C. Borcea, P. Kang, and L. Iftode, "Traffic view: A driver assistant device for traffic monitoring based on car-to-car Communication", in Proc. 59th IEEE Semannual Veh. Technol. Conf., Milan, Italy, May 2004, pp. 2946- 2950.
- [23] Sanjoy Das and D.K Lobiyal, "A Performance Analysis of LAR Protocol for Vehicular Ad Hoc Networks in City Scenarios", Oct. 2012.
- [24] Akhtar Husain, Ram Shringar Raw, Brajesh Kumar and Amit Doegar, "Performance Comparison of Topology and Position Based Routing Protocols in Vehicular Network Environments", *International Journal of Wireless & Mobile Networks*, vol. 3, no. 4, August 2011

ANALYZING AND PROCESSING DATA FASTER BASED ON BALANCED PARTITIONING

Annie .P. Kurian
Dept. of Computer Science & Engg.
Velammal Engg. College
Chennai, India

Prof. Dr. V. Jeyabalaraja
Dept. of Computer Science & Engg.
Velammal Engg. College
Chennai, India

Abstract— Big data has become a well-known buzzword to the public at large which handles enormous amount of data i.e., in terabyte to zeta byte. Processing and analyzing such huge amount of data is not possible with traditional and conventional environments. The existing system approaches for range partition queries are deficient to rapidly provide definite results in big data. In this paper, we propose a agile approach to range-aggregate queries in big data documents/table using balanced partitioning. This approach first divides the big data into independent partition with balanced partitioning, and then it generates a local estimation sketch for each partition. When a RA-query request arrives, the system quickly fetches and obtains the result directly by compiling local estimation from all partitions. The balanced partitioning avoids the overall scan of the data in order to provide the result. Big data ecosystem like HIVE and Impala is used to handle the structured data and uses the balanced partitioning to provide fast and accurate output. Partitioning provides maintenance, availability and improvised query performance to the users. It reduces the time complexity, i.e., O(1) time complexity for data updates. The overall performance of the dataset produced would be efficient, fault-tolerant, accurate and fast.

Keywords – range aggregate, big data, HIVE, Impala, partition, map reduce, HDFS.

1. INTRODUCTION

Over the past few years, there has been a significant shift in data storage, management, and processing. Organizations are storing more data from more sources in more formats than ever before. Organizations are finding new ways to use data that was previously believed to be of little value, or too expensive to retain, to better oblige their constituents. Sourcing and storing data is one half of the equation. Processing that data to produce beneficial information is rudimentary to the daily operations of every modern organization/industry.

Due to the massive data in today's world, the traditional system mechanism becomes difficult to handle these large amounts of data. The traditional techniques are meant for handling only structured data. The processing becomes unfeasible and non-scalable after certain amount. So, that is when Big Data came into existence, which handles tremendous amount of data.

Big data is an extensive term for data sets so vast or complex that traditional data processing applications are inadequate. Challenges in big data include analysis, capture, search, transfer, storage, sharing, visualization, and information privacy. Big Data is meant for its prodigious “Volume, Velocity, Variety and Veracity. Big data handles three types of data. They are:

- Structured data,
- Semi-Structured and
- Unstructured data.

Big data brings with it two rudimentary challenges: how to store and execute with voluminous data's, and also how to perceive data and turn it into a competitive advantage. Hadoop fills a gap in the industry/market and organization by effectively storing and generating computational capabilities over substantial amounts of data.

So, Hadoop is an open source framework for writing and processing distributed applications that process large amounts of data using simple programming models like map reduce. Distributed computing is an extensive and assorted field, but the key distinctions of Hadoop are that it is:

- **Accessible**—Hadoop runs on large clusters of machines or on cloud computing services such as (EC2).
- **Robust**— Hadoop is robust because it can gracefully handle most failures i.e., fault-tolerance.
- **Scalable**—Hadoop scales linearly to handle multiple nodes to the cluster.
- **Simple**—Hadoop grant end users to quickly write efficient parallel code.

HDFS is a distributed file system (DFS) which is highly – fault tolerant and yields high throughput access to application data and is highly suitable for large data sets. The HDFS consists of three daemons i.e., Namenode, Secondary

Namenode and Datanode. The programming model used in Hadoop is Map Reduce (MR). Map Reduce is the data processing functionality used in Hadoop which includes splitting the entire data/task into two parts, known as map and reduce. The Map Reduce function analysis process is done based on the [Key, Value] pair. In MR, the input data is divided into no. of chunks and passed to the mapper function. At a high-level, mappers read the data from HDFS, process it and generates intermedial results, then the shuffling of data happens which combines the similar data and send it to the reducers. Reducers are used to aggregate the intermediate results from the mapper, and are used to generate the final output which is again written to the HDFS.

The traditional system is meant for handling only structured data. The range aggregate query in the past system has row-oriented partitioning and also has only limited processing of data. In the traditional system the updation process and handling large amount of structured data was difficult and result produced was inaccurate. Also the result was obtained slowly.

Hive is a data warehouse structure built on Hadoop core that provides data summarization, adhoc querying and analysis of datasets. Hive is a sub platform in the Hadoop ecosystem and provides an SQL dialect, called Hive Query Language (HiveQL or just HQL) for querying data stored in a Hadoop cluster. This language is compiled by Map Reduce and enables (UDFs). The Hive platform is primarily constructed on three related data structures: partitions, tables and buckets. The features of Hive include:

- It stores schema in a database and handle data in the HDFS.
- It is delineated for OLAP.
- It provides SQL-Like language for querying called HQL.
- It is fast, simple, scalable and extensible.

The proposed system would resolve the existing system issues, like data size, fault-tolerance. The big data is fault-tolerant because it has replication factor, and these replication factor are customizable depending upon the project and the datasets. The fast RA-query using balanced partitioning would first partition the data based on certain criteria depending on the dataset and then would generate a local estimation sketch for each partitioned data. So, by doing this the system produces the result quickly by fetching the respective partitioned data instead of scanning the whole day, hence its fast. The results produced are also efficient and accurate compared to the existing system. The system produced efficient response with minimum delay. The next section contains related works which has amalgamated of survey papers. The latter section consist existing and the proposed system with module description. It also contains the future enhancement for the project.

2. RELATED WORKS

Online Analytical Processing (OLAP) is a technology that is used to organize large business databases and OLAP application is a multidimensional database which is also called as data cube. Range query applies an aggregation operation (SUM) over selected OLAP data cubes, which provide accurate results when data's are updated. This paper mainly focuses on performing aggregation operation with reduced time complexity. The algorithm used in this paper is double relative prefix sum approach to speed up range queries from $O(n^{d/2})$ to $O(n^{d/6})$, where d is the number of dimension and n is the number distinct tuples at each dimension [5]. The pre-computed auxiliary information helps to execute ad-hoc queries. The ad-hoc query is used to obtain information only when the need arises. So the prefix some approaches are suitable for the data which is static or which are rarely updated. COLA is used for answering cloud online aggregation for single and multiple join tables with accuracy. COLA supports incremental and continuous aggregation which reduces the waiting time before an acceptable estimate is reached. It uses Map Reduce concept to support continuous computing of aggregation on joins which reduces the waiting time. The techniques used in [8] OLA are block –level sampling and two- phase stratified sampling. The block level sampling consists of data which is split into blocks which forms samples. The stratified sampling, divides the population/data into separate groups, called strata. Then, a probability sample is drawn from each group. The efficiency in terms of speed is improved when compared to existing system efficiency. The OLA provides early estimated returns when the background computing processes are still running the results are subsequently refined and the accuracy is improved in succeeding stages. But users cannot obtain an appropriate answering with satisfied accuracy in the early stages. Also it cannot respond with acceptable accuracy within desired time period. Due to large data sets, traditional warehousing finds it difficult to process and handle the data. It is also expensive and produces non-scalable and inadequate result. In this paper, the authors have explored the use of HIVE an ecosystem of Hadoop. Hadoop is an open-source framework that allows to store and process big data in a distributed environment across clusters of computers using simple programming models and process model(MR). Map-reduce require hard maintenance, so the proposal system introduces a new framework called Hive on top of Hadoop framework. Hive is a data warehouse infrastructure built on top of Hadoop for providing data summarization, query, and analysis. Hive is a DB engine, which supports SQL like queries called HiveQL queries, which are then compiled into MR jobs [1]. Hive also contains a system log- metastore-which contains schema and semantics becomes useful during data exploration. HIVE ecosystem is best suitable for processing data, which is also used for querying and managing structured data built on top of Hadoop. This paper proposes a system model that is applicable for online aggregation analytic (OLA) over mapreduce in a large scale distributed systems. Hyracks is a technique involving pipelining of data processing which is faster than staged processing of hadoop process model [7]. Master maintains random block ordering. It consists of two intermediate set of files i.e., data files which

stores the values and the metadata files which stores the timing information. For estimation of aggregates- Bayesian estimator- uses correlation information between value and processing time. This paper destroys locality and hence introduces overhead. Since this approach is suitable only for static data, where updating of files becomes difficult and hence the result produced is inaccurate. Map Reduce is a popular programming function in the Hadoop open – source framework. To resolve the issue of fault tolerance, this paper allows the output of the MR task and job function to be materialized to the disk i.e. the HDFS before it is consumed. The reformed version of Map Reduce allows data to be pipelined between operators [3]. A pipeline is a set of data processing elements which is connected in series, where the output of one element is sent as the input of the next one. So, this improves and reduces the completion time and system utilization. MR supports online aggregation. Hadoop Online Prototype (HOP) supports continues queries, where programs written as event monitoring and stream processing, thus retaining fault tolerance. The drawback is that the output of map and reduce phase is materialized to stable storage before it is consumed by the next phase. Though the users consume results immediately, the users obtain results which are not appropriate and accurate. Also, the continuous query analysis processing is inefficient, because each new MapReduce job does not have access to the computational state of the last analysis run, so the state must be recomputed from scratch. The partitioning is done in large datasets in order to consume less time for processing the data and to provide output which is flexible and efficient. Range aggregation can be of any operation such as COUNT, SUM, MIN, MAX etc. The partition can be done based on different perspective such as: Random partition, Hash partition, Range Partition. Random partition is where the data's are randomly partitioned based on the size of the dataset. Hash partitioning of the data is based according to hash key value and the hash algorithm. Hash partitioning is a technique where a key value is used to distribute/partition rows equally across different partitions. Range partitioning separates the data according to range of values of the partitioning key. In range partition when the object resides on two different sets, then the operation has to be done separately on the sets and the resultant set are combined to produce the final output, based on the intersection operation. This type of process is called a range partition set operation [9]. The random partitioning might be easy to implement, but then some data's or objects maybe dependent on the other in order produce the data, so the processing of the results takes a longer time. So the range partitioning method is used in which several data are partitioned based on certain criteria and processing and analysis are done simultaneously. Therefore, it produces result with accuracy and it consumes linear space and achieves nearly-optimal query time, since the processes are in parallel.

HyperLogLog is an algorithm for the count-distinct problem, approximating the number of distinct elements in a multiset. Calculating the exact cardinality of a multiset requires an amount of memory proportional to the cardinality, which is impractical for very large datasets. This paper introduces algorithm for selection of range cardinality queries. The HyperLogLog++ algorithm is used for accurately estimating

the cardinality of a multiset using constant memory [4]. HyperLogLog++ has multiple improvements over HyperLogLog, with a much lower error rate for smaller cardinalities. It serializes the hash bits to bytes array in each bucket as a cardinality estimated. The HyperLogLog++ uses 64- bit hash function instead of 32- bits in HyperLogLog in order to improve the data-scale and estimated accuracy in big data environment. Hence this algorithm decreases the memory usage; accuracy increased and also reduces error. The big data as significant increase in data volume, and the preferred tuples maybe located in different blocks or files in a database. On the other hand, real time system aims to provide appropriate results within seconds on massive data analysis. This paper presents the architecture behinds Twitter real- time related query suggestion and spelling correction service. It describes two separate working systems that are built to solve the problem. They are: 1) Using hadoop implementation, 2) Using in-memory processing engine [6]. A good related query suggestion should provide Topicality and Temporality. Using hadoop, Twitter has robust and production Hadoop cluster. It uses Pig which is a scripting language to aggregate users search session, compute term and co-occurrence statistics. Due to this hadoop causes two bottlenecks that are log import and latency problem. Then the in-memory processing stores query co-occurrence and statistics, it stores the results in HDFS after the process and also contains replication factor. It becomes easier to fetch data from in- memory because it reduces the time complexity, and therefore it improves the efficiency. Due to the large datasets i.e. petabyte of data's, it becomes hard to scan the whole data and retrieve the result and also it's expensive. In order to overcome this, approximate statistics are built based on sampling. Block level sampling is more productive and efficient than the uniform-random sampling over a large datasets, but accountable to significant errors if used to create database statistics. In order to overcome it, two approaches are used Histogram and Distinct- Value estimation. Histogram uses two phase adaptive method in which sample size is decided based on first phase sample, and this is significantly faster than previous iterative methods. The 2-phase algorithm consists of the sort and Validate mechanism, and from it the required histogram is merged. The distinct value estimates appears as part of Histogram, because in addition to the tuple counts in buckets, histogram also keeps a count of the number of distinct value in each bucket [2]. This gives a density measure, which is defined as the average number of duplicates for the distinct value. The bucket weight is returned as the estimated cardinality of query.

3. EXISTING SYSTEM

The traditional system is meant for handling only structured data. The range aggregate query in the past system has row-oriented partitioning and also has only limited processing of data. The existing system processing and storage were impractical, non-scalable and less reliable. The results produced were inadequate. The existing system consists of the following issues:

- Analyzing and recovering range aggregate query based on balanced partitioning i.e., dividing a big data into independent partitions and then generating a local estimation for each partition.
- Updating of data should be done concurrently.
- Latency and errors should be reduced.
- Efficient response with minimum delay.
- The results retrieved should be faster and accurate.
- To achieve scalability.

4. PROPOSED SYSTEM

Many industries produce huge amounts of data in today's world, which consist of structured, semi-structured and unstructured data. In order to handle such large amount of data using Hadoop framework which consists of HIVE ecosystem is reliable and feasible. HIVE does the processing and analysis of structured data with the help of Map Reduce. RA-query executes the aggregate function based on the number of rows/columns. The traditional relational database system found it difficult to handle such huge amount of data. It processes only limited set of tuples and takes more time to access and produce the result with little accuracy and efficiency. Therefore, in order to effectively handle the query in big data, we would use the range partition mechanism. The balanced partitioning is done with the help of HIVE. Apache HIVE is a data warehouse structure build over Hadoop for performing detailed tasks such as analysis, querying and processing. The Apache HIVE is data warehouse software that helps querying and managing vast datasets residing in distributed storage/database. HIVE provides a technique to project structure to query the data using a SQL-like language called HiveQL or HQL. It also allows traditional Map/Reduce programming to plug in their custom mappers and reducers when it is impossible or inadequate to exhibit the logic in HiveQL.

In our system, we consider the structured data of music datasets, and create a table in order to perform the analysis. The HIVE consists of meta-store which has to be configured in order to process the data; the meta-store contains all the details like the number of tables, databases, time, partition etc.

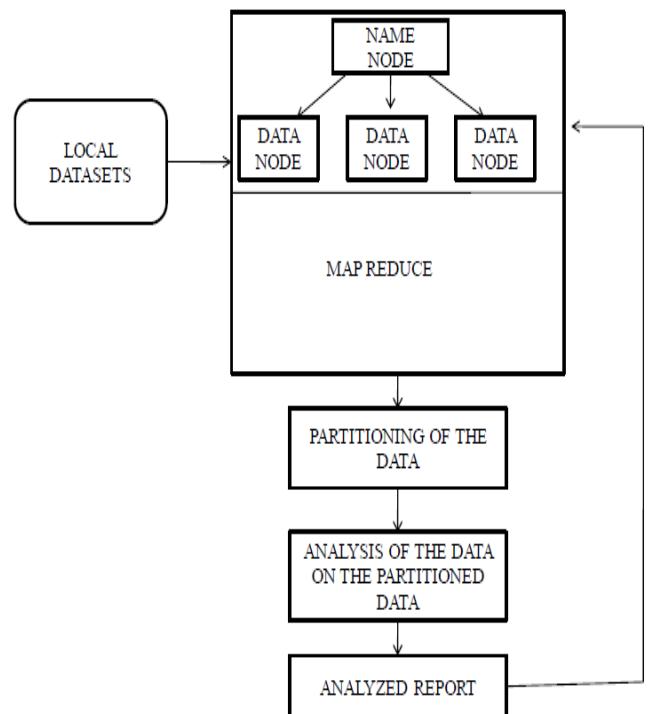


Fig.1. System Architecture Diagram

Depending on the vast data record, the big data is partitioned based on certain criteria and a local estimation blueprint is generated for each partition. So, when a user enters range-aggregate query, instead of scanning the whole data, it just generates the result by fetching the respective partitioned data. Thus the processing and searching of data becomes easier when records are partitioned.

A. Algorithm

Client C

C → name node // hadoop cluster

Name node ↔ secondary name node

C → data node

while data in HDFS is d and HIVE meta-store is h
h → d

if partition p is true

p → h

p → new directory (nd)

nd → d

while read

Search value v in p

Return p (v)

B. Block Diagram

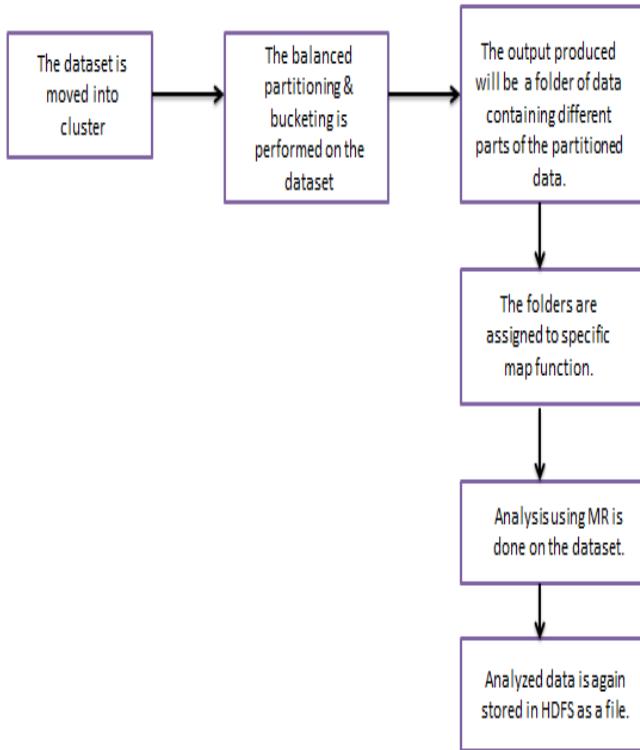


Fig.2. Block diagram

C. Implementation

The proposed system is tested and evaluated on publicly available datasets, namely music files. The datasets collected for structured data analysis should be in the table format. Therefore, the required pre-requisites are performed on the files before the analysis and processing of the data.

1) Preparation of the datasets

The datasets for the project is created with the help of the MySQL Workbench. The music database consist of song_details has its table name. The song_details contains fields like userid, songid, repeat times, song_status, song_category, song_year etc. The corresponding fields are updated with the required data.

2) Hadoop framework setup

Hadoop is an open-source framework for storing data and processing applications on clusters of commodity hardware. It provides enormous storage for any kind of data, immense processing power and the capability to handle virtually boundless concurrent tasks or jobs. Hadoop is a framework which requires LINUX OS system as a base. Ubuntu provides an up-to-date, secure operating system for average users, with a powerful focus on usability and ease of installation.

In this module we will install the pre-requisites and all the HADOOP related software on top of the LINUX. Once the Hadoop is setup, the data files like structured data (eg: Yahoo Music) are collected and moved from local system to the Hadoop where the HDFS resides using WINSCP. WINSCP is a secure open-source FTP, SFTP for Microsoft windows.

3) Creating table with partition

The data in HDFS will be in file format but HIVE requires the data in the TABLE format, in order to perform the MR operation. The balanced partition is done when the table is created for the data. The proposed system uses the balanced partitioning, where the data is split based on range value. Then bucketing is formed, where a subset of partitioned data is collected, in order to increase the efficiency of the query process. HIVE consists of meta-store which contains the actual DDL statements, which acts as interface and will load the actual files from HDFS. This HIVE meta-store will point to the data in HDFS and store the DDL whenever the table used in MR and the processing will be executed via the meta-store. HIVE must be installed on top of HADOOP, where HIVE meta-store will be automatically installed.

4) Analyze fields using Map Reduce

The HIVE HQL will perform the MR operation on the created table. The MR scans the partitioned data from HDFS in order to perform the analysis on the datasets. Map Reduce is a programming model and a related implementation for processing and producing large data sets with a parallel, distributed algorithm on a cluster. The MR is used to determine the various fields like for example, finding the maximum number of song liked by a user, number of times the same song listened by an individual. The analysis is done based on (key, value) pair on the data parallel. The respective count produced will be stored in the HDFS as a folder.

5. EXPERIMENTAL RESULT AND DISCUSSION

When the data are partitioned equally with range aggregate, the searching and analysis of data becomes easier. The proposed method would thus bring an integrated enhancement in handling structured data with availability, efficiency, consistency, accuracy and fast response. This approach limits relative errors when compared to the existing system and also provides efficient result. The below table shows that the time needed to execute data in Big data using Hive partition is less.

Dataset(in rows)	Traditional DB	Big data(HIVE)
Dataset 1(2000)	2min	1min
Dataset 2(200000)	30min	5min
Dataset 3(400000)	40min	10min

Table.1. Experimental Data Comparison

Also a comparison between the traditional RDBMS and emerging technology big data is made to show the efficiency and precedence in handling massive large amount of data. It shows that big data is more preferred when compared to the existing system.

CRITERIA	RDBMS	MAP REDUCE
Data size	Gigabyte, Terabyte	Petabyte, Zeta byte
Structure	Static scheme	Dynamic scheme
Data type	Structured	Semi-structured, structured, unstructured
Read/Write limit	1000queries/sec	Millions of query/sec
Availability	Not a fault-tolerant structure	Fault-tolerant
Processing speed/Transaction	Inefficient and time consuming	Fast and efficient
Storage	Stores in rows and columns	Stores in HDFS

Table.2. Comparison between traditional DB and big data

Thus, the experiment result manifest that the performance of handling big data with the help of HIVE balanced partitioning query is efficient, productive, cost-effective and scalable.

6. CONCLUSION AND FUTURE ENHANCEMENT

In this paper, we propose a fast range aggregate query method that acquires efficient estimations rapidly for RA-queries in big data environment. The traditional system representations were non-scalable, inadequate and unmanageable. Also, the cost increases as the growth of data increases. So, in our system we equally partition the data and provide sample/local estimation for each partition, which would make the analysis and processing of query easier and effective. It reduces the time complexity to O(1). The Hive is a data warehouse query language which is used for handling the structured data, and provides an efficient and cost effective result. The proposed system provides result for the user query fast by just fetching the data from the required partitioned data depending on the query/criteria. It produces the data with high efficiency and less time complexity for data updates. The fast RA-query with balanced partition would provide a good performance with high scalability, reliability and accuracy. Thus this approach would be good procedure for developing real – time answering methods for big data scrutiny and processing.

The future scope for structured data in big data environment would be to use Cloudera Impala. Impala

provides fast response since it has in-memory query processing. Also, Impala uses its own processing engine. It responds rapidly through massively parallel data processing. Also, the fast RA-query with balanced partition can be applied to heterogeneous factors/context. The concept can be used in today's market perspectives like real-time response method for analysis of data, industry/organization and education which contains huge amount of data's. In imminent years, big data technologies and cloud will play the crucial role for private sectors and organizations to handle the big data efficiently and accurately.

References

- [1] Ashish Thusoo ,Joydeep Sen Sarma, Namit Jain "Hive – A Petabyte Data Warehouse using Hadoop," *Proc. 13th Int'l Conf .Extending Database Technology (EDBT '10)*,2010.
- [2] Chaudhuri .S, Das .G, and Srivastava .U, "Effective use of block level sampling in statistics estimation," in Proc. ACM SIGMOD Int. Conf. Manage. Data, 2004, pp. 287–298.
- [3] Condie .T, Conway .N, Alvaro .P, Hellerstein .J .M, Gerth .J, Talbot .J, Elmeleegy .K, and Sears .R, "Online aggregation and continuous query Support in Map Reduce," in Proc. ACM SIGMOD Int. Conf. Manage. Data, 2010, pp. 1115–1118.
- [4] Heule .S, Nunkesser .M, and Hall .A, "Hyperloglog in practice: Algorithmic engineering of a state of the art cardinality estimation Algorithm," in Proc. 16th Int. Conf. Extending Database Tech., 2013, pp. 683–692.
- [5] Liang .W, Wang .H, and Orlowska .M .E, "Range queries in dynamic OLAP data cubes," *Data Knowl. Eng.*, vol. 34, no. 1,pp. 21–38, Jul. 2000.
- [6] Mishne .G, Dalton .J, Li .Z, Sharma .A, and Lin .J, "Fast data in theera of big data: Twitter's real-time related query suggestion architecture," in Proc. ACM SIGMOD Int. Conf. Manage. Data,2013, pp. 1147–1158.
- [7] Pansare .N, Borkar .V, Jermaine .C, and Condie .T, "Online aggregation for large MapReduce jobs," *Proc. VLDB Endowment*, vol. 4,no.11, pp. 1135–1145, 2011.
- [8] Shi .Y, Meng .X, Wang .F, and Gan .Y, "You can stop early with cola: Online processing of aggregate queries in the cloud," in Proc.21st ACM Int. Conf. Inf. Know. Manage. 2012, pp. 1223–1232.
- [9] Sharathkumar.R and Gupta.P, "Range-aggregate proximity queries," IIIT Hyderabad, Telangana 500032, India, Tech. Rep. IIIT/ TR/2007/80, 2007.
- [10] Yufei Tao, Cheng Sheng, Chin-Wan Chung, and Jong-Ryul Lee," Range Aggregation with Set Selection," *IEEE transactions on knowledge and data engineering*, VOL. 26, NO. 5, MAY 2014.

ICT Convergence in Internet of Things – The Birth of Smart Factories (A Technical Note)

Mahmood Adnan, Hushairi Zen

Abstract – Over the past decade, most factories across developed parts of the world employ a varying amount of the manufacturing technologies including autonomous robots, RFID (radio frequency identification) technology, NCs (numerically controlled machines), wireless sensor networks embedded with specialized computerized softwares for sophisticated product designs, engineering analysis, and remote control of machinery, etc. The ultimate aim of these all dramatic developments in manufacturing sector is thus to achieve aspects such as shorter innovation / product life cycles and raising overall productivity via efficiently handling complex interactions among the various stages (functions, departments) of a production line. The notion, *Factory of the Future*, is an unpredictable heaven of efficaciousness, wherein, issues such as the flaws and downtime would be issues of the long forgotten age. This technical note thus provides an overview of this awesome revolution waiting to be soon realized in the manufacturing sector.

Index Terms – Smart Factories, Fourth Industrial Revolution, Internet of Things, Ubiquitous Computing.

I. INTRODUCTION

WE often perceive Factories as dirty and noisy production amenities over - crowded with manpower and machinery incessantly executing same tasks again and again with abundant flaws and downtime. But now, Factories are about to get really smarter. We're rapidly heading towards fourth industrialization revolution, wherein, everyday machines that bakes sandwiches to blending of coffee and sophisticated machines manufacturing cellular phones and automobiles are about to get revolutionized. ‘Smart Factories or Factories of the Future’ (terminologies used interchangeably) are said to be employing a notion of ‘*Internet of Things*’ for operating complex manufacturing processes via hundreds and thousands of computers depending on the size of a particular industry.

Global competition for Smart Manufacturing is undoubtedly ravenous and Germany has taken this race with introduction of the first promising standard, i.e. Industry 4.0; and Government has accordingly invested amount to the tune of approximately €500m for materializing this technology [1, 2]. DFKI – German Artificial Intelligence Research Centre is now regarded as one of the acclaimed research centres worldwide for production of Smart Factories technology. European Commission’s worth \$2 billion project, *Factories of Future - Public Private Partnership* also aims to develop footprints / trails of Smart Manufacturing in European Union. Steps are now being taken to create a global Standard in certain developed parts of the world such as USA,

China, Korea, and Japan while the rest of the word still appears at quite a silence.

II. SMART FACTORIES – DEFINITION & CHALLENGES

Although there is no universal definition that defines aspects of Smart Factories, several research groups have their prophetic viewpoints. Smart Factories are actually envisaged on notion of *Internet of Things*, referred in the industrial sector as ‘*Industrial Internet of Things (IIoT)*’. The main intent is to empower all the assets / physical things on the shop floors, assembly lines, and batches with digital or virtual voice, which in turn enables them to communicate some sort of information about themselves (i.e. their status – what are they, where are they, their conditions like temperature, and hence so forth). If employed precisely, these interlinked devices from a convergence point between physical and digital world would empower the today’s industrial systems to transform into much smarter / intelligent systems [2].

Since the data from the shop floors (machine shop), assembly lines, and batches gets connected to a Cloud and is readily made observable in real time – successful companies can thus achieve shorter innovation and product life cycles, can add value to their offerings through faster time to the market, efficacious product personalization, transparency in their operations, well-informed processes, etc. The real challenges however lies in achieving its design principles including (but not limited to) *Interoperability, Virtualization, Real-Time Capability, Decentralization, Service Orientation, and Modularity, etc.*

CONCLUSION

The Smart Factory is believed to be a proclaimer of the fourth industrial revolution, an important swing in the operating norms that are expected to alter the mode via which the manufacturing companies today operates. It is just the matter of time; the world would soon see either a big IT-Multis, any visionary automation leader, or a small aspiring start-up to materialize this sphere.

REFERENCES

- [1] A. Radziwon, A. Bilberg, M. Bogers, and E. S. Madsen (2014), “The Smart Factory, Exploring Adaptive & Flexible Manufacturing Solutions”, Procedia Engineering, Vol. 69, pp. 1184-1190.
- [2] S. Wang, J. Wan, D. Zhang, D. Li, C. Zhang (2016), “Towards Smart Factory for Industry 4.0: A Self-organized Multi-agent System with Big Data Based Feedback & Coordination”, Computer Networks (Elsevier), [doi:10.1016/j.comnet.2015.12.017].

Mahmood Adnan is associated with the Faculty of Engineering, Universiti Malaysia Sarawak in the capacity of Postgraduate Researcher.

Hushairi Zen is Deputy Dean (Industry and Community Engagement) with the Faculty of Engineering, Universiti Malaysia Sarawak.

IEEE 802.11ac Vs IEEE 802.11n: Throughput Comparison in Multiple Indoor Environments

Zawar Shah ^a, Ashutosh A Kolhe ^a, Omer Mohsin Mubarak ^b

^a*Whitireia Community Polytechnic, Auckland, New Zealand.*
^b*Iqra University, Islamabad, Pakistan.*

Abstract— IEEE 802.11ac is a fifth generation WiFi standard that has many advanced features than the current widely used IEEE 802.11n. In this paper, we perform experiments in two real indoor environments (that possess interference and have different multipath characteristics) to quantify the gain in average throughput provided by IEEE 802.11ac compared to IEEE 802.11n. Our experimental results show that in an environment with less multipath effect, IEEE 802.11ac provides 51% and 126% gain compared to IEEE 802.11n at a distance of 5m and 18.5m from the wireless router, respectively. Similarly, in an environment with high multipath effect, IEEE 802.11ac provides gain of 21% and 32% compared to IEEE 802.11n at a distance of 1m and 18.5m from the wireless router, respectively. We conclude that IEEE 802.11ac can effectively handle interference caused by other IEEE 802.11n (5GHz) sources and provides higher throughput than IEEE 802.11n.

Keywords: IEEE 802.11ac, IEEE 802.11n, Throughput, MIMO.

I. INTRODUCTION

Wireless Fidelity (WiFi) networks based on the IEEE 802.11 standards are widely used today in offices, homes, shopping centres, airports etc. The availability of plethora of devices (laptops, smart phones etc.) that support high data rate is one of the main reasons of its growth. IEEE 802.11n standard is the most widely used standard today. However, more users these days are inclined to watch streaming multimedia content like High Definition videos that require high data rate. The extensive usage of popular streaming services like Netflix and YouTube further increase the demand for data rate. Due to this increase in demand, IEEE 802.11ac standard was introduced [1][2].

IEEE 802.11ac is an advancement of the IEEE 802.11n standard and operates only in the 5GHz frequency band. This helps it to avoid the interference present in the highly

congested 2.4 GHz frequency band. On the contrary, the IEEE 802.11n standard operates in both frequency bands of 2.4GHz and 5GHz. One of the main enhancement in IEEE 802.11ac is the support of larger channel width of 80MHz. However, IEEE 802.11n supports maximum channel width of 40MHz. Unlike IEEE 802.11n, IEEE 802.11ac supports higher modulation scheme of 256 Quadrature Amplitude Modulation (QAM). Another salient feature of the IEEE 802.11ac standard is that it has Multi-user Multiple Input and Multiple Output (MU-MIMO) which is not present in IEEE 802.11n networks. IEEE 802.11n supports a theoretical bandwidth of 450Mbps with 3*3 MIMO and 40MHz channel width. However, IEEE 802.11ac standard supports theoretical bandwidth to 1.3Gbps with 3*3 MIMO and 80MHz channel width [2][3][4][5].

Throughput analysis of various IEEE 802.11 standards in indoor environments have been discussed in literature [6][7][8][9]. Experiments are performed in [6] to measure the throughput obtained by IEEE 802.11b network. Throughput analysis of IEEE 802.11n is carried out in [7]. Similarly, throughput gain provided by IEEE 802.11ac over IEEE 802.11n is quantified in [8]. Effect of larger channel width on throughput provided by IEEE 802.11ac is discussed in [9].

In this paper, throughput comparison of IEEE 802.11ac and IEEE 802.11n is carried out in two indoor environments that possess different multipath characteristics. Interference from other IEEE 802.11n networks operating in 5GHz is also present in both environments. Our main aim is to perform experiments using common off-the-shelf equipment and quantify the average throughput gain provided by IEEE 802.11ac compared to IEEE 802.11n in both environments. Our main contribution in this work are (i) To determine the average throughput provided by IEEE 802.11ac in different indoor environments. (ii) To determine the average throughput provided by IEEE 802.11n in 2.4GHz and 5GHz frequency bands in two different indoor environments. (iii) To quantify the average throughput

gain provided by IEEE 802.11ac compared to IEEE 802.11n in two different indoor environments.

The rest of the paper is organized as follows. Section II presents the related work. In section III, we present our experimental test bed and equipment that is used to carry out the experiments. Experimental results are presented in Section IV. Discussion section is presented in section V and finally we conclude our work in section VI.

II. RELATED WORK

Many research studies in the past have carried out throughput analysis of various IEEE 802.11 standards in indoor environments. The authors in [6] determine the throughput provided by IEEE 802.11b networks by developing an analytical model. In [7], throughput analysis of IEEE 802.11n using 2*3 MIMO for Line of Sight and Non Line of Sight is carried out in an indoor environment. The throughput analysis using various commercially available IEEE 802.11n devices is carried out in [10]. In [8], authors carry out experiments and show that IEEE 802.11ac significantly improves throughput as compared to IEEE 802.11n. Similarly, authors in [9] conclude that higher throughput of IEEE 802.11ac is due to higher modulation scheme and larger channel width. The variation in throughput with frame aggregation is discussed in [11][12]. To the best of our knowledge, very limited studies exist in the literature that determine the gain in average throughput provided by IEEE 802.11ac compared to IEEE 802.11n in multiple indoor environments where interference from other IEEE 802.11n networks is present.

III. EXPERIMENTAL TEST BED

In this section we explain details of both environments. Our experimental setup and the equipment used to carry out the experiments are also explained in this section.

A. Environment 1

Our Environment 1 consists of lecture rooms and students labs in the main campus of Whitireia Community Polytechnic, Auckland, New Zealand. The lecture halls and labs are large in size and consists of chairs, tables, desktop computers etc. The environment 1, unlike environment 2 (see later), has more open space and hence

has less multipath effect. However, InSSider tool shows that there are six networks already operating in 2.4GHz frequency bands. Similarly, there are three networks operating in 5GHz band. Names of these networks along with the channels they are operating on are shown in Table 1. Our purpose is to test performance of both IEEE 802.11ac and IEEE 802.11n in this real environment where other WiFi Networks of institute will cause interference. Our experimental testbed for environment 1 is shown in Fig 1. The position for the router is shown as R. Various positions for measurements marked as A(5m), B(10m), C(10.5m), D(18.5m), E(15m), F(22.5m), G(28m), H(42m) and I (32m) are shown in Fig 1.

TABLE 1
Interfering WiFi networks in Environment 1

SSID	Frequency Band	Channel(s)	Channel Width (MHz)
WhitireiaNZ	5GHz	108 +112	40
WhitireiaNZ	5GHz	44 + 48	20
WhitireiaNZ	2.4GHz	36 + 40	20
Whiti-BOYD	2.4GHz	36 + 40	20
Whiti-BOYD	2.4GHz	100	40
WhitireiaNZ	5GHz	60 + 64	40
Whiti-BOYD	2.4GHz	60 + 64	40
Mikro	2.4GHz	60	40
TZikACNTx2			
Whiti-BOYD	2.4GHz	52	20

B. Environment 2

Our environment 2 consists of faculty offices at the Whitireia Community Polytechnic in Auckland, New Zealand. Each office has wooden tables, metal cabinets and a wooden door. All the offices are separated by thick wooden walls. The environment 2 provides high multipath effect unlike environment 1. The institute also has its own WiFi Networks operating in environment 2. Again our purpose is to test performance of both IEEE 802.11ac and IEEE 802.11n in this high multipath environment where other WiFi Networks of institute will cause interference. In this environment, we use inSSider tool to find other networks in both 2.4GHz and 5GHz frequency bands. We find that there are two other IEEE 802.11n networks already operating at 5GHz frequency band and six IEEE 802.11n networks in 2.4GHz. Names of these networks

along with the channels they are operating on are shown in Table II. We note that there are no IEEE 802.11ac network operating in both environments so the results obtained are free from the interference caused by other IEEE 802.11ac traffic source. Our experimental testbed for environment 2 is shown in Fig 2. The position for the router is shown as R. Various positions for measurements marked as A(1m), B(11.5m), C(15m), D(18.5m) and E(30m) are shown in Fig 2.

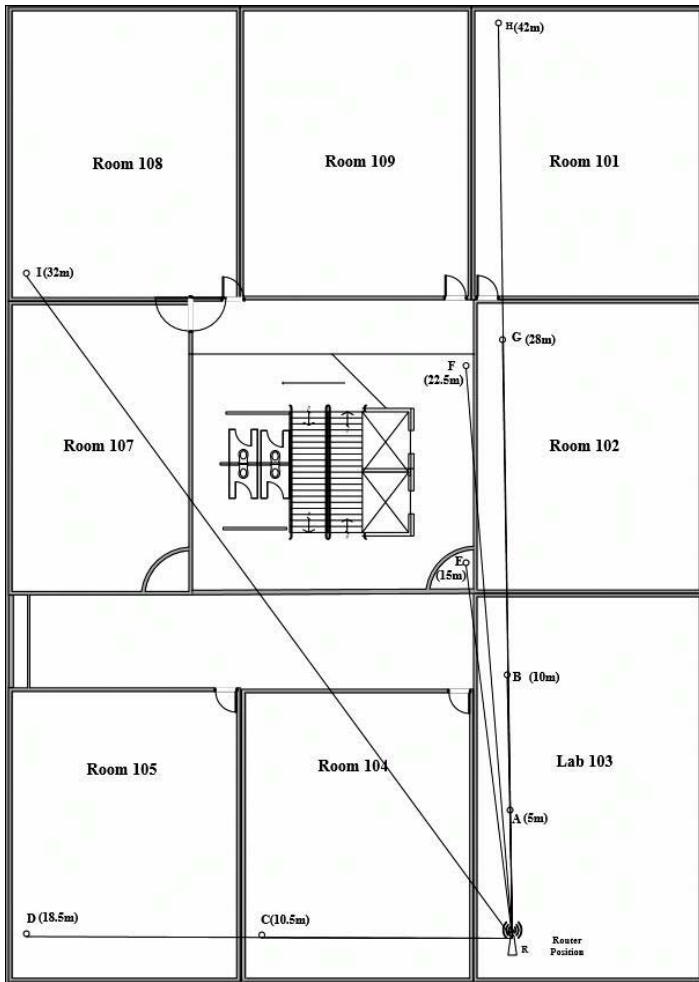


Figure 1: Environment 1 with Marked Measurement Positions.

B. Hardware and Software used in Environment 1 and Environment 2

In both the environments, the router used is Linksys WRT AC 1900 [12]. This router supports all features of IEEE

802.11ac standard like beamforming, 256 QAM etc. The router operates in both 2.4GHz and 5GHz frequency bands and can be configured to support only IEEE 802.11n. To enable our Laptops to support IEEE 802.11ac, we use D-Link AC1200 USB adapter [13]. This adapter also operates in dual band and supports both IEEE 802.11ac and IEEE 802.11n. IPERF [14] is used to generate UDP traffic in all our experiments conducted in both the environments. We use the InSSider tool [15] to measure Receive Signal Strength Indicator (RSSI). InSSider tool is also used to monitor the 2.4GHz and 5GHz frequency bands for other networks that may interfere with our networks.

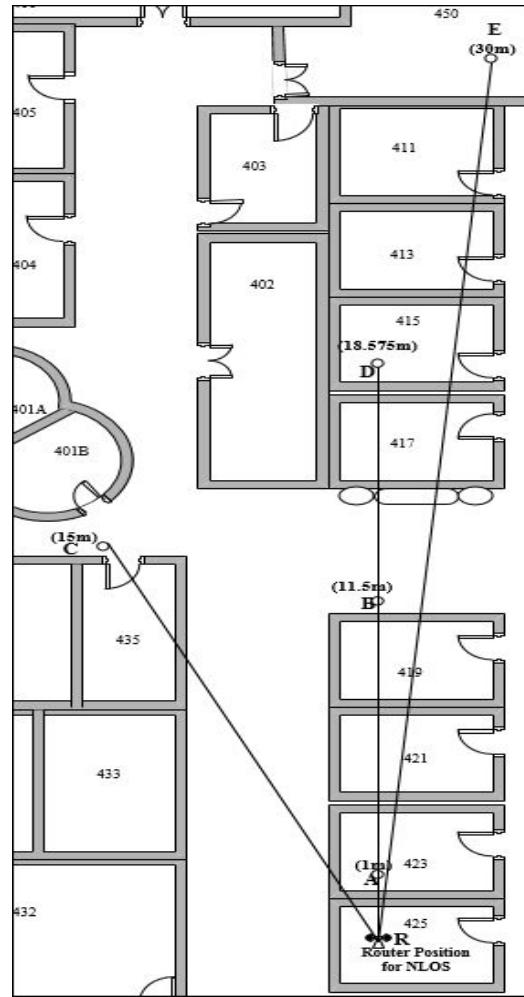


Figure 2: Environment 2 with Marked Measurement Positions.

C. Experimental Setup

In all our experiments traffic is generated from client to server over the WiFi Network. Our client is a Sony VAIO Laptop that has a wired connection with the Linksys WRT 1900AC router. A HP EliteBook laptop plugged with DWA-182 AC1200 USB adapter acts as a server. UDP traffic is generated from client to server using Iperf. The size of datagram generated in all our experiments is 1472 bytes and all the experiments are carried out during peak time. In order to capture the effect of interference in the best possible manner we repeat all our experiments over a period of three days and then take the average of values obtained. In all our experiments, we take a 40 seconds readings five times and then take the average of these values. All our results are obtained by generating one UDP stream as generating more than one stream results in high packet loss. Our experimental setup is shown in Fig 3.

TABLE II
Interfering WiFi networks in Environment 2

SSID	Frequency Band	Channel (s)	Channel Width (MHz)
Whiti-BOYD	5,2.4GHz	11,36,44, 52	20,40
Whitireia NZ	5,2.4GHz	44 + 48	20,40
Netgrm42 3	2.4GHz	36 + 40	20
FBIT-HotSpot	2.4GHz	36 + 40	20
FBIT-WLAN	2.4GHz	100	20
FBIT-WHotspot Guest	2.4GHz	60 + 64	20



Figure 3: Experimental Setup.

IV. RESULTS

In this section we explain our experimental results for both environments.

A. Results of Environment 1

1) Measurement of Received Signal Strength Indicator (RSSI)

We first measure the RSSI for both standards in environment 1. As the distance from the access points increases, there is a drop in the RSSI for both IEEE 802.11ac and IEEE 802.11n (that is operating on both 2.4GHz and 5GHz frequency bands). We obtain very similar results of RSSI for both IEEE 802.11n and IEEE 802.11ac in the 5GHz frequency band (RSSI varies between -45dbm to -65dbm). However, there was an interference from the IEEE 802.11n devices working in the same frequency which can be seen in table I.

It is observed that the IEEE 802.11 ac can function at higher distances compared to the IEEE 802.11n as it was possible to obtain RSSI readings even at H (42 meters) and point I (32 meters) for IEEE 802.11 ac standard. In contrast, no readings are obtained for IEEE 802.11n at points H and I. The RSSI readings were low for IEEE 802.11n (2.4GHz) because of high interference in this frequency band. Our results for RSSI are shown in Fig 4.

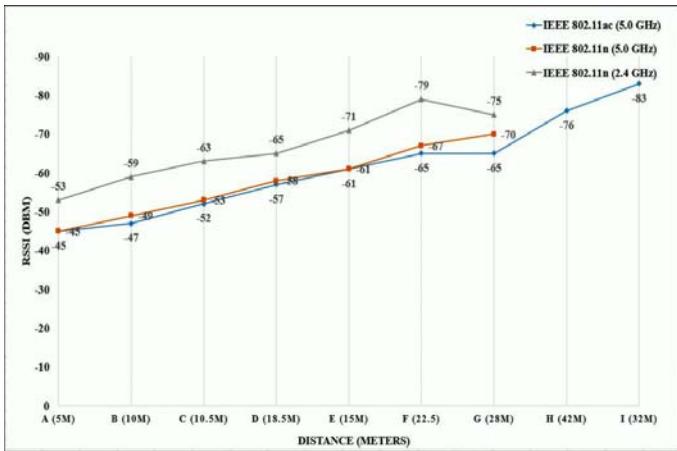


Figure 4: RSSI Measurement in Environment 1.

2) Measurement of Packet Loss

The packet loss obtained for both IEEE 802.11 n (2.4GHz and 5 GHz) and IEEE 802.11ac is shown in Fig 5. We observe that packet loss increases as we increase the distance for both standards. IEEE 802.11ac provides less packet loss than IEEE 802.11n (2.4GHz and 5GHz) at all the different positions e.g. at point G (28m from the wireless router) packet loss is 72%, 79.6% and 81% for IEEE 802.11ac, IEEE 802.11n (5GHz) and IEEE 802.11n (2.4GHz) respectively. Our results for packet loss are shown in Fig 5.

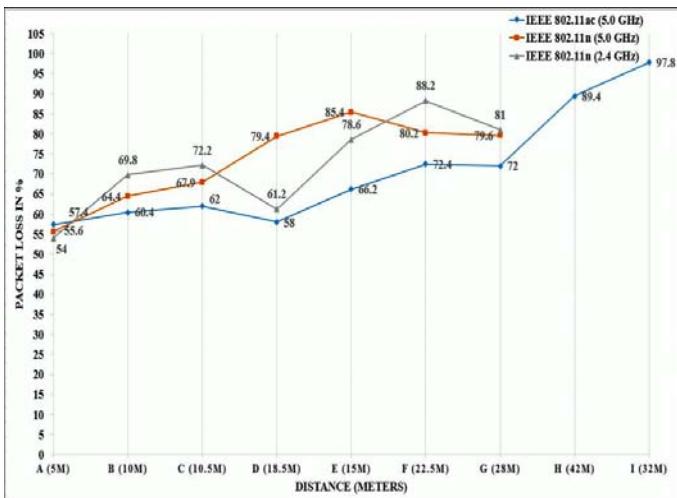


Figure 5: Average Packet loss in Environment 1.

3) Throughput Comparison of IEEE 802.11ac and IEEE 802.11n in Environment 1

We note that at all points IEEE 802.11ac standard provides the higher average throughput than IEEE 802.11n (2.4GHz and 5GHz). The average throughput for IEEE 802.11ac at point A is 280Mbps and the IEEE 802.11n functioning on 5GHz provides throughput of 190.4 Mbps. Similarly, IEEE 802.11n functioning on the 2.4GHz frequency provide a throughput of 91.64Mbps at point A. The throughput decreases for all standards as we move away from the wireless router. However, the decrease is less for IEEE 802.11ac than IEEE 802.11n (2.4GHz and 5GHz). At point F, IEEE 802.11ac achieves a throughput of 117Mbps while IEEE 802.11n provides throughput of 98.82Mbps and 22.9Mbps at 5GHz and 2.4GHz, respectively. IEEE 802.11n at 2.4GHz provides less throughput because of the congested 2.4GHz frequency band. At points G and H, no readings for IEEE 802.11n (for both 2.4GHz and 5GHz) are obtained as connection with the router is not established as distance is increase beyond 28m (point G). However, IEEE 802.11ac provides a throughput of 44.44Mbps and 7.02Mbps at points H and I, respectively. The gain provided by IEEE 802.11ac compared to IEEE 802.11n (5GHz) in environment 1 is given in table III. Fig 6 shows the average throughput provided by IEEE 802.11ac and IEEE 802.11n (2.4GHz and 5GHz).

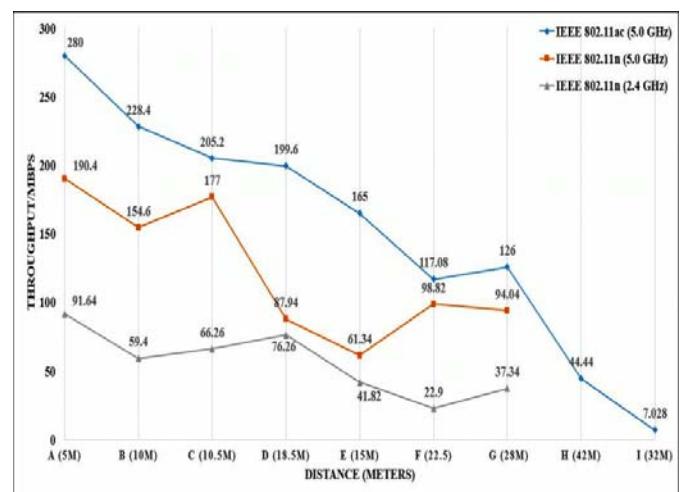


Figure 6: Average Throughput in Environment 1.

TABLE III

Gain Provided by IEEE 802.11ac compared to IEEE 802.11n (5GHz) in Environment 1.

Positions	IEEE 802.11ac (Mbps)	IEEE 802.11n (5GHz) (Mbps)	Gain (%)
A (5m)	288	190.4	51.2
B(10m)	228.4	154.6	47.7
C10.5m)	205.2	177	16
D (18.5m)	199.6	87.94	126
E (15m)	165	61.34	168
F (22.5m)	117.08	98.82	18.5
G (28m)	126	94.04	34
H (42m)	44.44	N/A	N/A
I (32m)	7.02	N/A	N/A

B. Results of Environment 2¹

In this section we explain the experimental results obtained in environment 2.

1) Measurement of Received Signal Strength Indicator (RSSI)

Fig 7 shows the RSSI measured at all the positions for both standards. We observe that for 5GHz frequency band there is not much difference between RSSI values obtained for IEEE 802.11ac and IEEE 802.11n at different positions. At point A the value of RSSI for both standards is -45 dbm. However, we observe slightly better RSSI for IEEE 802.11ac at points B, D and E. RSSI values of IEEE 802.11n (2.4GHz) was worse because of high congestion present in this frequency band. For IEEE 802.11n (2.4GHz), the wireless connection was terminated at point D and E hence no RSSI was obtained at these points.

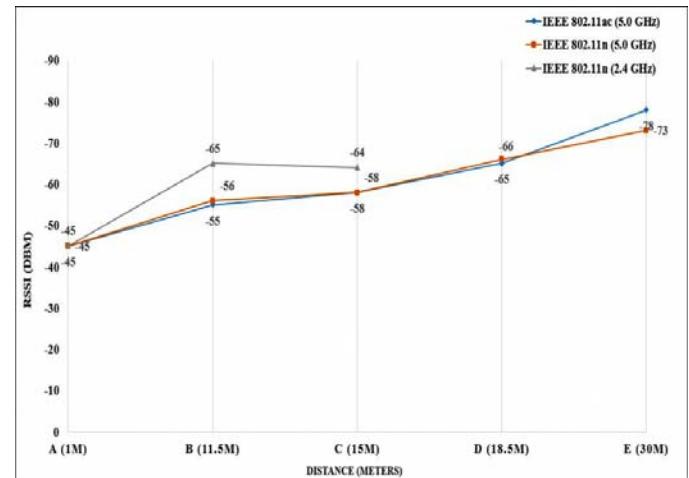


Figure 7: RSSI Measurement in Environment 2.

2) Measurement of Packet Loss

Packet loss obtained at different positions is also shown in Fig 8. It can be seen from Fig 7 and Fig 8 that packet loss increases with decreasing RSSI and increasing distance. These results of RSSI and packet loss clearly show that 2.4GHz band is congested and more interference is present in this band than 5GHz. It is to be noted that IEEE 802.11n (5GHz) also has more packet loss than IEEE 802.11ac e.g. at point C (15m) the packet loss of IEEE 802.11n (5GHz) is 52% which is much higher than IEEE 802.11ac (29%). This shows that IEEE 802.11ac is better able to handle interference present in 5GHz frequency band than IEEE 802.11n

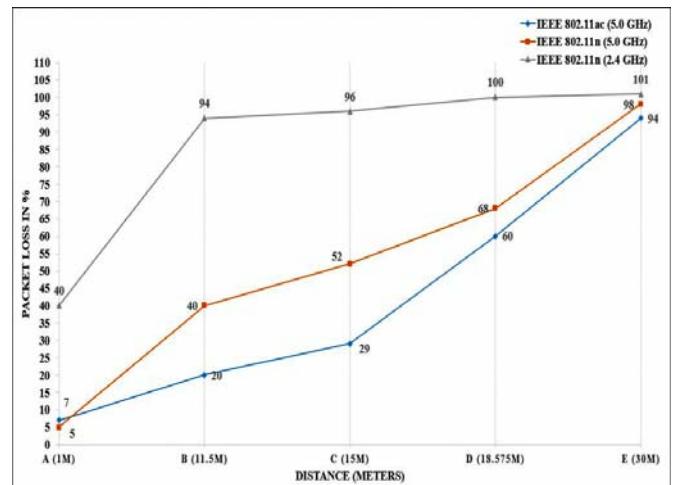


Figure 8: Average Packet loss in Environment 2

¹ More detailed results of environment 2 are available in Z. Shah, S. Rau and A. Baig, "Throughput Comparison of IEEE 802.11ac and IEEE 802.11n in an Indoor Environment with Interference", in IEEE International Telecommunication Networks and Applications Conference (ITNAC), Sydney, Australia, 2015.

3) Throughput Comparison of IEEE 802.11ac and IEEE 802.11n in Environment 2

The throughput obtained at various positions for both standards is shown in Fig 8. We note that for both standards, average throughput decreases with the decrease in RSSI and increase in distance both of which translate into higher packet loss (mentioned above). The average throughput for IEEE 802.11n (5GHz) at point A (with RSSI -45dbm) is 150Mbps which decreases to 59Mbps at point D (with RSSI of -66dbm). Similarly, the average throughput for IEEE 802.11ac at point A (RSSI of -45dbm) is 181.4Mbps which reduces to 78Mbps at point D (RSSI value of -65dbm). The important point to note here is that IEEE 802.11ac and IEEE 802.11n (5GHz) although have nearly same values of RSSI but the average throughput obtained by IEEE 802.11ac is higher than IEEE 802.11n (5GHz) at points A, B, C and D. This can be seen from Fig 9. A comparison of gain in average throughput provided by IEEE 802.11ac and IEEE 802.11n is shown in Table IV. At point A, IEEE 802.11ac provides a gain of 21% compared to IEEE 802.11n (5GHz). At point B, C and D the gain provided by IEEE 802.11ac compared to IEEE 802.11n (5GHz) is 45%, 55% and 32%, respectively. We note IEEE 802.11ac still provides higher average throughput than IEEE 802.11n (5GHz) as channel conditions deteriorate with increasing distance and signal attenuation caused by walls. However, at point E (distance of 30m) both IEEE 802.11n (5GHz) and IEEE 802.11ac provide nearly same average throughput because of the worst channel conditions (low RSSI and high packet loss). IEEE 802.11n (2.4GHz) provides the worst average throughput due to high interference present in 2.4GHz band. IEEE 802.11n (2.4GHz) provides 79.7Mbps at point A. However, at point C the average throughput reduces to only 3.42Mbps (high packet loss of 98%) and the connection is disconnected at points D and E.

IV. DISCUSSION

Our experimental results indicate that IEEE 802.11ac

provides much higher throughput than IEEE 802.11n in both environment 1 and environment 2. Environment 1 has less multipath effect and therefore it provides higher average throughput than environment 2. We note that in

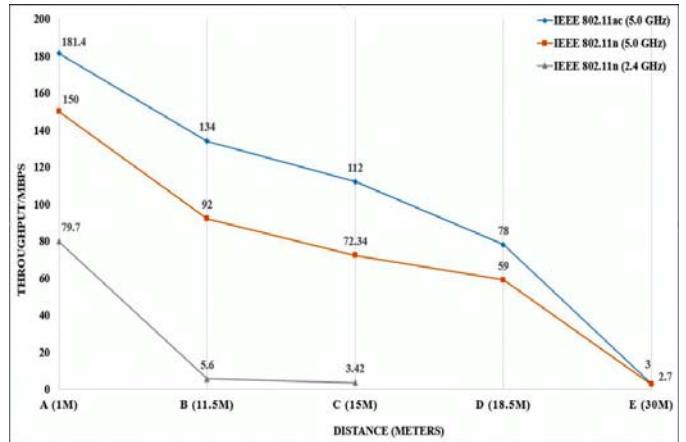


Figure 9: Average Throughput in Environment 2.

both the environments, RSSI values for IEEE 802.11ac and IEEE 802.11n in 5GHz frequency band are very close to each other. The higher average throughput of IEEE 802.11ac than IEEE 802.11n in both environments is due to the use of higher modulation scheme of 256 QAM (especially at points close to router), larger channel width of 80MHz coupled with the use of beamforming and MIMO. Our results show that in various indoor environments, IEEE 802.11ac is better able to handle interference caused by other IEEE 802.11n networks in 5GHz frequency band.

V. CONCLUSION

In this work we carried out experiments using common off-the-shelf equipment to compare the throughput performance of IEEE 802.11ac and IEEE 802.11n (2.4GHz and 5 GHz) in two indoor environments. Interference from other IEEE 802.11n networks operating in 2.4GHz and 5GHz frequency bands is present in both the environments. We note that in environment 1 (with less multipath effect), IEEE 802.11ac provides gain of 47% and 34% at distances of 10m and 28m, respectively. Similarly, in environment 2 (with high multipath effect), IEEE 802.11ac provides a gain of 21% and 32% at

distances of 1m and 18.5m, respectively. We conclude that IEEE 802.11ac can better handle the interference caused by other IEEE 802.11n networks and provides more throughput than IEEE 802.11n in multiple indoor environments.

TABLE IV
Gain Provided by IEEE 802.11ac compared to IEEE 802.11n (5GHz) in Environment 2

Positions	IEEE 802.11ac (Mbps)	IEEE 802.11n (5GHz) (Mbps)	Gain (%)
A(1m)	181.4	150	21
B(11.5m)	134	92	45
C(15m)	112	72.34	55
D(18.5m)	78	59	32
E (30m)	3	2.7	11

REFERENCES

- [1] M. Akbar, M. Saleem, A. Khalil, A. Qayyum and M. Yousaf, "Evaluation of IEEE 802.11n for Multimedia Application in VANET," in Procedia Computer Science, vol. 32, pp. 953-958, 2014.
- [2] E. Perahia and R. Stacey, "Next Generation Wireless LANS: 802.11n and 802.11ac" Cambridge University Press, 2013.
- [3] Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Enhancements for Very High Throughput for Operation in Bands below 6GHz, IEEE P802.11ac/D1.0 Std., Jan. 2011.
- [4] L. Verma, M. Fakharzadeh and S. Choi, "Wi-Fi On Steroids: 802.11ac and 802.11ad," in IEEE Wireless Communications, vol. 20, pp. 30-35, 2013.
- [5] N. Vaughan, J. Steven, "Gigabit Wi-Fi is on its Way," in IEEE Computer, vol. 11, pp. 11-14, 2010.
- [6] C. Chen and C. Law, "Throughput Performance Analysis and Experimental Evaluation of IEEE 802.11b Radio Link," in IEEE Information, Communications and Signal Processing Conference, 2007.
- [7] Y. Dama, R. A. Abd-Alhameed, S. Jones, D. Zhou and M. B. Child, "Experimental Throughput Analysis and MIMO Indoor Propagation Prediction for 802.11n System" in IEEE International Symposium on Electromagnetic Compatibility (EMC), York, UK, 2011.
- [8] M. Dianu, J. R. Arvi and M. Petrova, "Measurement-Based Study of the Performance of IEEE 802.11ac in an Indoor Environment," in IEEE International Conference on Communications (ICC), 2014.
- [9] Y. Zeng, P. H. Pathak and P. Mohapatra, "Throughput, Energy Efficiency and Interference Characterisation of 802.11ac," in Transactions on Emerging Telecommunications Technologies, 2015.
- [10] V. Visoottiviseth, T. Piroonsith, and S. Siwamogsatham, "An Empirical Study on Achievable Throughputs of IEEE 802.11n Devices," in IEEE International Symposium on Modelling and Optimization in Mobile, Ad Hoc, and Wireless Networks, pp. 1-6, 2009.
- [10] B. Bellalta, J. Barcelo, D. Staehle, A. Vinel, and M. Oliver, "On the Performance of Packet Aggregation in IEEE 802.11ac MU-MIMO WLANs," IEEE Communications Letters, vol. 16, pp. 1588-1591, 2012.
- [11] J. Cha, H. Jin, B. C. Jung, and D. K. Sung, "Performance Comparison of Downlink User Multiplexing Schemes in IEEE 802.11ac: Multi-user MIMO vs. Frame Aggregation," in IEEE Wireless Communications and Networking Conference (WCNC), pp. 1514-1519, 2012.
- [12] Linksys WRT 1900ac Router, <http://www.linksys.com/us/p/P-WRT1900AC/>
- [13] D-Link DWA-182 1200ac USB Adapter, <http://www.dlink.co.nz/home-solutions/wireless-ac1200-dual-band-usb-adapter>
- [14] A. Tirumala, F. Qin, J. Dugan, J. Ferguson, and K. Gibbs, Iperf: The TCP/UDP bandwidth measurement tool. Current version available online at <http://code.google.com/p/iperf/>.
- [15] inSSider tool, <http://www.metageek.com/products/inssider/index2.html>

Implementing Navigational aspect of Specific Testing Process Model

Garima Singh

Research Scholar, Dept. of Computer Science and
Engineering
JECRC University
Jaipur, Rajasthan, India

Manju Kaushik

Associate Professor, Dept. of Computer Science and
Engineering
JECRC University
Jaipur, Rajasthan, India

Abstract-Navigational modeling of web application and testing the navigational aspect of the web application is as important as the content displayed and security of application to maintain the quality and user satisfaction. Test paths are generated through the navigation model which is derived from the activity diagram. The objective of this paper is to implement navigational aspect of web application through a model.

Keywords-Specific Testing Process Model, Web application modelling, web application navigational testing.

I. INTRODUCTION

Navigational testing of a web application plays a vital role in ensuring that a page should relate to another page which contain information related to the event occur when a user click on content of web page. Several researchers cover the navigational testing aspect of web applications; here we have discussed related work. Researcher used the technique of User Interaction Diagram to retrieve navigation architecture of the web application from conceptual model [1]. Further, a reverse engineering model is used to navigate structure and behavior of the web application using Web Unified Modeling Language (WebUML) [2]. For the verification of various models of a web system a model checking systematic approach is used which describes the integrated navigational structure and the business processes through state machine diagram [3]. Using formal approach called FARNAV, the author describes the navigation modeling of web application [4]. Use Case Transition Model (UCTM) is used by author to depict sequence diagrams then converting them to graph and coverage message, for reducing and generating test cases [5]. To understand navigation of the system test cases are generated from activity diagram by considering three ways: a) Creating activity diagram from the information b) then from that activity diagram make an activity graph c) and derive test cases, this is called path criterion of an activity [6]. A method for the automated testing of web applications based on their navigation approach is to exercise the System Under Test (SUT) for performing the navigation from page to page by means of web links, for navigation, functional validation is carried out since the correctness of the links using three kinds of UML diagrams which are Use case, Activity and Presentation diagrams [7]. A Role Based Access Control (RBAC) is used to cover navigational aspect of the web

application which is the concept of Unified Web Engineering (UWE), to show secure navigation and patterns using state machine [8]. A methodology to generate test cases from UML sequence diagrams, using a case study sequence diagram is traversed, conditional predicates are selected using depth first search, which are changed into the source code [9]. The term navigation for the web application indicates the moment of the user cursor over the application for information on the same page, different pages of that application, searching, clicking etc. The essential features which are required to make error free in the navigation testing model are hyperlinks contextual and non contextual [10]. User move within the application called contextual hyperlink. Non-contextual hyperlink carries to other sources or application. Many researchers described navigation design and testing approach for the web applications. Here, researcher is describing and implementing the navigation aspect of their proposed Specific Testing Process Model [11].

II. FOUNDATION : NAVIGATION MODEL OF WEB APPLICATIONS

There are several methods like UML model, user session data; state based techniques etc. which are based on Model-based testing for web applications. All these methods are used to generate test cases. Here researcher generated test paths from the model. So that web application with quality is delivered. In today's scenario web applications are extreme dynamic, full of complexities and asynchronous. Using traversing technique of web pages through link researcher is describing the navigation of web application. According to [12] a web application is denoted by WA consist of a web state S_i which is functional element acts as an intermediate node in navigation. There can be many web states in a web application, So, $WA = \{S_1, S_2, \dots, S_n\}$. Web state S_i consist of different types of input and output elements e_{ij} like button, checkbox, text field, text, images and many more. Therefore, $S_i = \{e_{i1}, e_{i2}, \dots, e_{im}\}$. In the web application all its states S_i are interconnected by transitions. A sequence of action denoted by α applied on element e_{aj} of a state S_a together called a transition denoted by T , where actions are click, double-click, mouse over, key press etc. The result of an action reflects the changes in web state from S_a to S_b . Considering these concepts web application enriches

navigation through web pages and links. In model based testing, test tree is a method which gives a wide range to test paths for web applications, by traversing the model a test tree is constructed and then test paths are derived. For a web application, from root to the leaves of a tree a test sequence can be a test path. Researcher [12] shows a precise page navigation model of the online web application with its test tree. Kripke structure [14] gives transition of the application behavior which is used in the concept and definition for Navigation model [13] contain five parts that are S as a state of web page, there can be many states like s1, s2, s3... so on in a web application. These are also referred as pages of a website. Initial State is denoted by IS, home page can be taken as IS of web application, Atomic Section AS which shows attributes of page like its function, link, request, error, return and a label denoted by L which gives information about each state, Transition Relation is denoted by TR which mean $(s, n, ap) \in TR$, where request ap is made to move on n which is next page.

Here, $S \rightarrow$ All pages, for every state $s \in S$

$IS \rightarrow$ Initial State, Login page

$AS \rightarrow$ Atomic Section , $ap \in AS$ (Attributes of page like link, error, exit, return)

$TR \rightarrow$ Transition Relation , $(s, n, ap) \in TR$

$L \rightarrow$ Label of state.

Researcher is implementing the navigational aspect of specific testing process model on the dual security testing model [14] , that how we can test the navigational property of the model following the activity diagram, navigation model, creating test tree and then generating test path.

III. PROPOSED IMPLEMENTATION METHODOLOGY FOR NAVIGATION TESTING

Here, in this segment we discuss about how the approach is implemented for the navigation aspect of the model and how test paths are generated.

The proposed approach follows four basic steps:

- A. *Activity Diagram: On the basis of information provided web designer make activity diagram. Which shows a flow of activity performed on the application.*
- B. *Navigation Model: Display the navigation diagram with required information.*
- C. *Test Tree: Converting Navigation Diagram into Test Tree.*
- D. *Test Path: Generating test paths from the test tree.*

The navigation model works in the four sub-models which are as follows:

- 1. Login Registration Navigation sub model.
- 2. Complete Shopping and Billing sub model.

- 3. Shopping in association of Automated Guide sub model.
- 4. Shopping with the feedback result and interactive chatting sub model.

The navigation model is completely showing the root of online shopping cart which is designed through activity diagram. For implementing the navigational aspect on Dual Security Testing Model [14], Activity Diagram is designed then; Navigation model is displayed as shown in fig.1. This consists of four sub models, for each sub models an independent test tree is constructed shown in fig. 2. And test paths are derived from the tree.

IV. NAVIGATION SUB MODEL WITH TEST TREE AND THEIR PATHS

Here, we have divided the navigation model into the sub models so that test tree and test paths can be generated efficiently. For each sub models, there is a test tree and from the test tree, test paths are generated.

For Login Registration Navigation sub model in fig. 3, test tree is fig. 4 and test paths are as follows:

Test Path:

Path 1: $s1 - error - s1;$

Path 2: $s1 - link-s3 - error - s3;$

Path 3: $s1 - link-s3 - exit - s1;$

Path 4: $s1 - link- s4 - link s5 - link - s7 - link-s8;$

Path 5: $s1 - link- s4 - link s6 - link - s7 - link-s8;$

For Complete Shopping and Billing sub model in fig. 5, test tree is fig. 6 and test paths are as follows:

Test Path:

Path 6 : $s1 - error - s1;$

Path 7 : $s1 - link-s2 - exit - s1;$

Path 8 : $s1 - link-s2 - link s9 - return- s2;$

Path 9 : $s1 - link-s2 - link s9 - link - s10 - return- s9;$

Path 10: $s1 - link-s2 - link s9 - link - s10 - link- s11 - exit - s10;$

Path 11: $s1 - link-s2 - link s9 - link - s10 - link- s11 - link - s12 - return - s2;$

Path 12: $s1 - link-s2 - link s9 - link - s10 - link- s11 - link - s12 - exit;$

Path 13: $s1 - link-s2 - link s9 - link - s10 - link- s11 - link - s12 - exit;$

For Shopping in association of Automated Guide sub model in fig. 7, test tree is fig. 8 and test paths are as follows:

Test Path:

Path 14: $s1 - error - s1;$

Path 15: s1 – link-s2 – exit – s1;
 Path 16: s1 – link-s2 – link s9 – return- s2;
 Path 17: s1 – link-s2 – link s9 – link – s15 – exit – s2;
 Path 18: s1 – link-s2 – link s9 – link – s15 – link – s9;
 Path 19: s1 – link-s2 – link s9 – link – s15 – link – s16 –
 return – s15;
 Path 20: s1 – link-s2 – link s9 – link – s15 – link – s16;

For Shopping with the feedback result and interactive chatting sub model in fig. 9, test tree is fig. 10 and test paths are as follows:

Test Path:

Path 21: s1 – error – s1;
 Path 22: s1 – link-s2 – exit – s1;
 Path 23: s1 – link-s2 – link s9 – return- s2;
 Path 24: s1 – link-s2 – link s9 – link – s13 – exit – s2;
 Path 25: s1 – link-s2 – link s9 – link – s13 – link – s14 –
 return – s2;
 Path 26: s1 – link-s2 – link s9 – link – s13 – link – s14 –
 exit;

V. RESULTS

For the Specific Testing Process Model proposed in our previous research [14]. Described and implemented the navigational aspect that how the navigation model is divided into sub models. Tests paths are generated from the test tree developed for each sub model.

VI. CONCLUSION

Researcher has implemented navigation aspect of the specific testing process model. Using navigation model test tree is generated to describe test path of the web application. In future, researcher will validate the specific testing process model.

ACKNOWLEDGMENT

I am deeply indebted JECRC University, Jaipur, Rajasthan, India to support this research.

REFERENCES

1. Guell, N., Schwabe, D. and Vilain, P.,(2000), ‘Modeling Interactions and Navigation in Web Applications’, Stephen W. L., Heinrich C. M., Bernhard T. (eds.), Wrkshops on Conceptual Modeling Approaches for E-Business and The World Wide Web and Conceptual Modeling: Conceptual Modeling for E-Business and the Web, Utah, USA, Springer Berlin Heidelberg, pp. 115-127.
2. Bellettini C., Marchetto A., and Trentini A.. (2004), ‘WebUML: reverse engineering of web applications’, Sara C., Marlon D., Maristella M. (eds.) *In Proceedings of the 2004 ACM symposium on Applied computing (SAC '04). ACM*, New York, NY, USA, pp. 1662-1669.
3. Zhang G., Knapp A., (2006), ‘Model Transformations for Integrating and Validating Web Application Models’, in Ruth B. and Heinrich C. (eds.) *Modellierung, International workshop, MOD 2006*, Innsbruck, Austria; Springer, pp.115–128.)
4. Hofmeister C., and Han M (2006), ‘Modeling and verification of adaptive navigation in web applications’, in Ginige A., Wolber D., and Calder N. Brooks C (eds.) *Web Engineering, 6th International Conference ICWE 2006*, Palo Alto, California, ACM press, pp.329–336.
5. Zhongsheng Q., Liping L., Huaikou M., (2008), ‘A UML-Based Approach to Testing Web Applications”, Fei Y., Wen C., Zhigang C., Jie Y. (eds.), *International Symposium on Computer Science and Computational Technology*, Shanghai, China, IEEE Society, pp.397-401.
6. Kundu D. and Samantha D. (2009), ‘ A Novel Approach to Generate test Cases from UML Activity Diagrams’, *Journal of Object Technology*, **8(3)**, pp-65-83.
7. Garcia B., Juan C. Duenas.(2011), ‘Automated Functional Testing based on the Navigation of Web Applications’, Laura K., Rosario P. and Francesco T. (eds.), *7th International Workshop on Automated Specification and Verification of Web Systems*, Iceland, Electronic Proceedings in Theoretical Computer Science, pp. 49-65.
8. Busch M. , Knapp A. , Koch N., (2011) , ‘Modeling Secure Navigation in Web Information Systems’, Grabis J., Kirikova M.(eds.), *10th International conference on Business Informatics Research*, Riga, Latvia, Springer Berlin Heidelberg, pp.239-253.

9. Panthi V. and Mohapatra D. P., (2012), ‘Automatic test case generation using sequence diagram’, *International Journal of Applied Information Systems*, **2(4)**, pp.23-29.
10. Nora K., Andreas K. (2003), ‘Towards a common meta-model for development of web applications’, in Lovelle J., Rodriguez B., Aguilar L., Gayo J. and Ruiz M. (eds.) *Web Engineering, 3rd International conference, ICWE 2003*, Oviedo, Spain, July 14-18, 2003, Springer, pp.497.
11. Garica B., (2015), ‘Web browsing automation for applications quality control’, *Journal of web engineering*, **14 (5)**, pp. 474-502.
12. Kripke S.A., (1963), ‘Semantical Consideration on Modal Logic I. normal propositional calculi ’, *Acta philosophica fennica*, **9(5)**, pp. 67-96.
13. Liu P., Miao H., Zeng H. and Cai L. (2013), ‘An approach to test generation for web applications’, *International Journal of u-and e-service, science and technology*, **6(1)**, pp. 61-75.
14. Singh Garima, Kaushik Manju (2016) “Dual Security Testing Model for Web Applications”, *International journal of advanced computer science and applications*, **7(2)**, 2158-107X.

AUTHORS PROFILE

Garima Singh, Research scholar is pursuing her PhD from JECRC University, Jaipur, Rajasthan, India. She has completed her MCA from University of Rajasthan, Jaipur, Rajasthan, India with honors.

Dr. Manju Kaushik, Associate Professor, Dept. of Computer Science and Engineering at JECRC University, Jaipur, Rajasthan, India. She has completed her PhD from Mohan Lal Sukhadia University , Udaipur, Rajasthan, India.

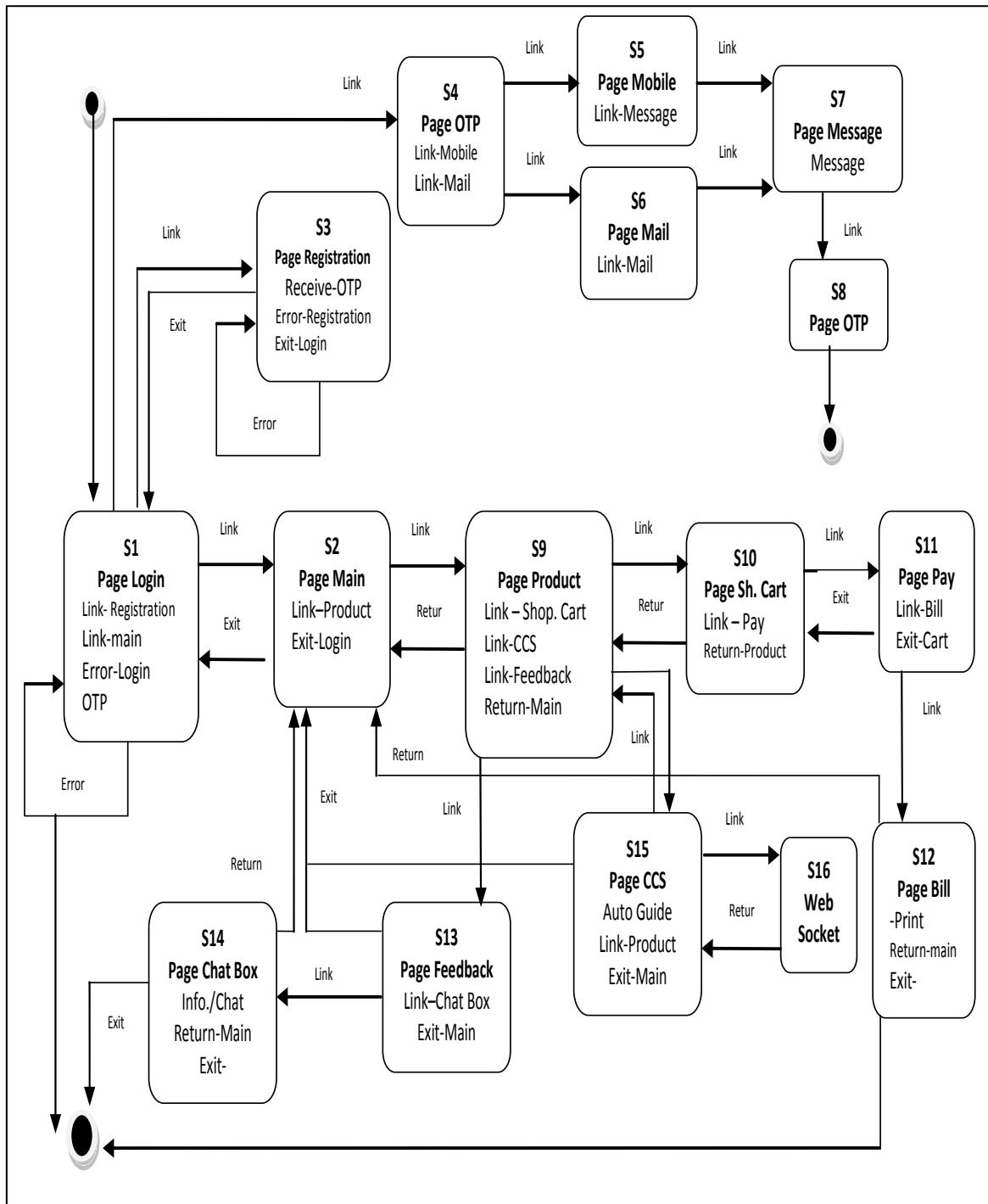


Figure1. Navigation Model for Dual Security Testing Model

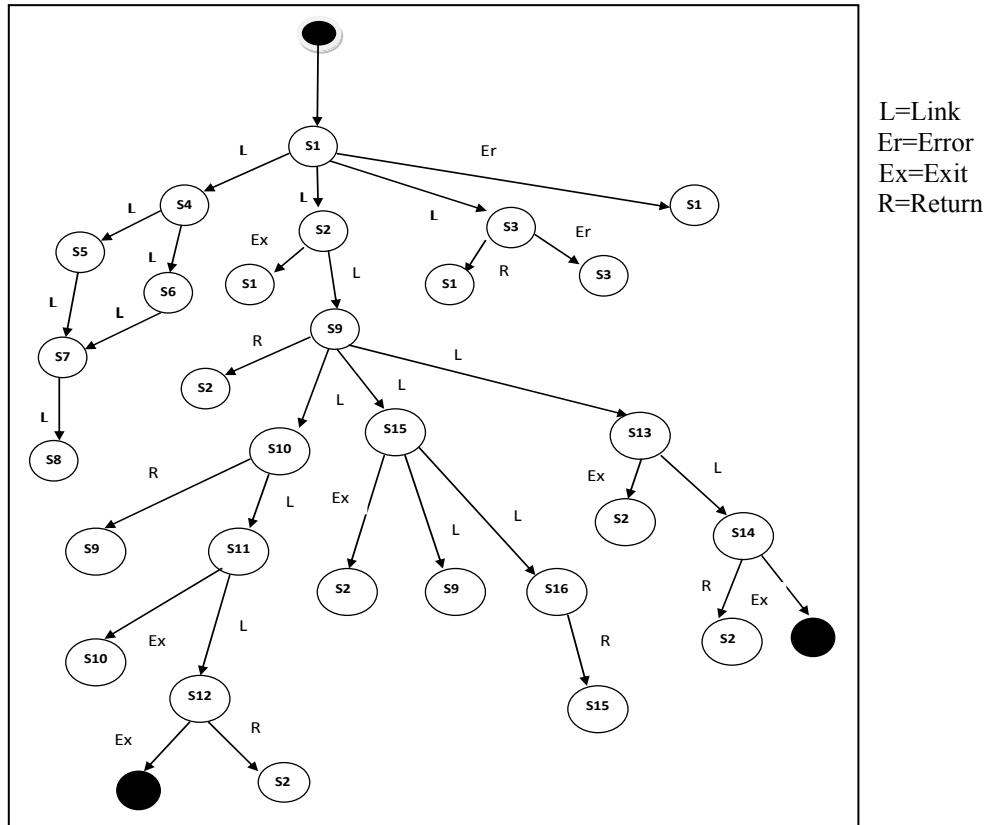


Figure 2. Test tree diagram for fig. 1.

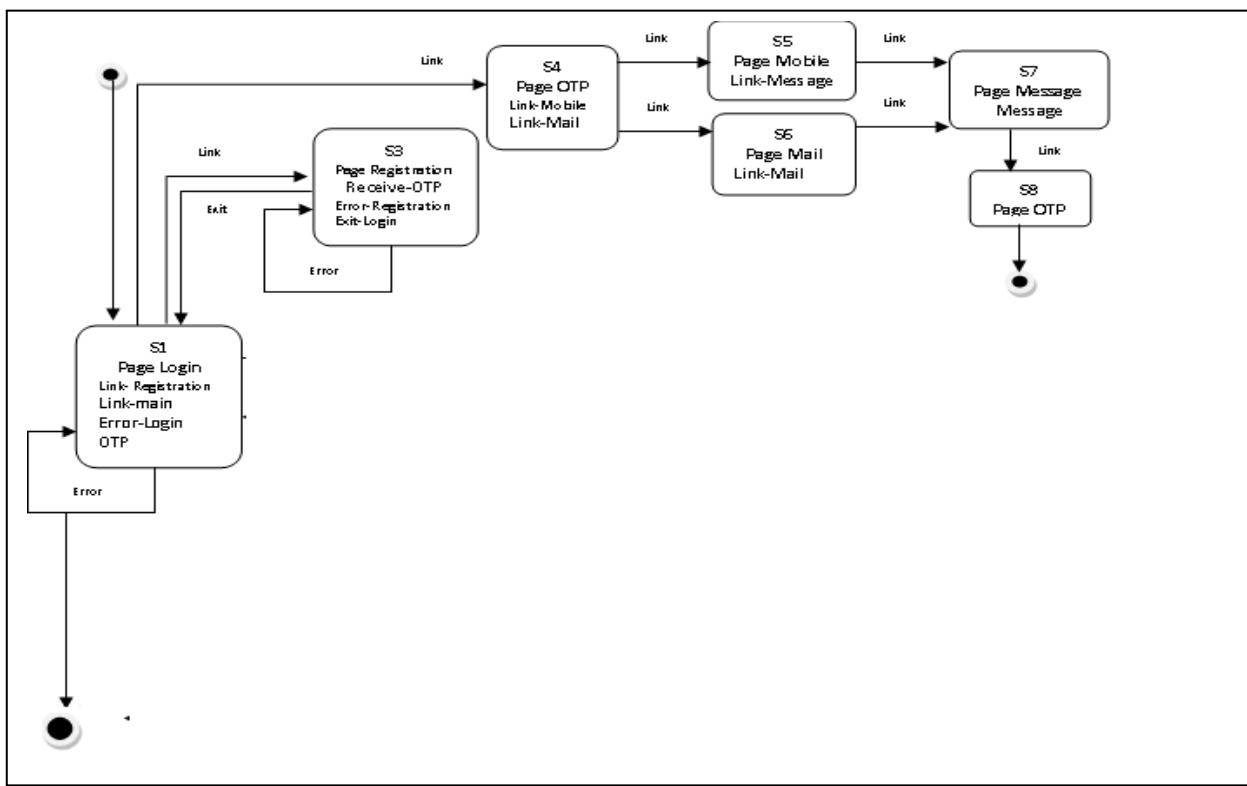


Figure 3. Login Registration Navigation sub Model

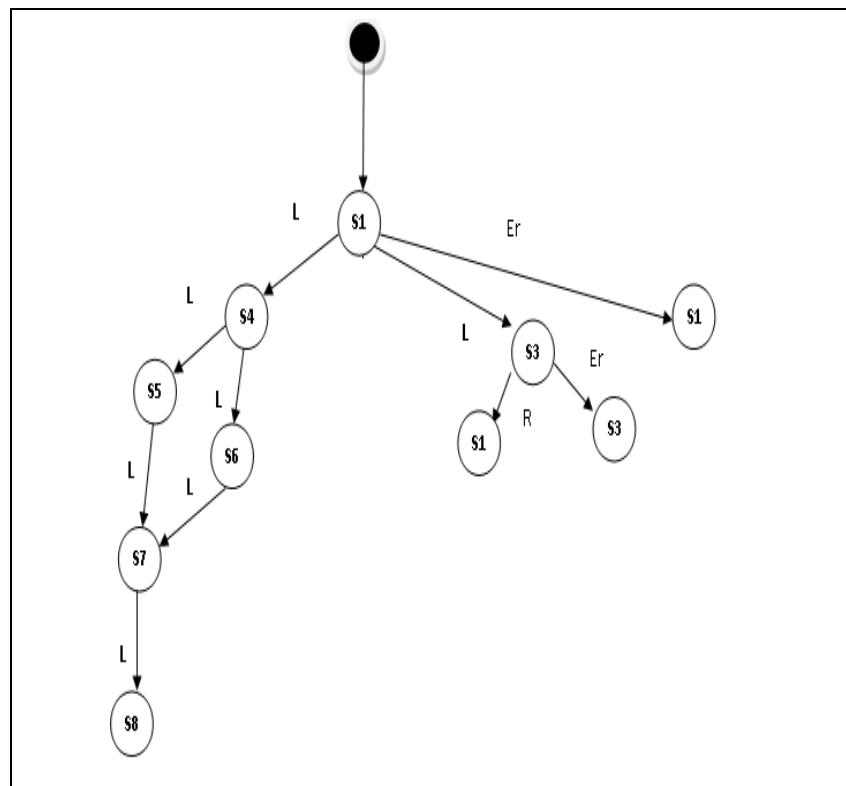


Figure4. Test tree for fig. 3

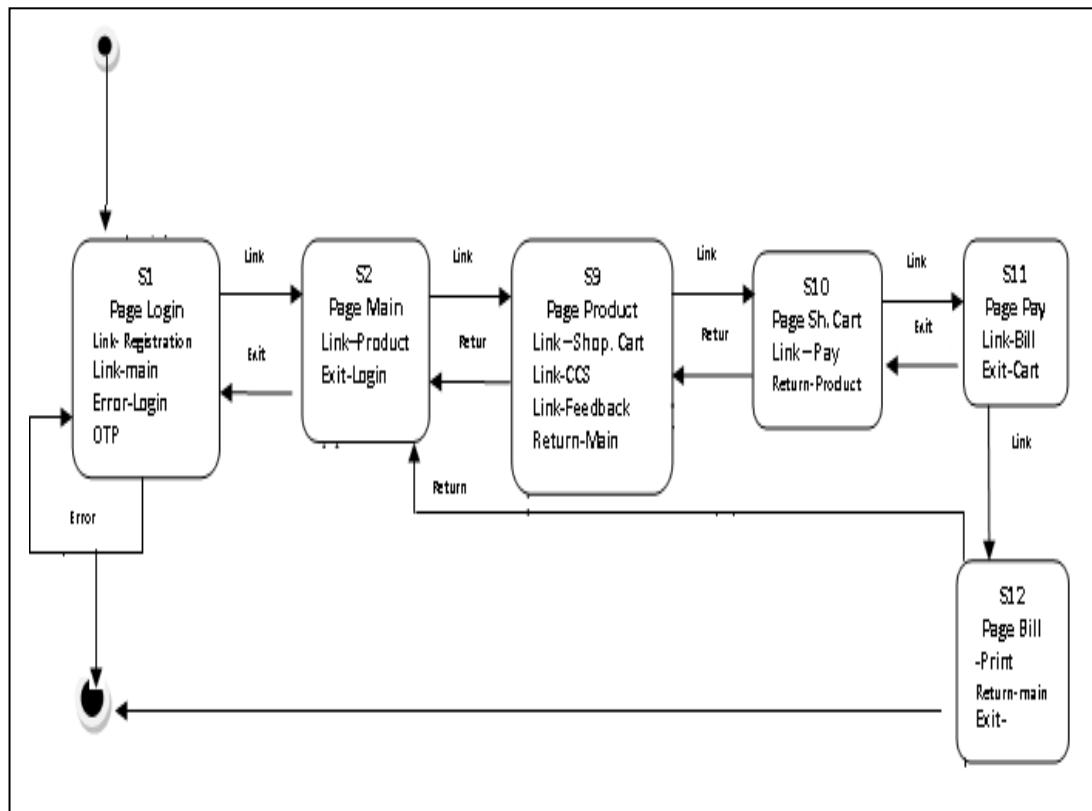


Figure5. Complete Shopping and Billing sub model

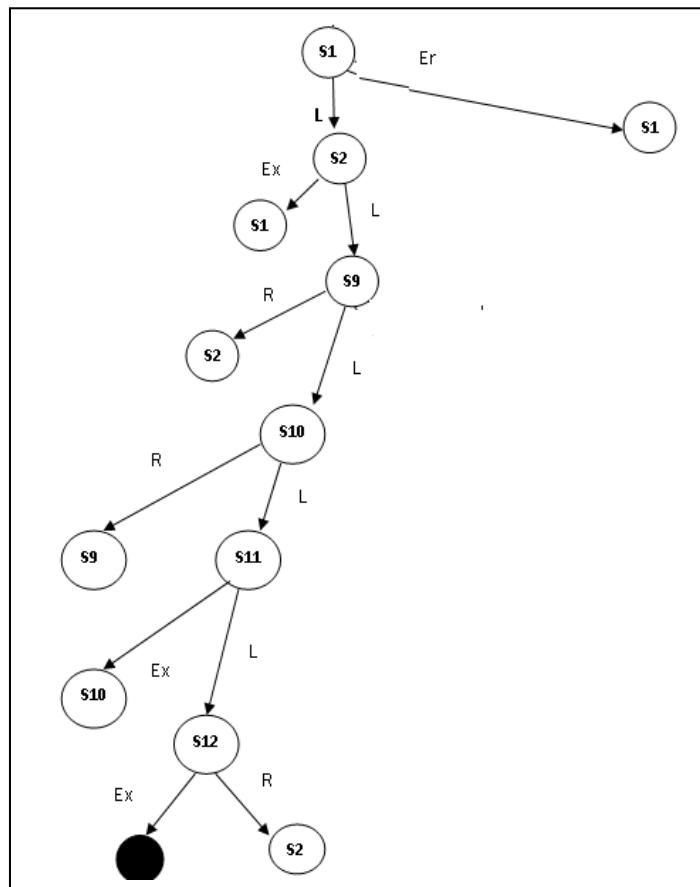


Figure6. Test tree for fig. 5

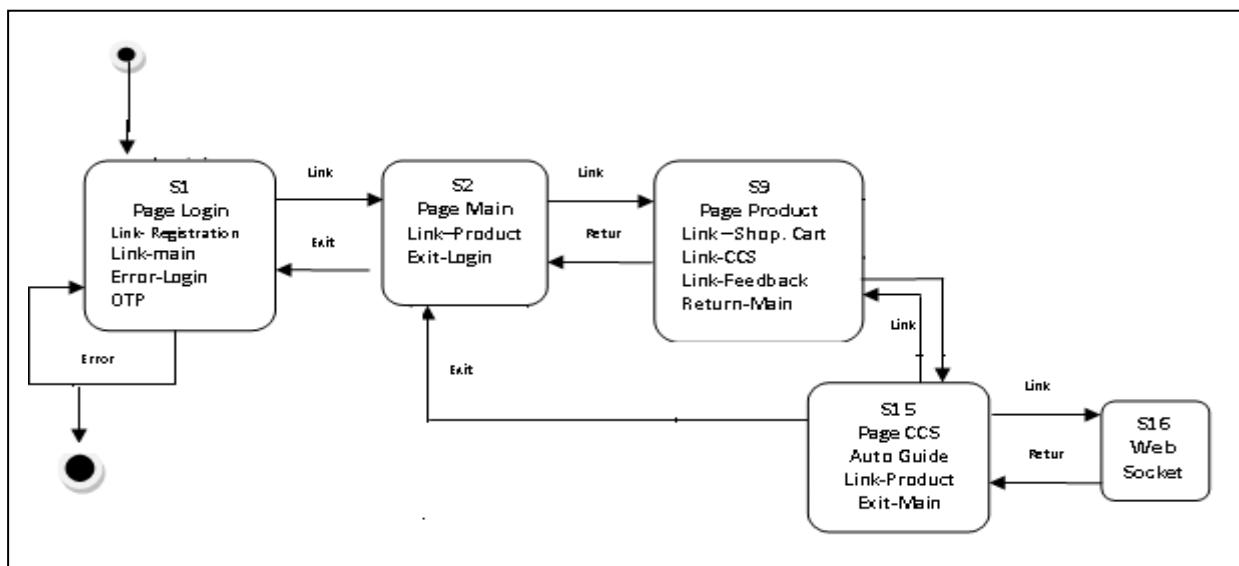


Figure7. Shopping in association of Automated Guide sub model

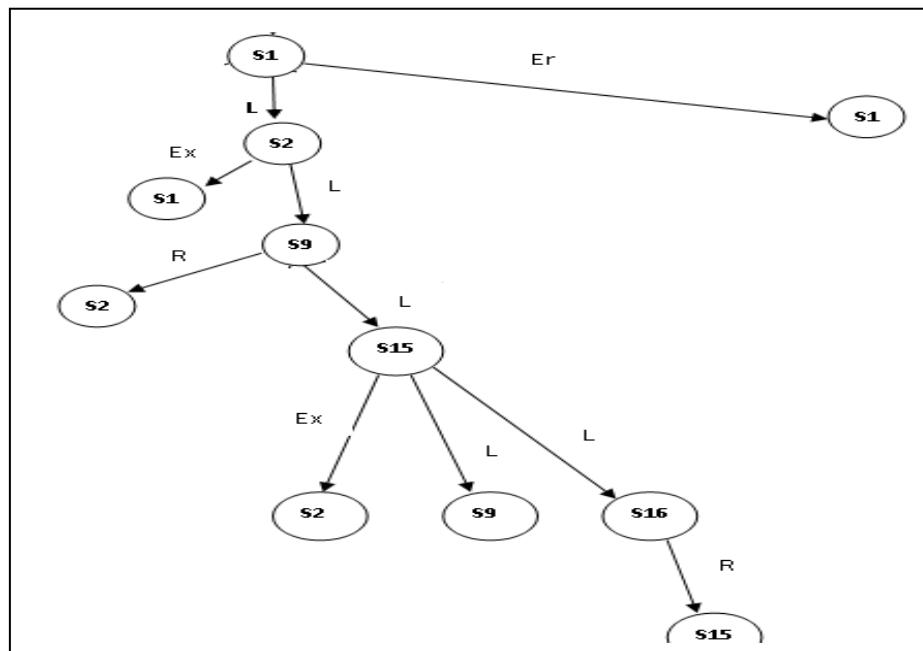


Figure8. Test Tree for fig.7

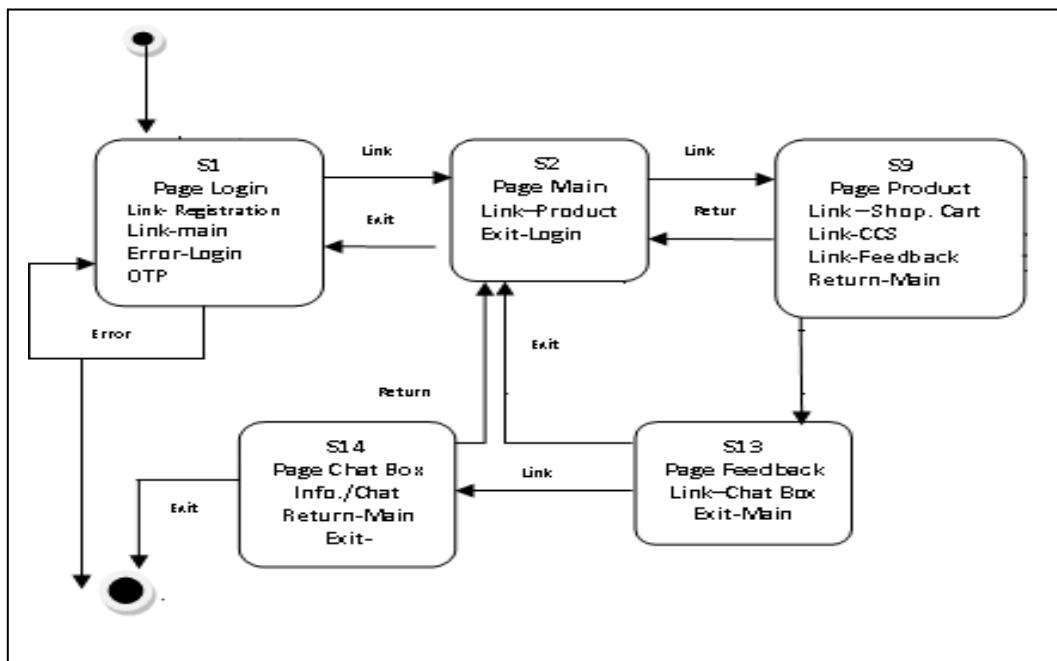


Figure9. Shopping with the feedback result and interactive chatting sub model

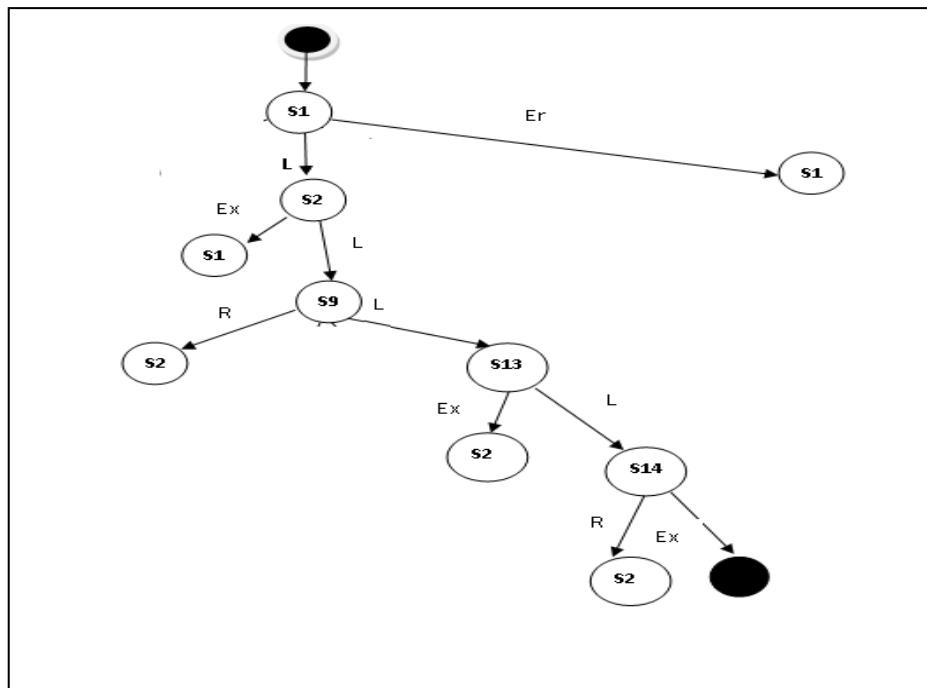


Figure10. Test Tree for fig.9

Comparative Analysis of LEACH and V-LEACH Protocols in Wireless Sensor Networks

Layla Aziz*¹, Said Raghay¹, Abdellah Jamali², and Hanane Aznaoui¹

¹ Laboratory(LAMAI),Cadi Ayyad University, Marrakech, Morocco

²Laboratory (RI2M), Hassan 1st University , Berrchid, Morocco

* Corresponding author

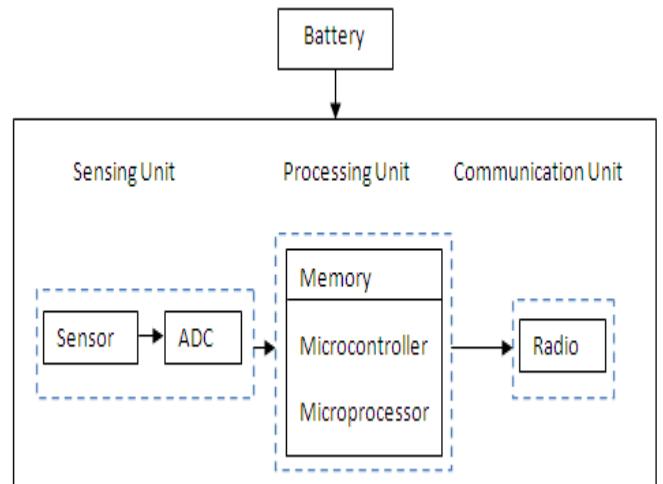


Fig. 1. Sensor node structure

Abstract—In the past few years, the research community is strongly attracted to wireless sensor networks (WSNs). Sensor node is generally driven by an irreplaceable battery which limits its energy supply. A number of new methods and strategies have been proposed to reduce energy consumption in WSNs. LEACH (Low Energy Adaptive Clustering Hierarchy) protocol is a well known approach using the Clustering mechanism to minimize the energy consumption and improve the lifetime of WSN . In this work, we describe various clustering algorithms and a comparative analysis of LEACH protocol with its improved version V-LEACH using NS2 simulator.

Index Terms— CLUSTERING, LEACH, NS2, V-LEACH, WSN.

I. INTRODUCTION

A wireless sensor network is a collection of nodes organized into a cooperative network [1]. Each sensor node consists of processing capability (microcontrollers, CPUs or DSP chips), integrating multiple types of memory (program, data and flash memories), having a RF transceiver (usually with a single Omni-directional antenna), having a power source (e.g., batteries and solar cells), various sensors and actuators. Basically, nodes are driven by batteries that replacement is overly complicated.

A typical sensor node includes four basic components: a sensing unit, a processing unit, a communication unit and a power unit as depicted in Figure. 1. Localization and Routing are the key factors and very crucial issues that need to be considered due to the severe energy constraints. Consequently

efficient energy management is the biggest challenge for the enhancement of the network lifetime.

We can classify routing protocols as follows [2,3]:

1) Flat/Data-centric routing : in this technique of routing, all nodes play the same role using attribute based addressing and collaborate together in order to perform the sensing of data. The sink node demands informations from sensor nodes in a particular zone. SPIN (Sensor Protocols for Information via Negotiation) [4] protocol represents a well known Flat/data-centric routing protocol.

2) Hierarchical: Hierarchical routing protocols consist of the clustering mechanism to organize the sensor network. In clustering, a particular node chosen among the sensor nodes called Cluster Head which is responsible for the aggregation of sensing data from the environment that allow an efficient communication and prolong the network's lifetime [5]. This kind of routing is designed to improve the overall energy-efficiency and make protocols more scalable. LEACH and PEGASIS (Power-efficient Gathering in Sensor Information Systems) represent the well known examples of hierarchical protocols.

3) Location-based: sensor node's location is very important to perform an efficient communication in the WSNs. Consequently, Sensor node can use incoming signal strength to estimate the distance of its neighbors [6]. Some approaches use the GPS (Global Positioning System) to localize sensor nodes in the entire network [7]. GEAR (Geographic and Energy Aware Routing) [8] represents a well known approach of this kind of routing.

Many strategies and techniques have been proposed to prolong WSN's lifetime. Among these, clustering based routing protocols have shown a significant position to utilize the energy efficiently and effectively. A network with clustering aims at dividing the sensor nodes into a number of groups called clusters .Each cluster elects a node as cluster head in order to collect the data locally from the cluster members and transmits the aggregated data either directly or via multi-hop transmission to the sink . All sensor nodes serve the requests

with a cooperative way. The main constraint in wireless communications is the limited duration of mobile terminals whose energy source is often a battery whose capacity is limited life. This constraint is much more important in wireless sensor networks. Two of the most popular hierarchical protocols are LEACH and PEGASIS. These protocols show significant reduction in the overall network energy over other non-clustering strategies. Section 2 describes different clustering algorithms like LEACH protocol. Finally, section 3 concludes with some simulation results to compare LEACH and V-LEACH protocols.

II. DESCRIPTION OF VARIOUS CLUSTERING ALGORITHM

Clustering is considered as a key mechanism exploited to prolong the sensor network lifespan by minimizing the energy consumption of nodes [9,10]. Forming clusters allows the sensor network to be more scalable. Clustering mechanism is based on the creation of virtual groups called Cluster. Each cluster has a local coordinator called Cluster Head chosen among nodes in order to perform inter-cluster and intra-cluster communication. Clustering has many advantages such as more scalability, less energy consumption, less load and more robustness. In clustered network, the communication is divided into intra and inter cluster communication [11].

Several approaches use the clustering mechanism to communicate efficiently in a Wireless Sensor Network . But the Cluster Heads selection is an important parameter which must be strongly considered in order to perform the energy efficiency in clustered networks.

Figure. 2 depicts the hierarchical clustering.

A. TEEN

Threshold sensitive Energy Efficient sensor Network (TEEN) [12,13] is a cluster based protocol proposed by Anjeshwar and Agrawal, it belongs to the hierarchical protocols family whose main goal is to react with sudden changes in the sensed attributes such as temperature. It is the first method designed for reactive networks. This new scheme merges the hierarchical approach and data-centric strategy. During

sensing data phase, each node senses its surrounding continuously with energy consumption cost less than that in the proactive network; consequently, transmitting data is performed less frequently.

TEEN scheme uses a 2-tier clustering topology and two main thresholds Hard Threshold(H_t) and Soft Threshold (S_t) transmitted by the Cluster Heads, The first one is a threshold value required for the sensed attribute step. When the sensor node senses this value, it is required to pass on its transmitter and report back to its CH if the hard threshold (H_t) is reached. The second threshold is a small change in the value of the sensed attribute which triggers the node to switch on its transmitter and transmit the detected data. Combining these two thresholds permits this protocol to control data transmission by transmitting only the sensitive data required, thus the energy transmission consumption is reduced. Additionally, receiving data become more effective and very useful. Figure. 3 shows the clustering topology in TEEN scheme.

B. APTEEN

Manjeshwar and Agrawal propose an extended version of TEEN scheme The Adaptive Threshold sensitive Energy Efficient sensor Network protocol (APTEEN). Its principal improvement over TEEN is that it permits to transmit data periodically and react to time critical situations [14]. It is an hybrid protocol that adapts threshold values used in TEEN

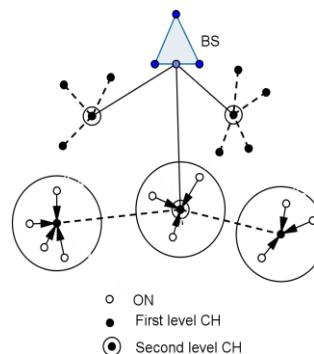


Fig. 3 TEEN protocol

according to user requirements and application types. This new approach considers a query system which supports three types of queries: historical, on-time, and persistent. Furthermore, QoS requirements are integrated for the on-time queries in order to respond to user needs and the TDMA schedule is modified in way to minimize delay .

In APTEEN protocol, four parameters are broadcasted by CHs in order to manage the sensor nodes transmission : the first parameter is Attributes which represent the physical parameters that the user is interested in obtaining data about. The second consists of Thresholds parameter , we have two thresholds : H_t is used to transmit the sensed data which means a sensor node can't transfer its data except it has a

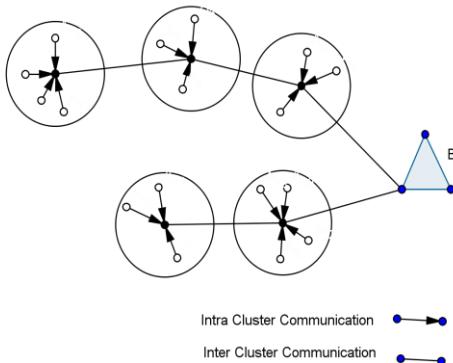


Fig. 2 Architecture of Cluster based protocols

particular value H_t . The second threshold is used to trigger a node to transfer data when a minor variation is detected. Third parameter is called the TDMA schedule or the schedule which permits every sensor node to send its sensed data in an allocated period.

The last parameter is Count time (CT) which is the maximum time allowing to manage the successive reports transmitted by a node. The hybrid APTEEN scheme permits the combination of both proactive characteristics like LEACH protocol and reactive characteristics like TEEN scheme. Thus, it is suitable for both proactive and reactive applications; this approach represents a great deal of flexibility by setting the count-time interval, and the threshold values for the energy consumption. Both TEEN and APTEEN have the same drawbacks like the additional overhead and complexity required to form clusters at multiple levels and implement the parameters such as threshold-based functions and the count time [15,16]. The way to deal with attribute-based naming of queries APTEEN more than TEEN.

C. EECS

EECS is another variant of LEACH protocol which considers the clusters to organize the sensor nodes and the direct communication between CHs and the BS. However, this clustering scheme considers the residual energy for selecting the network CHs [17].

The Non-CH node takes its decision to belong to a CH considering the distance parameter . That means this protocol uses a new weighted function to form clusters . This function does not depends only on the intra-cluster distance but also on the distance separating CHs from sink node. Consequently, sensor node joins the closest CH to conserve the cluster energy consumption and ease the role of the CHs considering minimum distance between CHs and BS.

D. HEED

Hybrid Energy-Efficient Distributed clustering (HEED) [18] is an efficient method proposed by Younis and Fahmy. It belongs to the multi-hop clustering algorithm family.

This new approach represents an energy-efficient clustering method which considers explicitly the residual energy of sensor node to select CHs instead of the random selection as in LEACH protocol. Thus, this protocol enhances the Cluster formation and performs it exploiting the hybrid combination of two important parameters: the node's residual energy and the intra-cluster communication cost.

HEED protocol resolves ties problem which can be occurred for some sensor nodes. That's means it can manage the localization of sensor node in more than one CH. The CH selection is performed according to the following probability:

$$CHprob = Cprob * Eresidual / Emax \\ CHprob = Cprob * \\ Eresidual / Emax$$

E. LEACH

The design of this protocol [19,20] aims at minimizing the energy consumption of the network. It is the most popular clustering algorithm for WSN which organizes the sensor

nodes in areas called clusters. Each sensor node attempts to be the local coordinator of its cluster. This selection is autonomous and depends on a stochastic threshold $T(n)$.

The main advantage of LEACH protocol is that it reduces the number of nodes that communicate directly with the base station and this is done by the formation of Cluster Heads. Then the other neighbor nodes connect and become a member of the CH, and they spend the least amount of energy. Only CH is allowed to communicate with the sink node. Each CH allocates a specific period to a neighbor node to establish a communication link. Leach protocol provides a conception of round which consists of two distinct operational phases. In each round, each node must decide whether to be selected as a cluster head based on a probability factor $T(n)$ and the fact it was not CH in the previous round, or it must join a cluster. LEACH protocol uses round as unit, each round is made up of a set-up stage and steady stage, in the setup stage, a cluster-head is chosen in order to manage the communication in its cluster. The steady phase consists of sending the sensed data to the central sink node. The steady phase takes more time than the setup phase.

1) Set-up Phase:

Cluster-setup phase is introduced by an advertisement sub-phase which consists of informing their neighborhood with broadcasting an advertisement packet to inform the entire network that they become CHs [21]. Remaining sensor nodes pick the advertisement packet with the strongest received signal strength. The decision of a sensor node to act as a CH is done independently on the other nodes and based on when the node served as cluster head for the last time the node that has not been cluster head for a long time has more probability to be elected. LEACH protocol uses a stochastic threshold algorithm which is allows that each node becomes a CH at least once .This is done according to a threshold value $T(n)$ which depends upon several parameters. The communication process between the CH and its members begins by the creation of a TDMA schedule which will be broadcasted to the cluster members. Every node desiring to play the role of a local coordinator (CH) chooses a random number between 0 and 1. Such node becomes currently a CH only if the chosen random number is less than the threshold value $T(n)$. Then each elected CH invites the remaining nodes to join their clusters by broadcasting an advertisement message in the network. Then, the non-cluster head nodes decide to join the clusters based upon the strength of the advertisement signal. The set-up phase is based on the selection of cluster head nodes among all the sensor nodes using a stochastic algorithm and several clusters are formed in a dynamic way.

2) Steady phase :

Figure. 4 shows the flowchart for steady phase of LEACH protocol. The phase of election of Cluster Heads is followed by informing the entire sensor network by the CH chosen for the current round .This is done by broadcasting an advertisement message ADV using a non persistent carrier sense multiple access CSMA to avoid the interferences. Non Cluster Head nodes belong to a cluster using a join request message (Join_REQ) transmitted back to the chosen cluster

head. After that Data Transmission stage began. This sub phase consists of sending data of the nodes to CH according to their predefined TDMA slot without spending more energy.

To minimize energy dissipation in the entire network, each non-CH node can be at a rest during the non allocated TDMA slots. Once all the data has been received by the CH from its members, it sends the aggregated data directly to the BS as shown in Figure. 5.

The direct routing of packets from CHs to BS represents the main drawback in LEACH protocol because we haven't any control of the distances between the CHs and the BS.

F. PEGASIS

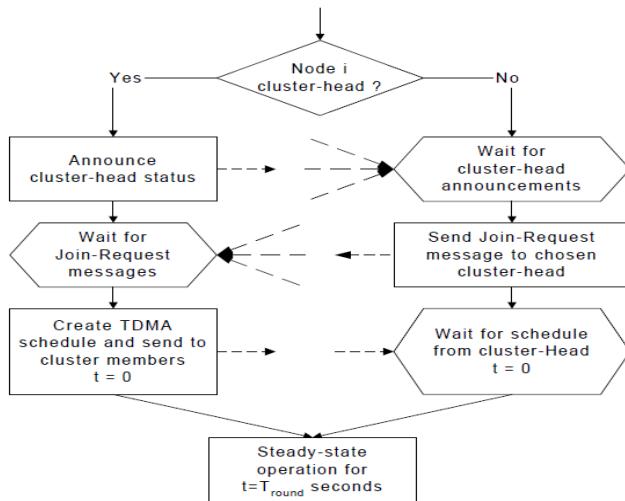


Fig. 4 Steady phase in LEACH protocol

PEGASIS [22] is based on a near optimal chain instead of clusters as in LEACH. This chain is carried out based on a greedy algorithm which begins from the furthest sensor node from the sink node as in the greedy approach. On the other hand, the sink node is able to calculate this optimal chain and transmits it to the entire sensor network. The main efficient improvement of this protocol is that routing of packets is occurred only with close neighbors, that's represents a great

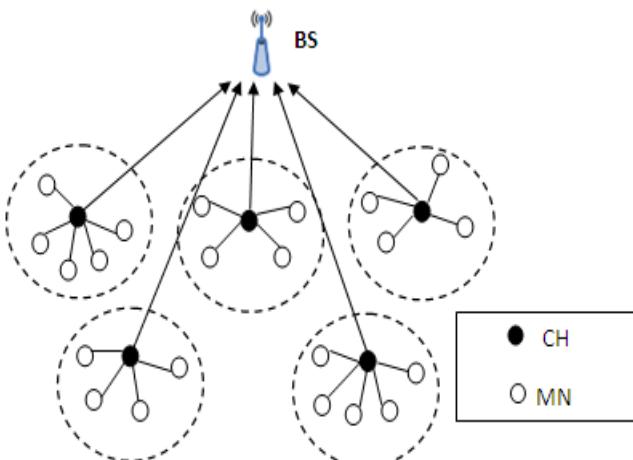


Fig. 5 LEACH protocol

enhancement over original LEACH and this allows the reduction of energy consumption by minimizing the distance and therefore the number of transmissions received by each node.

G. LEACH-C

This protocol [23] is based on a centralized approach where the information of node location and energy level are communicated to base station at the first phase of each round. This method is characterized by the strong integration of sink node to perform the CH selection and cluster formation. The cluster head is selected according to the average residual energy for all nodes computed by received data. In LEACH-C, the average energy is used as threshold for the CHs selection. The sink node broadcasts a message of the optimum cluster head IDs (Identifiers) in the network and selects the node having such optimum CH IDs as cluster head. After the CH selection, the Non-CH nodes wait for the TDMA schedule previously prepared.

The main advantage of LEACH-C is to overcome the problem of uncertainty on the number of cluster-head at each round in LEACH, but it still suffers from many problems including equal opportunities for cluster-head selection mechanism, and the unbalancing energy loads.

It can be possible to select CHs with insufficient energy which leads to communicational problems.

H. V-LEACH

It represents an enhanced version of LEACH protocol which defines a new scheme. This scheme is based on the CH and its members and an additional element known as vice-CH which replaces the CH when it is died. This protocol has improved the network lifetime because it handles the early death of nodes. Figure.6 shows the V-LEACH scheme.

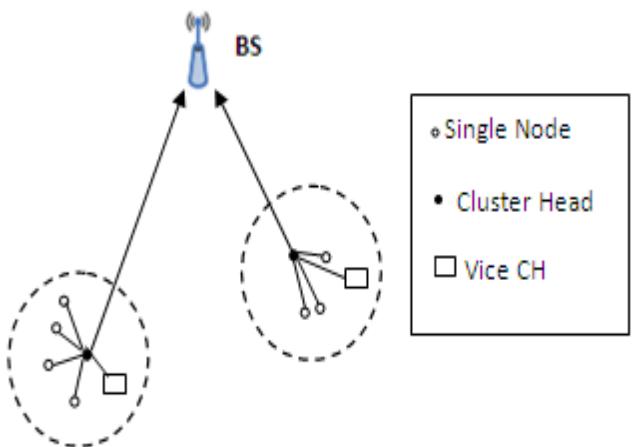


Fig. 6 V-LEACH protocol

TABLEI. PROTOCOLS COMPARISON

Routing Protocols	Classification	Mobility	Delivery Delay	Scalability	Load Balancing	Algorithm Complexity
LEACH	Clustering	Fixed BS	Very small	Limited	Medium	Low
		Fixed BS	Very Large	Good	Medium	High
PEGASIS	Reactive/Clustering					
HEED	Clustering	Stationary	Medium	Very good	Medium	Medium
LEACH-C	Clustering	Fixed BS	Small	Very good	Medium	Medium
TEEN	Reactive/Clustering	Fixed BS	Small	Low	Good	High
APTEEN	Hybrid	Fixed BS	Low	Good	Moderate	Very High
V-LEACH	Clustering	Fixed BS	Small			

Table 1 shows the comparison summary between the cluster based routing protocols [24, 26].

III. COMPARISON OF LEACH AND V-LEACH PROTOCOLS

Table 2 compares briefly LEACH protocol and LEACH-C and PEGASIS and V-LEACH protocols in terms of the assumption parameter which describes the strategy of each protocol to organize the sensor nodes using many mechanisms such as the clustering and the optimal chain scheme.

The CH selection criterion in the clustered WSNs is very important and plays a vital role.

The routing protocols use a various techniques to select the Cluster Head for the network clusters. This selection can be probabilistic like LEACH protocol but many improved versions of LEACH use the residual energy of sensor nodes to select the CHs and that resolves many problems and improves the network lifetime.

Using a distributed algorithm, the CH selection is autonomous without any centralized intervention. On the other side, the CH selection can be done based on a centralized management as in the several centralized versions of LEACH protocol such as LEACH-C.

In this centralized approach, the BS manages the clusters and chooses the CHs according to the residual energy and the node position.

In PEGASIS protocol, the sensor nodes are organized into a chain using a greedy algorithm which allows communication between nodes and their neighbors. PEGASIS uses the probabilistic approach for the CH selection like LEACH protocol.

V-LEACH protocol uses a vice-CH in order to alternate the CH when its energy is completely exhausted. This idea has prolonged the network lifetime which represents a great improvement over the original LEACH.

Scalability is another important aspect which must be considered to handle the long distance which separates the different sensor nodes in WSNs [27].

Routing protocols have to be scalable and more adaptive to the dynamic topology in the WSNs. More scalable routing protocols can be efficiently used in large-scale WSNs which have a great number of sensor nodes.

LEACH and V-LEACH protocols are compared in terms of important aspects as shown in the Table 2:

TABLEI. LEACH AND PEGASIS AND LEACH-C AND V-LEACH COMPARISON

Protocol	Assumption	CH Selection	Scalability	Hop Count	Energy Efficiency
LEACH	The nodes are distributed randomly, the nodes are homogenous	Probabilistic approach	Limited	Single	Poor
	Based on an optimal near chain instead of clusters	Probabilistic	Good	Single	Very high
PEGASIS	Uses the centralized approach and its Steady-state phase is identical to that of the LEACH protocol	The BS selects CHs based on their residual energy	Very good	Single	Very high
	Uses a vice-CH when the CH dies	Energy	Good	Single	High
LEACH-C					
V-LEACH					

IV. SIMULATION RESULTS

In this section, we present the simulation results of LEACH and V-LEACH protocols to make effective analysis. The scenario is based on varying the location of the BS. This simulation is done by the Network Simulator (NS-2.34) and the simulation parameters are shown in Table 3.

LEACH and V-LEACH protocols are compared based on many important metrics like the energy consumption and the number of alive nodes metrics [28,29]

TABLEIII. : SIMULATION PARAMETERS

Parameter	Value
Simulation area	1000*1000
Number of nodes	100
BS locations	(50,150) ,(50,200), (100,250)
Channel type	Wireless
Simulation time	400 sec
Node's initial energy	2 J

A. The energy dissipation over time:

Figure. 7 and Figure. 8 and Figure. 9 show the energy dissipation of LEACH and V-LEACH protocols according to the different BS locations . It is clearly shown that LEACH protocol consumes more energy than V-LEACH because it selects the CHs randomly using a probabilistic model that distributes the CH among the clusters in an uneven manner. In fact, sometimes we can have a possibility that more than one CH can be selected. So, a sudden increase or decrease of energy dissipation can be provided. Additionally, the original LEACH doesn't handle the communicational process after the death of CHs. While V-LEACH dissipates less energy than LEACH reasoning that this enhanced approach selects the cluster head dependently on the residual energy and alternates the died CH with the vice-CH. However, V-LEACH becomes instable when the BS location is far. The results instability is due to the lack of controlling the distance between the CHs and the BS.

We observe from simulation results that the BS location has a significant impact on the protocols performances. Consequently, it is required to consider the inter-cluster communication and the intra-cluster communication.

B. The number of alive nodes over time:

Figure.10 and Figure.11 convey that the number of alive nodes

decreases fast in LEACH Compared to V-LEACH with the variation of the BS location. That is due to the formation of an undesired number of cluster head in LEACH protocol. However, V-LEACH prolong the network lifetime because it modifies the cluster formation using an additional member : vice-CH which replaces the cluster CH after its death.

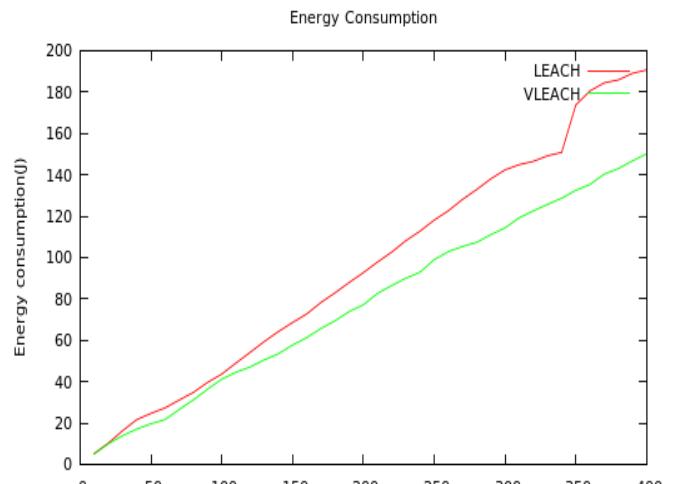


Fig. 7 Energy consumption with BS coordinate(50,150)

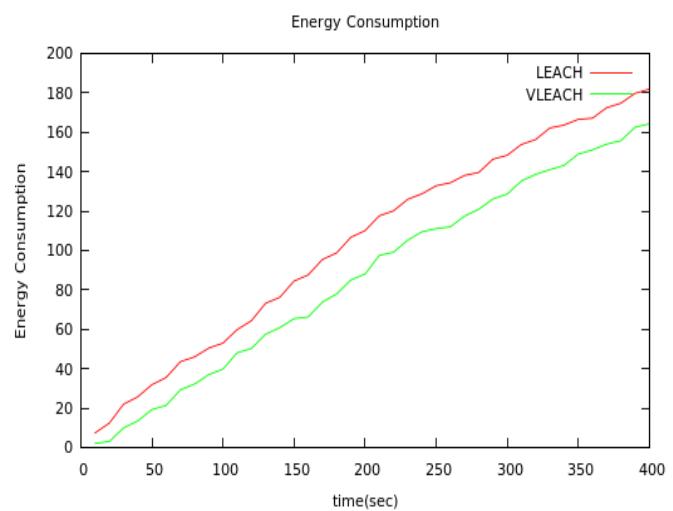


Fig. 8 Energy consumption with BS coordinate(50,200)

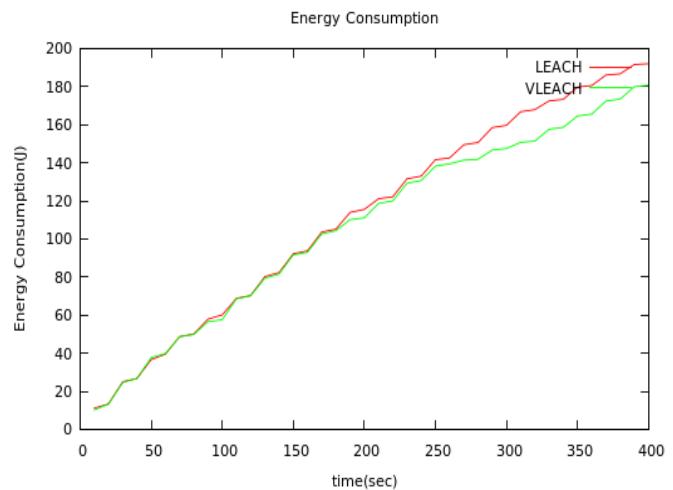


Fig. 9 Energy consumption with BS coordinate(100,250)

V. CONCLUSION

Wireless Sensor Networks are emerging in several research fields. In this context, there is a great need of approaches and strategies designed for such applications. Clustering represents an efficient mechanism to overcome many limitations in WSNs. In this paper, we describe a various number of clustering algorithms and present a comparison between well known protocols. Additionally, we present the simulation results and analyses of LEACH and V-LEACH protocols. From simulation results, it show be mentioned that V-LEACH is more suitable for application where the BS location is not farthest because this approach replaces the died CH which prolong the network lifetime. However, V-LEACH becomes instable when the BS location is far because it doesn't control the distance between CHs and BS. Hence, it is strongly required to handle the distance separating CHs from BS.

Our future work will be the study of the effect of the node mobility on the performance of the protocols.

ACKNOWLEDGMENT

I acknowledge the support provided by my supervisors : Pr. Said RAGHAY and Pr. Abdellah JAMALI and the members of the laboratory LAMAI (Laboratory of Mathematics Applied and Informatics) of the Faculty of Science and Technology-Cadi Ayyad University-Marrakesh

REFERENCES

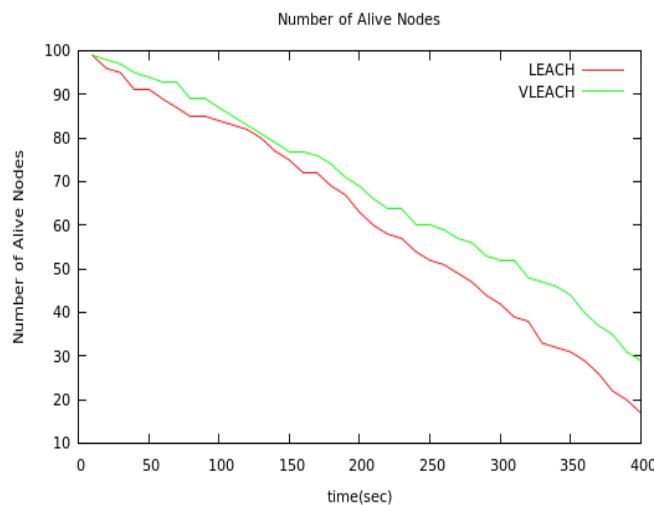


Fig. 10 Number of Alive nodes with BS coordinate(50,150)

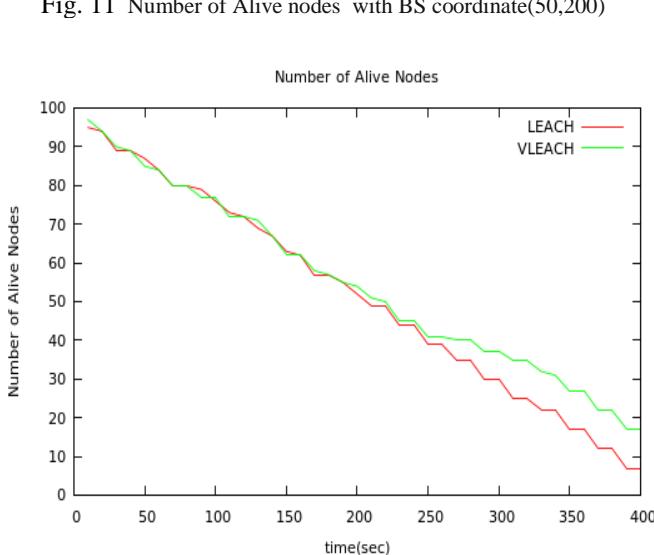


Fig. 11 Number of Alive nodes with BS coordinate(50,200)

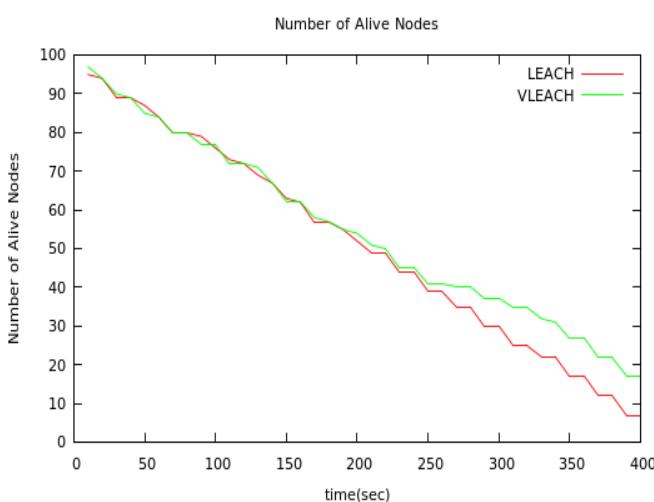


Fig. 12 Number of Alive nodes with BS coordinate(100,250)

1. S. El-Haddad, M. Girod Genet, and B. El-Hassan, "Mobile Wireless Sensor Networks using MDSAP, Model for a Hospital Application," 2008 4th Int. Conf. Wirel. Commun. Netw. Mob. Comput., pp. 1–6, 2008.
2. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," IEEE Commun. Mag., vol. 40, pp. 102–105, 2002.
3. K. Akkaya and M. Younis, "A survey on routing protocols for wireless sensor networks," Ad Hoc Networks, vol. 3, pp. 325–349, 2005.
4. W. R. Heinzelman, J. Kulik, and H. Balakrishnan, "Adaptive protocols for information dissemination in wireless sensor networks," Proc. 5th Annu. ACM/IEEE Int. Conf. Mob. Comput. Netw. - MobiCom '99, pp. 174–185, 1999.
5. C. Konstantopoulos, D. Gavalas, and G. Pantziou, "Clustering in mobile ad hoc networks through neighborhood stability-based mobility prediction," Comput. Networks, vol. 52, pp. 1797–1824, 2008.
6. D. Bhattacharyya, T. Kim, and S. Pal, "A Comparative Study of Wireless Sensor Networks and Their Routing Protocols," Sensors, vol. 10, pp. 10506–10523, 2010.
7. J. Arias, J. Lázaro, A. Zuloaga, J. Jiménez, and A. Astarloa, "GPS-less location algorithm for wireless sensor networks," Comput. Commun., vol. 30, pp. 2904–2916, 2007.
8. Y. Yu, R. Govindan, and D. Estrin, "Geographical and Energy Aware Routing: a recursive data dissemination protocol for wireless sensor networks," Energy, 2001.

9. J. N. Al-Karaki and a. E. Kamal, "Routing techniques in wireless sensor networks: a survey," *IEEE Wirel. Commun.*, vol. 11, pp. 1–37, 2004.
10. V. Katiyar, N. Chand, and S. Soni, "A survey on clustering algorithms for heterogeneous wireless sensor networks," *Situations*, vol. 19, p. 20, 2011.
11. P. Ding, J. Holliday, and A. Celik, "Distributed Energy-Efficient Hierarchical Clustering for Wireless Sensor Networks," in *IEEE International Conference on Distributed Computing in Sensor Systems*, 2005, pp. 322–339.
12. B. Krishnamachari and C. S. Raghavendra, "An adaptive energy-efficient and low-latency MAC for data gathering in wireless sensor networks," in 18th International Parallel and Distributed Processing Symposium, 2004. Proceedings., 2004, pp. 224–231.
13. a. Manjeshwar and D. P. Agrawal, "TEEN: a routing protocol for enhanced efficiency in wireless sensor networks," Proc. 15th Int. Parallel Distrib. Process. Symp. IPDPS 2001, 2001.
14. Manjeshwar A., D. P. Agrawal, and a Manjeshwar, "APTEEN: A hybrid protocol for efficient routing and comprehensive information retrieval in wireless sensor networks," in International Parallel and Distributed Processing Symposium, 2002, vol. 00, pp. 195–202.
15. D. Kandris, P. Tsioumas, A. Tzes, N. Pantazis, and D. D. Vergados, "Hierarchical energy efficient routing in wireless sensor networks," in 2008 Mediterranean Conference on Control and Automation Conference Proceedings MED08, 2008, pp. 1856–1861.
16. R. Vidhyapriya and P. T. Vanathi, "Conserving energy in wireless Sensor networks," *IEEE Potentials*, vol. 26, pp. 37–42, 2007.
17. T. Houngbadji and S. Pierre, "QoSNET: An integrated QoS network for routing protocols in large scale wireless sensor networks," *Comput. Commun.*, vol. 33, pp. 1334–1342, 2010.
18. O. Younis and S. Fahmy, "HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks," *IEEE Trans. Mob. Comput.*, vol. 03, pp. 366–379, 2004.
19. W. B. Heinzelman, a. P. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," *IEEE Trans. Wirel. Commun.*, vol. 1, pp. 660–670, 2002.
20. L. Aziz, S. Raghay, and A. Jamali, "A New Improved Algorithm of LEACH Protocol for WSN", in proceeding of IEEE Mediterranean Microwave Symposium (MMS'14), 2014
21. N. Marriwala and P. Rathee, "An approach to increase the wireless sensor network lifetime," *Inf. Commun. Technol. (WICT)*, 2012 World Congr., pp. 495–499, 2012.
22. S. Lindsey and C. S. Raghavendra, "PEGASIS: Power-efficient gathering in sensor information systems," in Proceedings, IEEE Aerospace Conference, 2002, vol. 3, pp. 3–1125–3–1130.
23. S. P. Singh and S. C. Sharma, "A Survey on Cluster Based Routing Protocols in Wireless Sensor Networks," *Procedia Comput. Sci.*, vol. 45, pp. 687–695, 2015.
24. X.-X. Liu, "A Survey on Clustering Routing Protocols in Wireless Sensor Networks," *Sensors*, vol. 12, pp. 11113–11153, 2012.
25. S. Naeimi, H. Ghafghazi, C.-O. Chow, and H. Ishii, "A survey on the taxonomy of cluster-based routing protocols for homogeneous wireless sensor networks.,," *Sensors (Basel)*, vol. 12, pp. 7350–409, 2012.
26. X. Liu, and J. Shi, "Clustering Routing Algorithms in Wireless Sensor Networks: an overview", *KSII Transactions on Internet and Information Systems*, 6/7, pp. 1735-1755, 2012.
27. C. Li, H. Zhang, B. Hao, and J. Li, "A survey on routing protocols for large-scale wireless sensor networks.,," *Sensors (Basel)*, vol. 11, pp. 3498–526, 2011.
28. M. Ahmadiania, M. R. Meybodi, M. Esnaashari, H. AlinejadRokny," Energy-efficient and multi-stage clustering algorithm in wireless sensor networks using cellular learning automata", *IETE Journal of Research*, vol.59,pp. 774-782 , 2014.
29. D. Kumar, "Performance analysis of energy efficient clustering protocols for maximising lifetime of wireless sensor networks," *IET Wirel. Sens. Syst.*, pp. 9–16, 2013.

Slow Wave-IDC Loaded High Bandwidth Microstrip Antenna Operates For Multi Band Applications

Brajlata Chauhan,

*Uttarakhand Technical University, Dehradun
UK India*

Abstract— A slow wave structure as inter-digital capacitor (IDC) is incorporated in micro-strip patch to obtain Miniaturized and high band width antenna specially for WLAN, X & Ku –bands . The antennas are loaded with IDC to slow down the guided wave to increase Gain - Bandwidth product. The simulated antennas offered gain of 6.47dB, directivity of 6.47dB and radiated power of 0.001066 watt(antenna2). This paper presents increased bandwidth to 55.33% by inserting a slot on the above patch offered nominal change in gain of 5.8852 and The loaded slot antenna produce directivity of 7.38832dB and radiated power of 0.0299368 watt (antenna 3) in the range of VSWR is less than 1.5.

Keywords- Slow wave structure; *inter-digital capacitor (IDC); Gain band width product; multi band micro-strip patch antenna; rectangular slot; equivalent circuit.*

I .INTRODUCTION

Microstrip transmission line has disadvantage of low bandwidth and it is a great challenge to improve the gain and bandwidth in microstrip with compact size. As the operating frequency is increased, inductance and capacitance of the resonant circuit must be decreased in order to maintain resonance at the operating frequency. Because the gain and bandwidth product is limited by the resonant circuit, so non resonant periodic circuits or slow –wave structures are designed for producing large gain over wide bandwidth. The directive power of an antenna can be increased by increasing the gain and that is limited by the Gain Bandwidth product. A Compact Inter-digital Capacitor-Inserted Multiband Antenna for Wi-max and WLAN application has been proposed [1].

Sandip Vijay *Dept. of Electronics & communication
Engg. ICFAI Univ. Dehradun UK India*

S C Gupta
*Department of Electronics & communication
Engineering DIT Dehradun UK India*

Miniaturization of slow wave antennas exploiting the slow wave enhancement factor is presented in inverted PIFA structure [2]. Two Elements antenna array using inter-digital capacitor with composite right / left handed transmission line (CRLH-TL) ground plane has been introduced[3].Different types of miniaturization and band width enhancement techniques for micro-strip antenna has been developed in last two decade. Here, A new miniaturized antenna for multi band operation with high band width is proposed in this research paper. This is achieved by using slow wave structure as IDC. An IDC inserted in between the two patches, and provide good impedance matching at the quarter-wavelength mode. In the proposed structure the gain bandwidth product has been increased. An equivalent circuit is prepared and analysis for the designed antenna circuit parameter to calculate the value of IDC capacitance and Pad capacitance. These capacitance values of the IDC fine-tune the slotted rectangular microstrip patch antenna to multi bands.

A triple band antenna has been developed for satellite communication by using synthesized transmission line structure[1-5]. A spiral shaped antenna is fabricated for triple band has been discussed. Furthermore the proportion of the two frequencies can be very much controlled in order to maintain the ratio by slot and IDC. This antenna covers different bands like GPS, ISM, WLAN, Bluetooth, public safety band, X-band etc. Finally, the paper is concluded in conclusion.

II. THEORY OF SLOW WAVE

Slow-wave structures are wave-guides or transmission lines in which the wave travels with a phase velocity equal to or less than a certain pre-designed velocity of wave propagation. The slow wave structures are Folded back line, **Interdigital line** (IDC and Helical line etc. used in microwave frequency range. For slow waves,

$\beta > k_0$ (or $V_p < C$, or $\lambda_g < \lambda_0$) .Slow wave carried by the inhomogeneous transmission line stricture such as surface wave and quasi TEM wave work in their fundamental mode of microstrip transmission line structure . Consider a infinite aperture in xy plane supporting a losses less medium with real phase constant and assume no variation in y direction then the electric field E in $z > 0$ region,

$$E(x, z) = y' e^{-j\beta x} e^{-j\sqrt{k_0^2 + \beta^2} z} \quad (1)$$

Equation 1 shows that ,the plane wave is radiating away from the structure at angle $\sin \theta = \beta/k_0$

for $|\beta| < k_0$ fast wave $\sqrt{k_0^2 + \beta^2}$ is real (1a)

for $|\beta| > k_0$ slow wave $\sqrt{k_0^2 + \beta^2}$ is imaginary (1b)

1b indicate ,evanescent wave in z direction ,no radiation in all real θ .It (for finite & infinite aperture) are conclude that, a uniform cross section slow wave structure have potential to radiate energy for finite aperture and radiation is limited to near end fire or end fire directions [6].To increase the radiation IDC is incorporated in between the two patch.

III ANTENNA STRUCTURE & CONFIGURATION

The dimension of IDC and the dimension & position of the slot in patch 1 are selected in such a way that the current path lengths changes for different modes in a different ratio to obtain the desired frequency ratio of dual-band operation. In present case, the slot ratio is also approximately equal to L/W ratio of rectangular microstrip patch.

Step followed to achieve proposed antenna:

III. 1-Designing And Simulation Of IDC

III. 2-IDC Loaded Antenna

III. 3-IDC Loaded Antenna Without Slot

III. 4-IDC Loaded Proposed Antenna With Slot

III.1-DESIGNING AND SIMULATION OF IDC

Slow Wave Element –IDC and it's schematics shown In figure 1 and proposed IDC loaded structure without slot and with slot shown in figure 3 and 3 respectively. This is printed on 1.51mm thick RT Duriode substrate with relative permittivity of 2.32. The IDC has finger length $L= 4.896$ mm width $W=0.504$ mm and number of finger $N=6$. This finger length provide proper impedance matching for the patch. Simulation results for IDC demonstrates the working frequency range in figure 1.The Inter-Digital Capacitor is a periodic structure that comprises narrow gaps of 0.5mm with 6-finger, it is an

element for producing a capacitor-like, high pass Characteristic using micro-strip lines. Conductors or “Fingers” provide coupling between the input and output ports across the gaps.

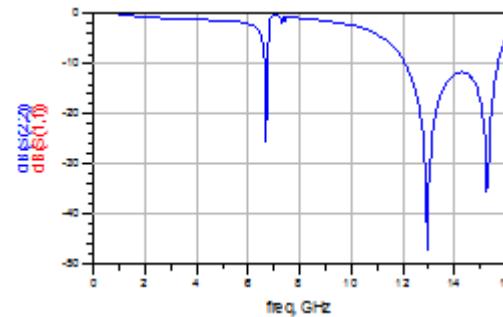
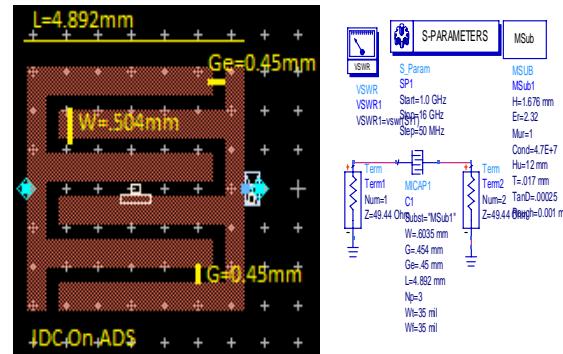


Fig. 1 IDC & It's Schematic with s parameter for Antenna for dual band operation

The capacitance between the strips having thickness t, width W, separation laying on a dielectric with constant K , is given in Pf/Cm

$$C = \frac{0.12t}{w} + .09(1+k)\log_{10}\left(1 + \frac{2w}{s} + \frac{w^2}{s^2}\right) \quad (2)$$

$$C = \frac{0.12t}{w} + .018(1+k)\log_{10}\left(1 + \frac{w}{s}\right) \quad (3)$$

$$C \approx \epsilon_0 \frac{1.25 t}{w} + .87(\epsilon + \epsilon_0)\log_{10}\left(1 + \frac{w}{s}\right) \quad (4)$$

This IDC having 6 fingers, by reducing the width of the fingers reduces the required area, but increases the characteristic impedance of the line and in general lowers the effective capacitance. The formulations to calculate the capacitance of IDC are not accurate because the parasitic effects make the capacitance be frequency dependant. At present, the accuracy to calculate the capacitance value of IDC needs to be improved, especially for the operating frequency beyond C-band.

III. 2-IDC LOADED ANTENNA

Primarily IDC inserted between two patch with $L=9.837$ mm, $W=9.234$ mm, $Z_0=49.44$ ohm impedance

feed line antenna that's offers multiband characteristics with considerable gain of 4.347dB at 12.01GHz. Antenna resonating at 10,12,16 GHz with return losses of -38 dB,-19 dB, -18db respectively, shown in fig. 2.

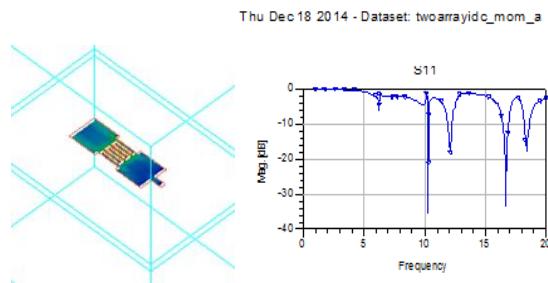


Fig.2 Initial IDC loaded antenna and S_{11} at input

III.3-IDC Loaded Antenna without Slot

In the proposed antenna, Characteristics impedance is adjusted, in such a way so that multiple resonating peak merged into two resonating frequency for WLAN and X band application. Antenna Layout and Simulation results are shown in figure: 4 and 5 respectively. This design offering gain of 6.47dB.

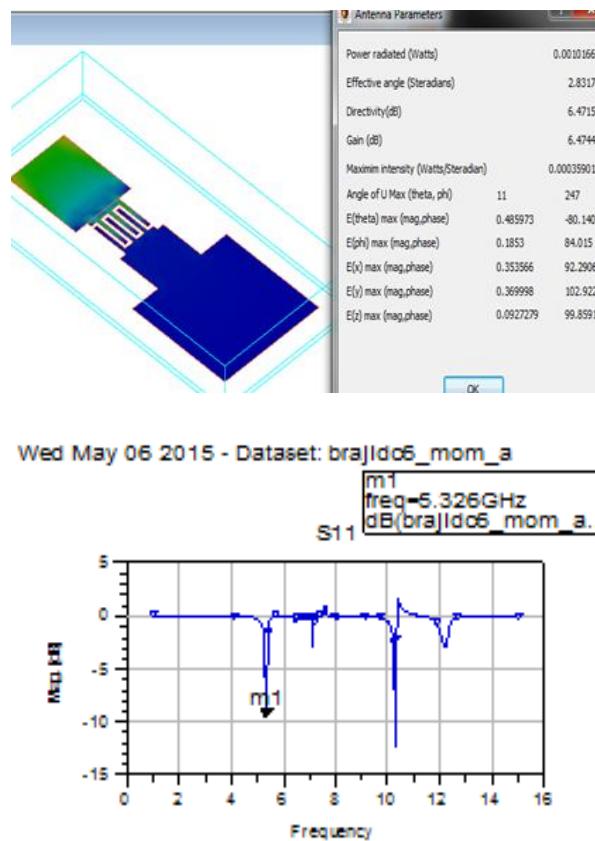


Fig. 3 Antenna without slot and It's parameter

III. 4-IDC Loaded Antenna with Slot

For increasing the bandwidth, a slot has been created on small patch at higher frequencies. The combination of patch and slot gives an additional degree of freedom in designing of a patch antenna. Dimension of the patch-1 are; W=8.12mm and length L=9.314mm dimension of the slot are; W_s=2.012mm and length L_s=5.814mm, The slotted antenna shown in fig. 4&5, resonating lower and higher frequencies at 9.313 and 16.04 GHZ.
 $\% \text{ BW} = f_2 - f_1 / f_0 = (16.04 - 9.313) / 12.88 \text{ GHz} = 52.228\%$

where f₂, f₁ and f₀ are higher, lower and resonance frequencies respectively. Producing -10dB BW =6.57GHz and % bandwidth is 52.228%.

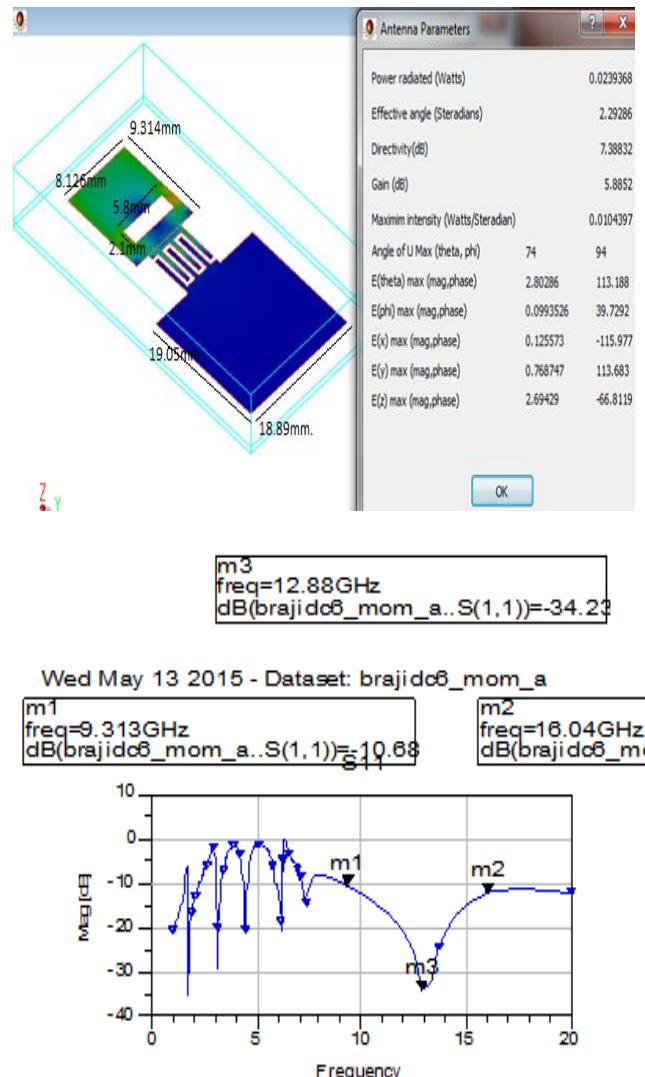


Fig.4 Proposed antenna with slot

VSWR of the proposed antenna lying between 1.12 - 1.54 throughout the resonating frequencies range. The 3-D radiation pattern offers gain of 5.882dB.

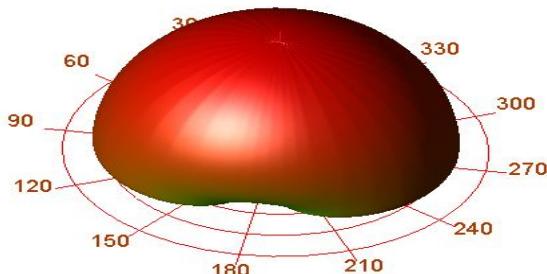


Fig. 5 Radiation pattern

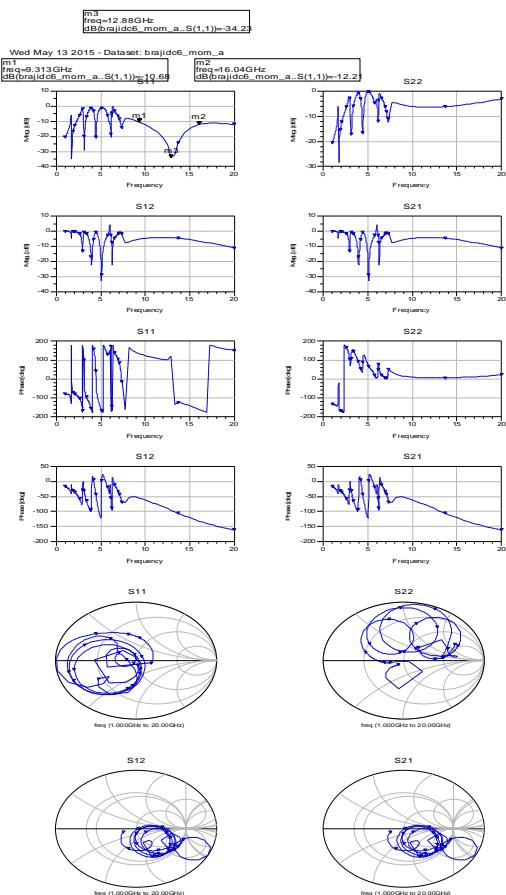


Fig.6. S- parameter and smith chart of the antenna3

IV Equivalent Circuit of the proposed antenna

When the IDC is coupled in the series with RLC circuit of slotted rectangular patch 1 it gets tuned to WLAN and X-band. The equivalent circuit of patch , a slot and IDC elements are shown in given figure. The element are as follows. R_{a1} , L_{a1} , C_{a1} and R_{a2} , L_{a2} , C_{a2} are the Resistance, Inductance and capacitance of rectangular micro-strip patch-1 and patch 2 respectively antenna respectively. R_1 - Radiation resistances of slot respectively X_1 and X_2 :Reactive components of first and second slot Respectively.

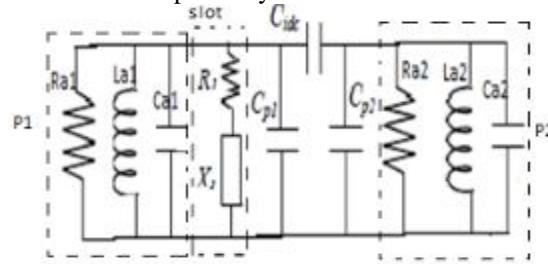


Figure: 7 Equivalent circuit of antenna

The capacitance of IDC (C_{idc}) is calculating the equation given below-

$$C_{idc} = \epsilon_0 \frac{(E+1)}{\pi} [(N - \Delta)L] \quad (5)$$

Where L is the physical length of overlapping width of inter-digital finger. Δ is width correction factor, expressed as $\Delta = 0.5 (W_{eff} - w')$ and W_{eff} is effective corrected transmission line width.

$W' = 2 \times I_L + I_L$ calculated value of C_{idc} is 0.139pf and Pad capacitance C_p can be calculated as:

$$C_p = \left[\frac{2.33 \epsilon_{eff}}{\ln(1 + (1/2) \left(\frac{4k}{w_{eff}} \right) \left(\frac{4k}{w_{eff}} \right) - \sqrt{\left(\frac{4k}{w_{eff}} \right)^2 - \pi^2}} \right] \times \frac{L_1}{25.4 \times 10^{-3}} \quad (6)$$

V. Comparative analysis of the Antennas

S N	Antenna	Freq. F GHz	S ₁₁ dB	Gain G dB	Directi vity D dB	Power Radiated Watt
1	IDC loaded	f1=10.1 f2=12.3 f3=16.5	-38 -19 -18	4.359	4.347	0.008588
2	IDC loaded without slot	f1=5.41 f2=10.2	-9.9 - 12. 8	6.474 5.978	6.471 5 6.401	0.001016 6

3	IDC loaded with slot	f1=4.9	-20	6.173	6.697	0.023936
		f2=5.8	-22	5.885	7.388	8

Table: 1

IVConclusion:

A high bandwidth antenna is presented in this paper with good characteristics of antenna parameter. the interdigital line's resonators are interlaced with each end attached with the two patch resonator .Table 1 presented comparative analysis of IDC loaded antennas and inserted slot antenna .this antenna is useful for GPS, WLAN , and-10 dB wide frequency range operates in 10 to 16 GHz at centre frequency 12.88GHz.The offered bandwidth is **52.228%**. This antenna also offered isolation S₁₂ and S₂₁ greater than -10 dB for low frequencies.

References:

- [1] Jing-Xian Liu, , and Wen-Yan Yin, "A Compact Interdigital Capacitor-Inserted Multiband Antenna for Wireless Communication Applications" . IEEE Antennas And Wireless Propagation Letters, VOL. 9, pp 922-925 , 2010.
- [2] D.-B. Lin and IT Tang "Interdigital capacitor ifa for multiband Operation in the mobile phone" *Progress In Electromagnetics Research C*, Vol. 15, 1{12, 2010.
- [3] Yasser M. Madany , Darwish A. Mohamed, Bishoy I. Halim "Analysis and Design of Microstrip Antenna Array Using Interdigital Capacitor with CRLH-TL Ground Plane for Multiband Applications" (EuCAP 2014) IEEE 978-88-907018-4-9/14 pp 922-926 2014
- [4] Chiu, C. W., C. H. Chang, and Y. J. Chi, "Multiband folded loop antenna for smart phones," *Progress In Electromagnetics Research*, Vol. 102, 213{226, 2010.
- [5] Saeid M. Jaghargh, P Rezaei, and J.S. Meiguni "Effect of Slow Wave Structures on Scan Angles in Microstrip Leaky-wave Antennas PIERS Proceedings, Prague, Czech Republic, July 6{9, 2015
- [6] A.sutinjo Michal Okoniewski, Ronald H. Johnston " Radiation from Fast and Slow Traveling Waves" IEEE Antennas and Propagation Magazine, Vol. 50, No. 4, August 2008
- [7] Tang, I. T., D. B. Lin, and T. H. Lu, "Apply the slow wave to design the compact antenna," *Microwave Journal*, Vol. 51, No. 6, 96{105, 2008.
- [8] Jing-Xian Liu, *Student Member, IEEE*, and Wen-Yan Yin A Compact Interdigital Capacitor-Inserted Multiband Antenna for Wireless Communication

Applications , IEEE Antennas And Wireless Propagation letters, vol. 9, 2010

- [9] Zhou, D., R. A. Abd-Alhameed, C. H. See, and P. S. Excell,|Wideband balanced folded dipole antenna with a dual-arm monopole structure for mobile handsets," *IET Microw. Antennas Propag.*, Vol. 4, No. 2, 240{246, 2010.

- [10] P.-Y. Ke, etal "Characterization Of Compact V-Band Gaas CMRC Filter Using Slow Wave CPW Transmis-Sion Lines Technology" *Progress In Electromagnetics Research B*, Vol. 43, 355{372, 2012

- [11] **R. S. Chen, X. Zhang, K. F. Tsang, and K. N. Yung** "Modeling and design of Interdigital capacitor based on Neural networks and genetic Algorithm" h_t_t_p:///_w_w_w._p_a_p_e_r_.e_d_u_.c_n_

Authors Profile



Brajata Chauhan received her Master Degree in Digital communication from Uttrakhand technical University Dehradun Uttrakhand in 2010, India and also pursuing her PhD on Beam Forming Conformal Antenna from Uttarakhand technical University Dehradun, UK. She is working in Dehradun Institute of Technology, Dehradun as AP in ECE Department. A life member of Institute of Electronics and Telecommunication Engineers (IETE) India and Ex-member of ISTE new Delhi. She is having teaching experience of 10 years in Engineering Institutions and publishes more than 20 papers in national /international journal/conference.



Sandip Vijay received B.Sc. (Engg.) from PIT Patna in 2000 **M.Tech.** ECE in 2005, the member of IEEE(USA), NSBE (USA), IANEG(USA), ISOC (USA),Life Member of ISTE (INDIA) has published over Hundreds research papers in national and international journals/conferences and IEEE proceeding publication in field of Wireless & Digital Communication Network, and supervised more than 40 projects/dissertation of M.Tech. & B.Tech. Students. He finished his **Doctorate** in 2011 from I.I.T. Roorkee in the field of Wireless Computing. He is working as Associate Professor in Department of ECE & AEI at **DIT, University**, an autonomous college ofUTU, **Dehradun** (Uttrakhand).He published more than 100 papers in national /international journal/conference.



S.C. Gupta, Professor Emeritus, received his B.Sc., B.E., M.Tech (I.I.T. Bombay) Ph.D(1971) in Electronics & Communication Engineering. (Canada & U.O.R.Roorkee) IIT Roorkee, having total experience of about 39 years as Prof. & Head Deptt of Electronics & Communication IIT Roorkee , Now he is working in DIT Dehradun as Dean (PG Course) of Electronics and communication department. He received Khosla Award Gold Medal for best Research paper

from Roorkee University (1972, 1981, 1994) Full-Bright scholarship by council of International Exchange of Scholars, United State of America, University of Lowal State, USA. Lifetime Achievement Award For The Year 2011 From Istitution Of Engineers & I S T E India Life member system society India. He has published many book and around 150 research paper and received many awards by different privet /Government organization. Total No. of publication are 170.

An Efficient Anti-noise Fast FCM clustering for Glioblastoma Multiforme Tumor segmentation

B. Srinivasa Rao,

Research Scholar,

ANUCET, Acharya Nagarjuna University,
Guntur-522510, Andhra Pradesh, India.

Dr. E. Sreenivas Reddy,

Professor, ANUCET,

ANUCET, Acharya Nagarjuna University,
Guntur-522510, Andhra Pradesh, India

Abstract-- Image segmentation plays an important role in medical image processing. Magnetic Resonance Imaging (MRI) is primary diagnostic technique to do image segmentation. Clustering is an unsupervised learning method of segmentation. The conventional FCM algorithm is sensitive to noise, suffers from the computation time overhead and is very sensitive to cluster center initialization. In order to overcome this problem, a new method called Anti-Noise Fast Fuzzy C-Means(AN-FFCM) clustering algorithm for segmentation of Glioblastoma Multiforme tumor segmentation is proposed. The proposed algorithm is able to minimize the effects of impulse noise by incorporating noise detection stage to the clustering algorithm during the segmentation process without degrading the fine details of the image. This method also improves the performance of the FCM algorithm by finding the initial cluster centroids based on histogram analysis, reducing the number of iterations for segmentation of noisy images. The advantages of the proposed method are: (1) Minimizes the effect of impulse noise during segmentation, (2) Minimum number of iterations to segment the image. The performance of the proposed method is tested on BRATS data set. Experimental results show that the proposed algorithms are superior in preserving image details and segmentation accuracy while maintaining a low computational complexity.

Index Terms: *Glioblastoma Multiforme(GBM), image segmentation, Histogram, salt-and-pepper noise, Fuzzy c-means, Medical Image processing.*

I.INTRODUCTION

Glioblastoma multiforme (GBM), a World Health Organization (WHO) grade IV astrocytoma, is the most common human brain tumor comprising about 12%–15% of all primary central nervous system (CNS) tumors and accounting for about 50%–60% of all astrocytomas[1]. The type is determined by the cells they arise of, most frequently astrocytomas (astrocytes), oligodendrogiomas (oligodendrocytes) or ependymomas (ependymal) cells. Furthermore, there are mixed forms containing different cell types, such as oligoastrocytomas. With over 60%, astrocytic tumors are the most common tumors. The grading system for astrocytomas according to the World Health Organization (WHO) subdivides grades I-IV, whereas grade I tumors tend to be least aggressive [2].The highly malignant grade IV tumor is given the name glioblastoma multiforme (GBM). It is the most frequent glioma with approximately 50%,

followed by astrocytomas WHO I-III with 25%. Oligodendrogiomas and Ependymomas are less frequent with 18% and 2-9%, respectively. Survival for patients with glioblastoma, although individually variable, averages 14 months after diagnosis[3]. Clinical trials are investigating effective treatments for GBM brain tumors, and imaging is playing an important role.

Clustering is an unsupervised classification of patterns into groups of similar objects; widely used in medical diagnostic studies. Bezdek first proposed the fuzzy c-means (FCM) algorithm in 1981 [4]. Since then it has become a popular clustering method which divides data into different groups according to their degree of attribution. Data may partially belong to more than one group, represented by a fuzzy membership value of between 0 and 1. During image analysis, each pixel is classified according to their attributes: a membership value of 1 means that a pixel contains only one specific tissue class; whereas a membership value of 0 means that a pixel does not contain that tissue class. Since the unsupervised FCM does not require training data researchers have widely used this method in the segmentation of MR images [5,6].

the FCM algorithm comes with good accuracy in the absence of noise, it is sensitive to noise and other imaging artifacts. Therefore, enhancements have been tried to improve its performance by including local spatial and grayscale information. Ahmed et al. [7] modified the objective function by adding a term for the spatial information of neighboring pixels but the main drawback of this algorithm is computationally expensive as the local neighborhood term has to be calculated in each iteration step. To overcome this drawback, Chen and Zhang [8] calculated grayscale of a filtered image in advance, and used kernel function to replace the Euclidean distance. Although the accuracy has been improved, it is sensitive to high level noises and different types of noises. This work is divided into four sections. First, section 2 gives FCM algorithm,. Then, in section 3, Fast FCM. Subsequently the proposed Anti Noise Fast FCM is introduced in section 4 and Experimental results in section 5. Finally, the paper conclusions are summarized in section 6.

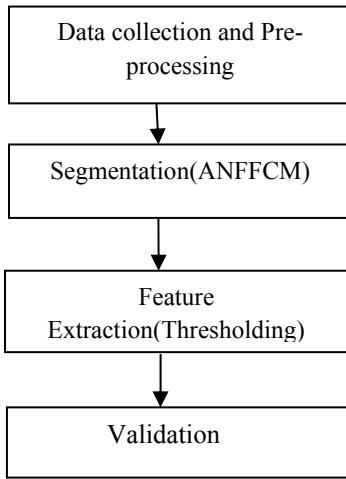
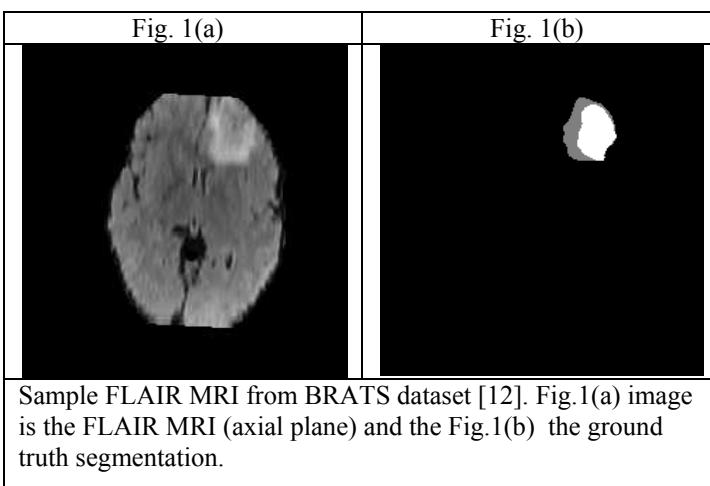


Fig.2 Block diagram of the proposed method

II. Fuzzy C-Means(FCM)

The Fuzzy c-means [9] is an unsupervised clustering algorithm. The main idea of introducing fuzzy concept in the Fuzzy C-Means algorithm is that an object can belong simultaneously to more than one class and does so by varying degrees called memberships. It distributes the membership values in a normalized fashion. It does not require prior knowledge about the data to be segmented. It can be used with any number of features and number of classes. The fuzzy C-means is an iterative method which tries to separate the set of data into a number of compact clusters. The Fuzzy C-means algorithm is summarized as follows:

Algorithm Fuzzy C-Means(x,n,c,m)

Input:

n = number of pixels to be clustered;

$x = \{x_1, x_2, \dots, x_n\}$: pixels of real time image;

c= number of clusters

m=2: the fuzziness parameter;

Output:

u: membership values of pixels and segmented Image

Begin

Step_1: Initialize the membership matrix u_{ij} is a value in (0,1) and the fuzziness parameter m (m=2). The sum of all membership values of a pixel belonging to clusters should satisfy the constraint expressed in the following.

$$\sum_{j=1}^c u_{ij} = 1 \quad (1)$$

for all $i = 1, 2, \dots, n$, where c (=2) is the number of clusters and n is the number of pixels in the image.

Step_2: Compute the centroid values for each cluster c_j . Each pixel should have a degree of membership to those designated clusters. So the goal is to find the membership values of pixels belonging to each cluster. The algorithm is an iterative optimization that minimizes the cost function defined as follows:

$$F = \sum_{j=1}^N \sum_{i=1}^c u_{ij}^m \|x_j - c_i\|^2 \quad (2)$$

where u_{ij} represents the membership of pixel x_j in the i^{th} cluster and m is the fuzziness parameter.

Step_3: Compute the updated membership values u_{ij} belonging to clusters for each pixel and cluster centroids according to the given formula. If x_j is noisy pixel get the pixel from R(i,j)

$$u_{ij} = \frac{1}{\sum_{k=1}^c \left(\frac{\|x_j - v_k\|}{\|x_j - v_i\|} \right)^{2/(m-1)}}, \quad (3)$$

and

$$v_i = \frac{\sum_{j=1}^N u_{ij}^m x_j}{\sum_{j=1}^N u_{ij}^m}$$

Step_4: Repeat steps 2-3 until the cost function is minimized.
End.

III. Fast Fuzzy C-Means

Algorithm Fast Fuzzy C-Means(x,n,c,m)

Input:

N=number of pixels to be clustered;

$x = \{x_1, x_2, \dots, x_n\}$: pixels of real time image;

c= number of clusters;

Output:

u: membership values of pixels and segmented Image

Begin

Step_1: Find the histogram of the image.

Step_2: Based on the number of clusters divide the histogram bins into l/c parts where l is the maximum gray value and c is the number of clusters.(e.g: for 3 clusters 1-85,86-170,171-256).

Step_3: Consider the highest peak intensity value from each part (excluding noise pixels), get the pixels with these intensity values initialize these values as initial centroids.

Step_4: Start FCM algorithm with these initialized centriods

End

IV. THE PROPOSED ANTI NOISE FAST FCM CLUSTERING TECHNIQUE

We propose a new method of clustering based segmentation technique, specifically for images corrupted with impulse noise. The technique known as anti noise clustering is introduced to overcome the problem of noise sensitivity in the segmentation process which increases the robustness of the segmentation process with respect to noise. This proposed method is a two stage process, in the first stage the detection of salt-and pepper noise and its locations .The second stage will perform the actual clustering process. The ‘noise-free’ pixels will be totally considered as the input data and they will give full contribution on the clustering process. Otherwise, for the ‘noise’ pixels, the fuzzy concept is applied to determine the degree of contributions of these ‘noise’ pixels on the clustering process. The combination of noise detection, cancellation and the clustering allows more versatile and powerful methods to achieve a better segmentation especially on noisy images.

A. Salt-and-pepper noise detection and noise cancellation:

For a gray scale digital image the intensity is stored in an 8-bit integer, giving a possible 256 gray levels in the interval[0,255]. The salt-and-pepper noise takes on the minimum and maximum intensities. It can be either minimum intensity value near 0 i.e. L_{lower} (appears black i.e pepper) or maximum intensity value near i.e 255 L_{upper} (appears white i.e salt).The histogram of the image is used to identify these two types of noise intensities. If an image corrupted with salt-and-pepper noise would peak at the ends of the noisy image histogram[10]. These two salt-and-pepper noise intensities will be used to identify possible ‘noise-pixels’ in the image. According to [11], a binary noise mask $Q(i,j)$ will be created to mark the location of ‘noise-pixels’ by using;

$$Q(i,j) = \begin{cases} 0, & X(i,j) = L_{Upper} \text{ or } L_{Lower} \\ 1, & \text{Otherwise} \end{cases} \quad (4)$$

Where $X(i,j)$ is the pixel at the location (i,j) with intensity X , $Q(i,j)=1$ represents the ‘noise-free’ pixel to be retained in the next clustering stage while $Q(i,j)=0$ represents ‘noise’ pixels.

B. Noise cancellation and clustering :

After the binary mask $M(i,j)$ is created, in order to allow more versatile methods of clustering- based segmentation in noisy images all “noise pixels” marked with will be replace by an estimated correction term

$$X^1(i,j) = (1 - F(i,j)) X(i,j) + F(i,j) M(i,j) \quad (5)$$

where $M(i,j)$ is the median of in the 3×3 window given by:

$$M(i,j) = \text{median}\{ X(i+k,j+l) \text{ with } k,l \in (-1,0,1) \} \quad (6)$$

After the median pixel is found, the absolute luminance difference, $d(i,j)$, is computed by using;

$$d(i+k,j+l) = \{X(i+k,j+l)-X(i,j) \text{ with } (i+k,j+l) \neq (i,j)\} \quad (7)$$

Then the local information of the ‘noise’ pixels in 3×3 window is calculated by taking the maximum value of the absolute luminance difference given by;

$$D(i,j) = \max\{ d(i+k,j+l) \} \quad (8)$$

According to [11], “noise pixels” will be set to the maximum intensity 255 while “noise-free pixels” will assume other values in the dynamic range. Based on this the choice of using maximum operator rather than the minimum operator is justified in [11]. Next the fuzzy reasoning is applied to the extracted local information $D(i,j)$. The fuzzy set defined by the fuzzy membership function $F(i,j)$ is defined by;

$$F(i,j) = \begin{cases} 0 & ; D(i,j) < T1 \\ D(i,j) - T1/T2-T1; T1 < D(i,j) < T2 \\ 1 & ; D(i,j) \geq T2 \end{cases} \quad (9)$$

whereby for optimal performance, the threshold value $T1$ and $T2$ are set to 10 and 30 respectively as described in [11]. Then the corrected value of noise pixel is calculated using (5).

To improve the efficaciousness of the FFCM clustering towards noise, these corrected values (i.e., for the noise pixels) are used to replace original pixels values during the process of assigning the data to their nearest centre. Then the new position for each cluster is calculated using (2). The term x_j in (2) is substituted by:

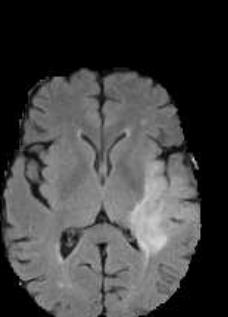
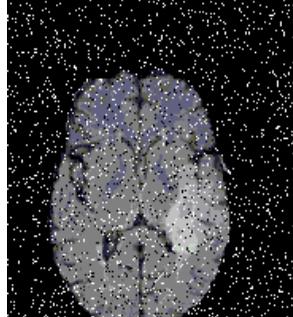
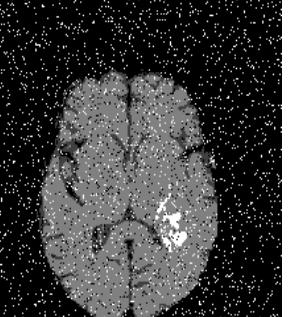
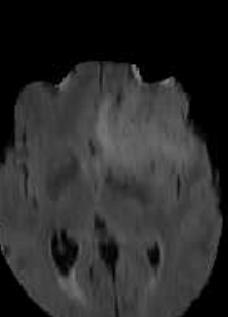
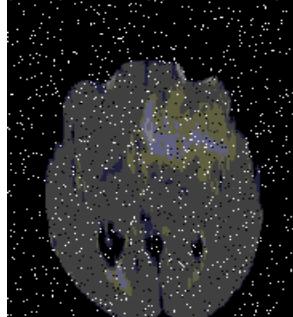
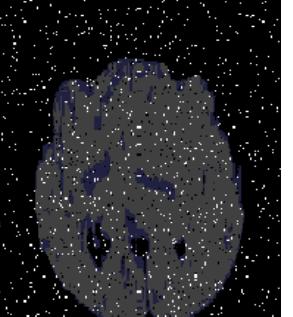
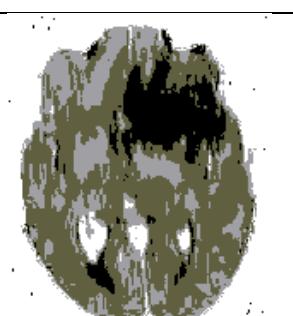
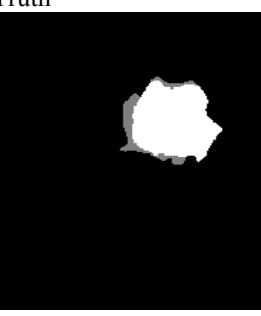
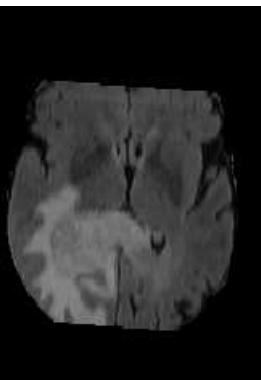
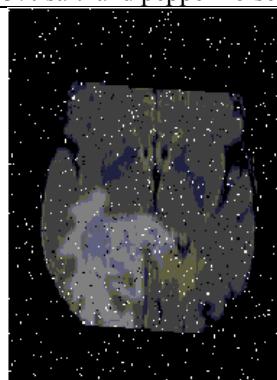
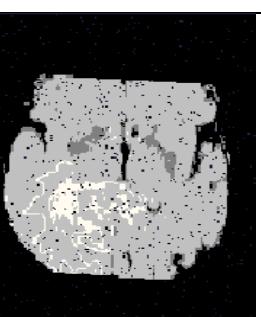
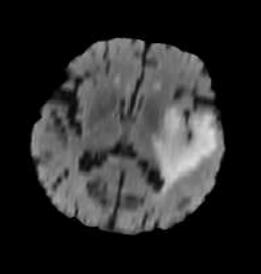
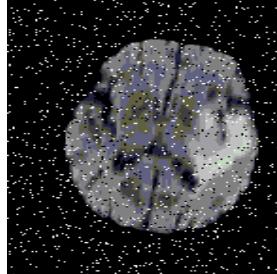
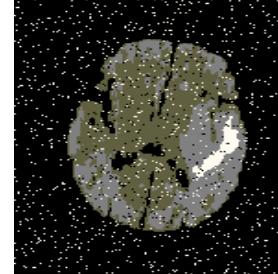
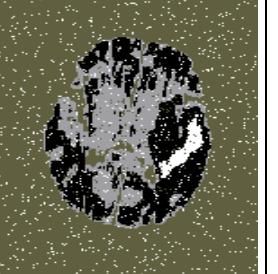
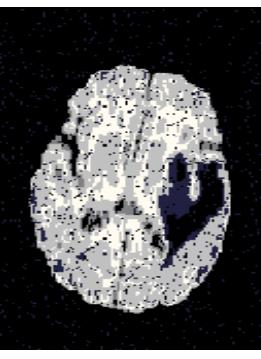
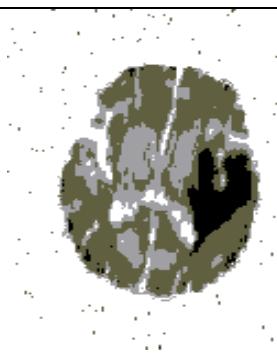
Fig 3.(a) Original Image	Fig.3(b) Original image with 10% salt and pepper noise	Fig.3(c) K-Means	Fig.3(d) FCM
			
Fig 3.(e) MFCM	Fig 3.(f) Proposed Method	Fig.3(g)Extracted Feature (Thresholding on Fib.3(f))	Fig.3.(h)Ground Truth
			
Fig 4.(a) Original Image	Fig. 4(b) Original image with 5% salt and pepper noise	Fig.4(c) K-Means	Fig.4(d) FCM
			
Fig 4.(e) MFCM	Fig 4.(f) Proposed Method	Fig.4.(g) Extracted Feature (Thresholding on Fib.4(f))	Fig.4.(h)Ground Truth
			

Fig 5.(a) Original Image	Fig.5(b) Original image with 3% salt and pepper noise	Fig.5(c) K-Means	Fig.5(d) FCM
			
Fig 5.(e) MFCM	Fig.5(f) Proposed Method	Fig.5.(g) Extracted Feature (Thresholding on Fib.5(f))	Fig.5.(h)Ground Truth
			
Fig.6(a) Original Image	Fig.6(b) Original image with 7% salt and pepper noise	Fig.6(c) K-Means	Fig.6(d) FCM
			
Fig.6(e) MFCM	Fig.6(f) Proposed Method	Fig.6(g) Extracted Feature (Thresholding on Fib.6(f))	Fig.6(h)Ground Truth
			

$$x_j = \begin{cases} X(i,j) & \text{if } Q(i,j) = 1 \\ X^l(i,j) & \text{if } Q(i,j) = 0 \end{cases} \quad (10)$$

By the end of this stage we get a image $R(i,j)$ which is noise free image, if x_j is noise free then the value of x_j will be Original image pixel value(i.e $X(i,j)$) otherwise consider the pixel from $R(i,j)$. Integrating this method in the fast FCM clustering algorithm, the new proposed algorithm is called anti-noise fast fuzzy C-Means clustering(AN-FFCM).

V EXPERIMENTAL RESULTS

In this section , The performance of the AN-FFCM is compared with K-means[13], conventional FCM[9], MFCM[7]. We present the experimental results on The Brain Tumor Image Segmentation (BRATS) Benchmark dataset [12] is used. In this experiment , we have used images corrupted with the salt-and-pepper noise to test the effectiveness and the efficiency of the proposed AN-FFCM. The BRATS dataset is publicly available through the annual Medical Image Computing and Computer Assisted Intervention (MICCAI) Society brain tumor segmentation challenge [12]. The dataset consists of 30 fully anonymized multi-contrast MR scans of glioma patients along with expert annotations, i.e., ground truth manual segmentations. We use 22 images of the FLAIR MRI (axial plane) modality. Fig.3(a),Fig.4(a),Fig.5(a),and Fig.6(a) are ds1,ds2,ds3 and ds4 respectively. The experiments were performed in a 2.99 GHz Intel Core 2 Duo processor, Windows XP with 3.21 GB RAM, using Matlab R2012a.

Segmentation results on BRATS data set are shown in Fig. 3. The noise removal performances are compared on the accuracy of the algorithms K-Means(Fig.3(c)), FCM(Fig.3(d)), MFCM(Fig.3(e)), From these results it is obvious that K-Means and FCM are very sensitive to the noise, while the result and efficiency of MFCM are not satisfied. Though MFCM provide better segmentation there exist obvious misclassification Pixels. Visually, the proposed method achieves the better result, over K-Means, FCM, MFCM. Similarly Fig.4, Fig.5 and Fig.6 achieves betters results.

A.Quantitative results:

In order to compare objectively the different algorithms, the optimal segmentation accuracy (SA) is used. SA is defined as the sum of the correctly classified pixels divided by the sum of the total number of pixels of the test image

$$SA = \frac{\sum_{i=1}^c \text{card}(A_i \cap C_i)}{\sum_{j=1}^c \text{card}(C_j)} \quad (11)$$

where c is the number of clusters, A_i is the set of pixels belonging to the i th cluster found by the algorithm, C_i is the set of the i th cluster in the ground truth segmented image.

B. Segmentation Accuracy: The differences in JS between the proposed algorithms and the other 3 algorithms are clear for the axial slice with noise 10%,7%,5% and 3% which are better than the other 3 algorithms which are shown in table.1.

C. Computational Cost: In terms of computational cost, the objective function of FCM algorithm in its original form [5] contains only the difference between the grayscale of the current pixel i and the cluster centers V_j . This is basically to cluster grayscales as there is no spatial information, so it less computational cost. The enhancement of original FCM, [6] modified the objective function by adding a term for the spatial information of neighboring pixels. The MFCM algorithm is computationally expensive as the local neighborhood term has to be calculated in each iteration step. The proposed algorithms having the lowest computational cost 19,14,10 and 21iterations for ds1,ds2,ds3 and ds4 respectively.

D. Neighborhood Size. The local neighborhood window size is a crucial factor to determine the smoothness of clustering and details to be preserved. We have experimented with different window sizes and found that a window size of 3×3 pixels achieves the best balance between segmentation accuracy and computational cost. Increasing window size to 5×5 pixels has very small impact on the JS but 7×7 pixels or more will, significantly, decrease the accuracy.

CONCLUSION

FCM is a popular clustering method and has been widely applied for medical image segmentation. Although many researchers have developed various extended algorithms based on FCM, none of them is flawless. MRI is the most effectively image model used for diagnostic image examination for brain tumor. On the other hand, K-mean algorithm can detect a brain tumor faster than Fuzzy C-means, but Fuzzy C-means can predict tumor cells accurately. Original Fuzzy C-means algorithm fails to segment image corrupted by noise, outliers, and other imaging artifacts. Therefore a new algorithm named anti-noise fast Fuzzy-C-Means clustering algorithm is proposed for GBM tumor segmentation, especially for images corrupted with salt-and-pepper noise. The proposed algorithm produces results faster than the conventional FCM with the novel initialization method based on histogram analysis to start the FCM clustering for segmentation of an image. Our framework

consists of four stages: pre-processing, Segmentation, Feature extraction, and validation stages. From the experimental results, we proved the effectiveness of our approach in GBM tumor segmentation by comparing it with three state of-the-art algorithms: K-means, Fuzzy C-means and MFCM. Our proposed system determines the initial cluster k value to minimize the execution time. The performance of the proposed technique, its minimization time strategy, and its quality has been demonstrated experimentally. We tested this on Brain Tumor Image Segmentation (BRATS) Benchmark dataset, the results shows that the processing time is reduced to segment the image. It also produces better results through its inclusion of the noise detection and cancellation stage in its clustering process. This stage reduces the effect of noise during the segmentation process. Furthermore, this finding suggests the AN-FFCM clustering as a novel method for the segmentation GBM tumors from MR images.

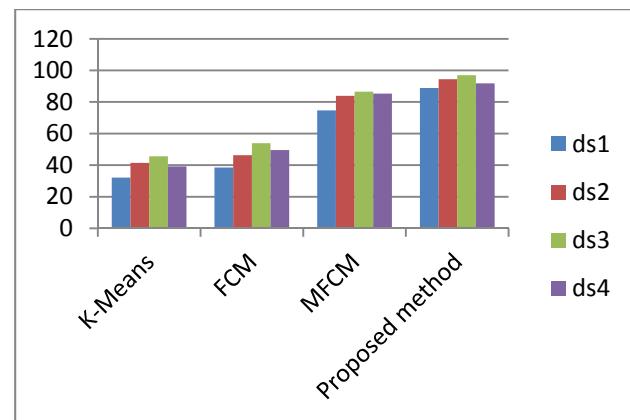
Table.1 Average segmentation accuracy (SA%) of the four algorithms according to the level and the percentage of noise for four clusters.

	K-Means	FCM	MFCM	Proposed method
ds1	32.17	38.47	74.66	88.82
ds2	41.40	46.34	83.91	94.39
ds3	45.61	53.86	86.49	96.93
ds4	39.24	49.52	85.27	91.77

Table :2 Comparison in number of iterations

	FCM	MFCM	Proposed method
ds1	35	41	19
ds2	31	40	14
ds3	19	28	10
ds4	37	45	21

Table. 3: The quantitative evaluation (JS) for K-Means, FCM, MFCM and the proposed method.



REFERENCES:

- [1] D. Lipsitz, R. J. Higgins, G. D. Kortz, P. J. Dickinson, A. W. Bollen, D. K. Naydan, and R. A. Lecouteur, "Glioblastoma multiforme: Clinical findings, magnetic resonance imaging, and pathology in five dogs," *Vet.Pathol.* **40**, 659–669 (2003).
- [2] P. Kleihues, D. N. Louis, B. W. Scheithauer, L. B. Rorke, G. Reifenberger, P. C. Burger, and W. K. Cavenee, The WHO classification of tumors of the nervous system, *Journal of Neuropathology & Experimental Neurology*; 61(3): 215-229; discussion 226-9, 2002.
- [3] E. G. Van Meir, C. G. Hadjipanayis, A. D. Norden, H. K. Shu, P. Y. Wen, and J. J. Olson, "Exciting new advances in neuro-oncology: The avenue to a cure for malignant glioma," *Ca-Cancer J. Clin.* **60**(3), 166–193 (2010).
- [4] Bezdek JC, Hall LO, Clarke LP: Review of MR image segmentation techniques using pattern recognition. *Med Phys* 1993, 20:1033-48.
- [5] Kobashi S, Hata Y, Kitamura YT, Hayakata T, Yanagida T: Brain State Recognition Using Fuzzy C-Means (FCM) Clustering with Near Infrared Spectroscopy (NIRS). In *Fuzzy Days 2001 LNCS 2206*. Edited by: Reusch B. Berlin Heidelberg: Springer-Verlag; 2001:124-136.
- [6] Kannan SR, Sathy A, Ramathilagam S, Pandiyarajan R: New Robust Fuzzy C-Means Based Gaussian Function in Classifying Brain Tissue Regions. In *Contemporary Computing, Communications in Computer and Information Science*. Volume 40. Edited by: Ranka S et al. Berlin Heidelberg: Springer; 2009:158-169.
- [7] M. N. Ahmed, S. M. Yamany, N. Mohamed, A. A. Farag, and T. Moriarty, "A modified fuzzy c-means algorithm for bias field estimation and segmentation of MRI data," *IEEE Transactions on Medical Imaging*, vol. 21, no. 3, pp. 193–199, 2002.

- [8] S. Chen and D. Zhang, "Robust image segmentation using FCM with spatial constraints based on new kernel-induced distance measure," *IEEE Transactions on Systems, Man, and Cybernetics Part B: Cybernetics*, vol. 34, no. 4, pp. 1907–1916, 2004.
- [9] LJun-Hao Zhang, Ming Hu HA , Jing Wu," Implementation of Rough Fuzzy K-means Clustering Algorithm in Matlab", Proceedings of Ninth International Conference on Machine Learning and Cybernetics", July 2010.
- [10] W. Luo, "Efficient removal of impulse noise from digital images," *IEEE Trans. Consumer Electron.*, vol. 52, no. 2, pp. 523-527, May 2006.
- [11] K. K. V.Toh. and N. A. Mat-Isa, "Noise Adaptive Fuzzy Switching Median Filter for Salt-and-Pepper Noise Reduction," *IEEE Signal Processing Letters*, vol.17, no.3, pp 281-284, 2010.
- [12] B. Menze, A. Jakab, S. Bauer, J. Kalpathy-Cramer, K. Farahani, and et al., "The multimodal brain tumor image segmentation benchmark (BRATS)," *IEEE Trans. on Medical Imaging*, 2014.
- [13] Bandhyopadhyay SK, Paul TU. Automatic segmentation of brain tumour from multiple images of brain MRI. *Int J Appl Innovat Eng Manage (IJAIEM)* 2013;2(1):240–8.

Ear Classifying in Profile Images Based on Curves and Shape

Mohammad Mahmoudi

Department of Computer Science and Engineering
Khoy branch, Islamic Azad University
Khoy, Iran

Ali Habiboghi

Department of Computer Science and Engineering
Khoy branch, Islamic Azad University
Khoy, Iran

Abstract—In this research we are going to classify ears based on their appearance. For this aim, region of ear in profile image should be extracted. Then by using margins surrounding around the ear and the center of ear would be obtained by the proposed method. Finally by determining appropriate threshold the ears were classified based on their shapes. The database used in this article is CVL. Simulating and classifying of this article have acceptable accuracy 83.6%.

Keywords--Classification, Ear Recognition; Image Processing; Profile Images

I. INTRODUCTION

Traditionally, there were different methods for licensing and accessing, which in general, they could be classified into traditional and biometric methods. Traditional methods included watchword, ID, Password, biometric methods included finger print, retina, vein pattern, audio patterns, signature, typing, and face patterns. For example the ways of walking and signing belonged to behavioral type while finger print, face and ear biometric belong to physiological group [11].

The traditional methods due to their disadvantages and limitations lead to biometric identification method and develop more rapidly. Among biometric features, physiological group methods due to the high reliability which is one of the most important principles in the field of access, attracted more attention. Ear biometric due to its special privileges first, ear is one of the most resistant and stable characteristic of human anatomy that doesn't change significantly during the life. While in contrast, human faces by getting older make significant changes. Also the shape of human face changes for makeup reasons, facial hair and human hair style, while ear is excluded from such changes. Second, biometric characteristics such as human face in emotional situations, joy, fear, surprise and concern show different modes. In contrast the characteristic of ear is unchangeable. Moreover ear is one of our body sensors which we hear sounds through it. Ear images can be achieved even over long distances without getting noticed. High attention to biometric characteristic can be found out by studying numerous books and articles.

Several research groups utilized different ways to select and extract ear biometric characteristics. Chen and Bhanu offered three different approaches to diagnose ear. In one of these approaches, classified section was used, which showed special distribution of index form. This method only worked on certain images and was sensitive to any scale, rotation and diversification. In their next strategy they took steps to identify an area of the ear image. Ear related areas with large curved edges were diagnosed with edge detection technique, then a template which contained a variety of external and anti – helix was divided into clusters of line[5]. In a study which was carried out to diagnosis ear, the contour lines of ear were used. The outer contour of ear is obtained by searching the longest continuous edge of image. By selecting the top, bottom and detected left edge, triangle with selected points was formed [6]. Another example for the diagnosis of ear, by using ear contour lines have been described, they were positioning the outer contour of ear by searching the longest edge of the image. By selecting the top, bottom and left side of the detected boundary a triangle with selected points was formed [7].

Yuan and Mu presented a method for real time application for detecting ear. In their method constant comparative mean shift was used [8]. CAMSHIFT algorithm often used in face tracking applied programs, based on matching region and skin color model.

Other studies were being done on ear biometrics as well, various tasks have been done, including ear image conversion to the force field and feature extraction from it, extraction of geometric relationships. Extraction of vector feature from ear contour by using oval model, data extraction by using log-Gabor wavelet, the adjacent graph model composed of Voronoi diagrams, the curved shapes of the ear, 3D dimensional form of ear, artificial neural networks (ANN), and the rules of the nearest neighborhood, extraction of features with the help of SHIFT operator, by combining them and creating a component model [9].

Bhanu and Chen by using twenty 3D images, collected from 10 persons, reached the best. In another study of 3D images 28 out of 30 samples got to the desired results. In this study ICP algorithm was used and ear images manually separated from other parts of the ear [10].

Methodology and proposed algorithm

Our aim in this study is determining the location of ear in profile image. Based on Ali Habiboghi et al [4], we are going to classify them on the basis of threshold value for each of the three directions specified in all ears. In next the section, we present proposed algorithm with details. In section three our proposed algorithm compared with other ways. Finally we present conclusion of paper.

II. PROPOSED METHOD

Before describing the different parts it is necessary to explain that in this study we discuss to categorize images in three groups based on the shape of the ear. In other words primarily based on the appearance of the ear, classify them into three groups then we apply our algorithm on images, that our algorithm offered classification of ears with an accuracy of 83 percent. The database used in this article is CVL [3].

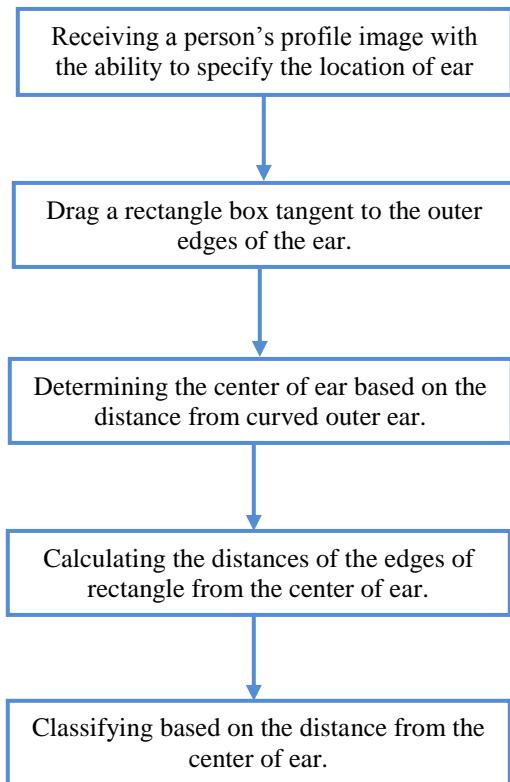


Figure 1. Details of the proposed algorithm

A. Receiving a person's profile picture with the ability to specify the location of ear

In Ali Habiboghi et al [4], the location of ear diagnosed with an accuracy of 91 percent. We continue to work on this article. In the following we outline the proposed methodology.

B. Drag a rectangle box tangent to the outer edges of the ear

Rectangular box drawn on ears was based on the maximum amount of the edge of the ear on all four sides, up, down, left, right. In other words, we did this based on the edges of ear, by using Sobel's edge detection algorithm as follows:

The edges of image are pixels of image, where the difference in intensity of pixels is high compared with neighboring pixels. To find the edges of image from image in the direction of x and y we make derivation. Then we compute the gradients of image at any point of image, and pixels of image that their gradient value is larger than threshold considered as an edge of image.

To calculate the derivative of the first order, high pass filters have been designed, in the meantime, Prewitt, Sobel, Freichen filters are more important. Each of the aforementioned filters consists of two different masks that one of the masks derived in the X direction and another mask derived in the Y direction calculate any point of the image. The remarkable point is that mask derived in the X direction transpose mask derived in the Y direction. The edges are high frequency of image, while flat areas are low frequency of image. One of the strategies to improve the edges, is using the filters which emphasize high frequencies, hold low frequency components, but reinforce high frequency components.

The edges of an image show the structure of its objects. Edge detection is an important preprocessing stage to detect and identify objects. Because edges are high frequency components of an image. Edge detection is usually done by using high frequency filters that absorb low frequency components. Then a threshold is applied. An edge detection is Sobel operator, which consists of two filters

$$H_x = \begin{bmatrix} 1 & 0 & -1 \\ 2 & 0 & -2 \\ 1 & 0 & -1 \end{bmatrix}, H_y = \begin{bmatrix} 1 & 2 & 1 \\ 0 & 0 & 0 \\ -1 & -2 & -1 \end{bmatrix}$$

High filters are two high-pass filters in horizontal and vertical directions. For detecting an image these two filters on one image were used, which represents horizontal and vertical edges for each pixel. If you are only interested in detecting horizontal edge, compare horizontal edge with threshold, and consider those pixels as edge. If you are interested edges in all directions, calculate the size of gradient with $g_m = \sqrt{g_x^2 + g_y^2}$ consider pixel as edge which $g_m > T$

C. Determining the center of ear based on the distance from curved outer ear

After determining the edges of ear with a specified distance to the edges, draw a box around the ear and consider its center as center of the ear, then according to this center the distance is calculated from three directions.

To find the exact location of the ear, surround it in a box, then we attempt to identify the center of ear by using a function that was implemented in MATLAB to this purpose, first the

area of ear is calculated, then by calculating the average X and Y coordinate act according the following formula to calculate the center of ear precisely.

```
area = sum(sum(im));
meanx = sum(sum(double(im).*x))/area;
meany = sum(sum(double(im).*y))/area;
```

This calculation is done for all the database images. The three distances calculated for each database image. Then we calculate the average of all three distances. In fact by this strategy we create some threshold for classifying ears based on their sizes.

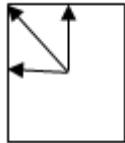


Figure 2. three considered distances for classifying

An example of received images in our proposed methodology was shown below.

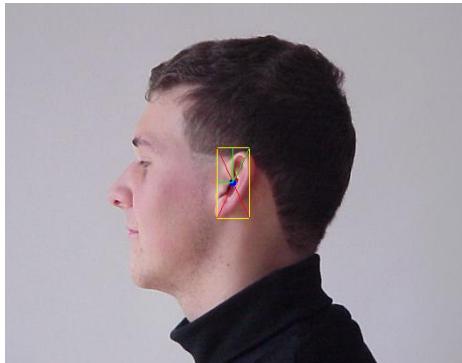


Figure 3. determining the center of ear and calculating the distance of edges from the center of ear in three directions.

D. Calculating the distance of rectangular edges from the center of ear

In the proposed method a box was used to surround diagnosed ear, and a method was proposed for classifying ears based on calculation of the distance from the center to the sides of the box.

For classifying ears three points were considered, these three points have potential to cover rectangular, square, long diagonal forms of ear. So these three distances were considered for all ears. As mentioned above, the average distance to all ears as a threshold criteria for classifying ears, was considered. After calculating every three distances for 90 ear samples, we got their average. So we have three criteria which these three criteria will be used in categories.

E. Classifying based on the distance from the center of ear

Since there are three ear types in our database and practically they have been classified in three categories, the purpose of our proposed method is reaching to the categories which are as close as much as possible to the real category.

TABLE I. CLASSIFYING EAR IMAGES IN DATABASE BASED ON THEIR APPEARANCE.

Ears with small sizes	1,4,5,9,13,17,45,46,49,50,53,54,57, 60,66,70,71,76,81,82,85,86,90,91	24
Ears with normal sizes	10,16,21,22,28,30,33,41,43,47,51,6 2,63,64,67,68,69,73,77,78,79,80,83, 87	24
Ears with abnormal sizes	2,3,6,7,11,12,14,15,18,19,20,23,24, 25,26,27,29,31,32,34,35,36,37,38,3 9,40,42,44,48,52,55,56,58,59,61,65, 72,74,75,84,88,89	44

As shown in the table, collections of selected images were classified in three categories. These three categories include, small ears, normal ears, and ears that have larger size, in other words their shapes are different from other ears.

In this paper, the proposed methodology and calculation of threshold criteria for classifying in three classes were considered. The output of the proposed method was shown in table 2. Total number of selected ears for each class along with the number of correct and wrong choices was shown in the table. Finally to calculate the accuracy of classification based on the proposed method, confusion matrix was used. According to the findings the classification accuracy was equal to 83.6 percent.

TABLE II. CLASSIFYING EARS BASED ON PROPOSED METHOD.

	Ear Label	Choice Number	True Choice	Wrong Choice
Ears with small sizes	1,4,5,9,13,17,25,45,4 6,48,50,53,57,59,60,6 6,69,70,71,76,77,81,8 2,85,86,90,91	28	24	4
Ears with normal sizes	10,16,30,33,41,43,47, 51,52,54,62,63,67,68, 73,78,79,83,89	19	16	3
Ears with abnormal sizes	2,3,6,7,8,11,12,14,15, 18,19,20,21,22,23,24, 26,27,28,29,31,32,34, 35,36,37,38,39,40,42, 44,45,46,48,51,56,58,61,64,65, 72,74,75,80,84,87,88, 92	45	37	8

III. COMPARING AND DISCUSSION

In one of the most prestigious researches by Hurly- Nixon which was done on XM2VT database, field vectors for extracting features and Template Matching method for classifying ear images were used. In this study 255 ear images,

4 images for each 63 people were used, which the result of 99/2 percent has been achieved in terms of changing the lighting intensity [1]. Yan and Bowyer by using two dimensional and three dimensional images taken from ear and separating ear image from other parts head automatically Active Contour Detection algorithm and also ICP algorithm for extracting features and classifying was used. The result of 97.8% for 415 people was reported [2].

In the study which the same database was used, several methods were utilized to detect and classify.

IV. CONCLUSION

Ear biometric a method of authentication and identification in various application, was considered by researchers. What we did in this study was based on classifying of ears based on their shapes and sizes. Therefore to determine the edges of ears we launched to specify the center of ear. A frame was drawn which covered ear. Then based on the mathematical calculations, distance from the center to edges was obtained in three directions. Finally based on these distances, ears were classified. So that the threshold value obtained from the distance average would be as a measure for determining ear categories, which in this study three categories were considered for ears. So in a nutshell, in this study for different sizes of ears, three classifications were considered, and these classifications were managed with 83.6% accuracy.

It is worth mentioning, the aim of this article was not identification based on ear biometrics, but our aim was determining the center of ear, obtaining the distance from center to edges, obtaining the appropriate threshold value for classifying ears, and finally classifying ears into three different categories based on threshold value. Therefore our proposed method can be used as a prelude to identify based on ear.

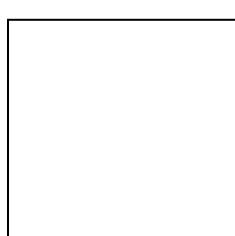
REFERENCES

- [1] Hurley, D. J., Nixon, M. S., & Carter, J. N. (2005). Force field feature extraction for ear biometrics. *Computer Vision and Image Understanding*, 98(3), 491-512.
- [2] Yan, P., & Bowyer, K. W. (2007). Biometric recognition using 3D ear shape. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 29(8), 1297-1308.
- [3] Peer, P. (2015). Cv face database. Computer vision lab., faculty of computer and information science, University of Ljubljana, Slovenia. Available at <http://www.lrv.fri.uni-lj.si/facedb.html>
- [4] Habiboghi , A. & Nabiyev, V., V. (2015). Ear Region Detection in Profile Face Images, Global Journal on Technology [Online]. 08 , pp 67 -73 . Avai l abl e from: <http://awer-center.org/gjt/>

- [5] Chen, H., &Bhanu, B. (2007). Human ear recognition in 3D. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 29(4), 718-737.
- [6] Pflug, A., & Busch, C. (2012). Ear biometrics: a survey of detection, feature extraction and recognition methods. *Biometrics, IET*, 1(2), 114-129.
- [7] Galdámez, P. L., Arrieta, M. A. G., & Ramón, M. R. (2014, January). A Brief Approach to the Ear Recognition Process. In *Distributed Computing and Artificial Intelligence, 11th International Conference* (pp. 469-476). Springer International Publishing.
- [8] Yuan, L., & Mu, Z. C. (2007, August). Ear detection based on skin-color and contour information. In *Machine Learning and Cybernetics, 2007 International Conference on* (Vol. 4, pp. 2213-2217). IEEE.
- [9] Kumar, A., & Zhang, D. (2007, April). Ear authentication using log-gabor wavelets. In *Defense and Security Symposium* (pp. 65390A-65390A). International Society for Optics and Photonics.
- [10] Chen, Y., Pappu, B. P., Zeng, H., Xue, L., Morris, S. W., Lin, X& Wang, D. (2007). B cell lymphoma 10 is essential for FcεR-mediated degranulation and IL-6 production in mast cells. *The Journal of Immunology*, 178(1), 49-57.
- [11] Ramin Dehgani, Ali Habiboghi.(2016,March). An Algorithm for Signature Recognition Based on Image Processing and Neural Networks, *International Journal of Computer Science and Information Security(IJCSIS)*,Vol. 14, No. 3,56-60.



Ali Habiboghi received the B.S. degree from department of engineering of Islamic Azad University, KHOY Branch in 2004. He received the M.S degrees from electronic, computer engineering and information technology from Islamic Azad University of Qazvin Branch, Iran in 2007. From 2007 to already is with the Islamic Azad University of KHOY Branch. His research focuses on artificial intelligence, algorithms, biometric and image processing.



Biometric.

Mohammad Mahmoudi received the B.S. degree from department of engineering of Islamic Azad University Khoy Branch in 2011. He received the M.Sc. degree in computer science from Islamic Azad University, Khoy Branch, Iran in 2016. His research focuses on image processing,

Color Coding Based Detection and Prevention Mechanism for Wormhole Attack in MANET

Harsh Bansal

Assistant Professor

Lovely Professional University

Phagwara, Punjab, India

Gurpreet Singh

Student

Lovely Professional University

Phagwara, Punjab, India

Abstract—MANET is infrastructure-less, lacks centralized monitoring and has dynamic changing network topology. The high usage of MANET demands more security and confidentiality and integrity of the data communicated through network. Security has turned out to be a major concern so as to provide non-endangered communication between mobile nodes in an unfriendly environment of MANET, which poses a number of trivial challenges to security design. The wormhole attack is one of the most threatening and hazardous attacks. In this paper we have classified the well-known countermeasures against wormhole attack in the network according to detection and prevention techniques based on hop counts and delay, protocol modification, trust and reputation. The projected technique to be used for detection of wormhole attack using trust based mechanism, neighbor monitoring concept and credits based mechanism will help to detect and isolate the malicious nodes hence enabling the formation of trusted network.

Keywords— *MANET, Intrusion Detection, Wormhole Attack, Secure Routing, Network Security.*

I. INTRODUCTION

MANET is represented as a wireless network that could be a group of heterogeneous mobile devices and is self-organizing, self-configuring. During this kind of network the devices communicate through a wireless medium with one another. The data packets are transmitted via intermediate devices when there is no direct path from source to target. Mobile ad-hoc network is decentralized and not depend on established infrastructure, such as routers in wired networks [24]. Transfer of packets is completed with the help of routing protocols. The routing protocol is responsible for creating the correct path from supply to destination for initiating as well as maintaining a communication between the nodes. Due to mobility of nodes network topology is dynamic in nature, which result in high link breakage and interruption in communication over the network.

Due to highly dynamic nature of wireless network, routing protocols have to face so many challenges. [22]. Routing protocols in MANETs can be characterized into Proactive, Reactive and Hybrid. Proactive protocols regularly keep the updated topology of the network and are usually table-driven. The Proactive routing protocols contain DSDV, OLSR. Reactive protocols are also recognized as source-originated on-demand protocols, they do not update the routing information periodically[4]. They start route discovery process

only when they are requested to do so, source node wants to find a path to a desired a destination. AODV and DSR are some example of these types of protocols. Lastly hybrid protocols, they utilize the functionality of both the protocols i.e., reactive and proactive approaches. Zone Routing Protocol falls under hybrid type. The MANET is more prone to security threats due to high mobility of nodes, self-organizing and distributed nature as compare to hardwired physical landline networks.

MANETs are easily attacked by attacker internally or externally [25]. As proactive and hybrid protocols are table driven, reactive protocols specially AODV among other reactive protocols is more prone to black hole, wormhole and Denial of Service attacks because of its weaker design. In wormhole attack the malicious node uses the routing protocol to promote itself by said having the shortest path to reach destination in network by sending the route reply message earlier than actual destination node. The fake entries in routing tables are placed and whole traffic starts following the wormhole path. Due to which network performance diminishes rapidly and network throughput starts sinking.

Trust based mechanisms are more appropriate for MANETs as compared to protocol modification and hop-time based mechanisms for detection of the above said attacks. Although numerous work has been done in this area, but only few of them has found the solution to attack detection using second hand information from neighbor nodes. Direct and indirect observations have been used to find the trust value.

In this paper we purposed color coded trust based mechanism to identify the malicious nodes and isolate them from the network. The trust value is calculated using neighbor monitoring technique by taking direct observation during actual data transmission and indirect observation during the testing of the naïve nodes when the network traffic is low. The round trip time, color value of the packet received, average delay per hop, number of hop counts are the parameters used for trust evaluation. The trusted network is then formed by detecting the malicious nodes and excluding them from the network.

The paper is structured as follows: Section II gives the brief information about Ad-hoc On-demand Distance Vector routing protocol. Section IV gives the review of literature survey. Section V explains the purposed detection technique based upon the attacks discussed in Section III which is the

foundation of this research paper. Summary and conclusion is assembled in final Section of this paper.

II. AD-HOC ON DEMAND DISTANCE VECTOR VECTOR (AODV) ROUTING PROTOCOL

AODV is Ad-hoc On-Demand Distance Vector routing protocol [3] which is the combination of table driven proactive protocol DSDV and reactive on-demand protocol DSR. The Destination Sequenced Distance Vector (DSDV) protocol uses the prior information of all paths stored in routing table at each node, it uses periodic updates for updating the table entries to select the fresh shortest path to reach the destination as there is more memory and bandwidth consumption in table driven and they cannot be used in large network with high mobility, so on-demand based reactive protocol are used. The main drawback of Dynamic Source Routing protocol (DSR) is use of all intermediate nodes headers in route request and reply messages. This causes more routing overhead and bandwidth consumption. So is not also used in large network with high mobility of nodes. AODV uses only source and destination address and sequence number for route request and route reply messages. AODV is mostly preferred in large network for its good throughput and less routing overhead as compare to other reactive protocols.

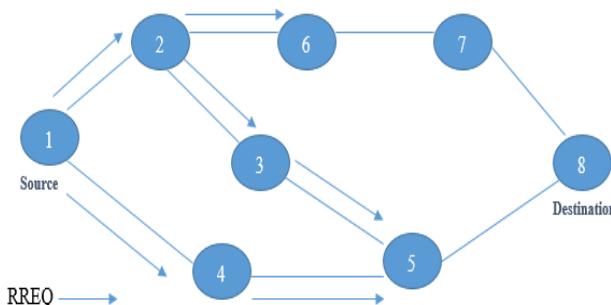


Figure 1: RREQ Broadcasted in the Network

It generates the path with the Route Request (RREQ) / Route Reply (RREP) mechanism as displayed in Figure 1. If the source node has no path to end point, then it broadcast the RREQ message to all neighboring nodes. The nodes which receive the message patch-up the source node information. The information contains source IP address; it also contains the generic sequence number, and transmission identification number. The route request message consists of the sequence number to the target node. The header format of the route request message is given in Table 1. The node which accepts the route request message send back the RREP message, it can be the destination node or the path to destination node includes the sequence number which would be maximum than the route request message. It unicasts the route reply message to the origin node or else it retransmits the route request message. The node will manage the route request's origin location and the transmit identifier. When the node gets the route request message analyzed, it licenses the route request message.

Table 1: Header of a Route Request Packet

Source address	Request Id	Destination Sequence number	Source Sequence number	Destination Address	Hop Count
----------------	------------	-----------------------------	------------------------	---------------------	-----------

As route request message transmits from the origin, it creates the set of nodes to the destination node. When the origin node gets the route reply message as presented in Figure 2, it starts to transmit the data messages to the destination node. When the origin node gets the route reply packet consisting of the sequence number with less number of hop counts, it resumes send the packets via the updated route to the destination node.

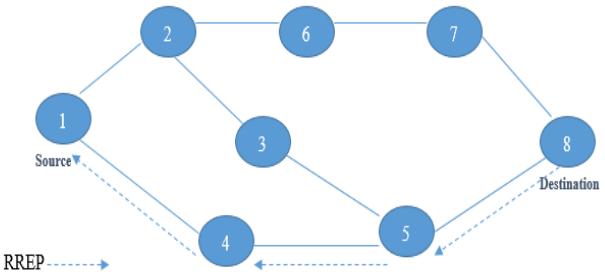


Figure 2: RREP Propagates Back to the Source

Table 2 shows the header format of RREP packet. When the path is alive, it can be utilized. The path is contemplated as alive when the data messages transmit from the origin node to the destination node in the route. When the origin node does not transmit the message, the paths are discarded from the nodes. When the route is broken if the path is alive, the node generates the Route Error (RERR) packet to the origin to brief the unapproachable destination node. When the origin receives the RERR, the origin resends the RREQ for the path reconstruction.

Table 2: Header of a Route Reply Packet

Source Address	Destination Address	Destination Sequence number	Hop Count	Life time	Color Value
----------------	---------------------	-----------------------------	-----------	-----------	-------------

III. ATTACKS IN MANET

Due to various security issues such as dynamic topology, lack of central coordinator, limited resources, no predefined boundary etc., MANETs are more easily attacked by intruders externally as well as internally. The possible well known attacks on MANET are discussed below:

1) *Black hole Attack*: Malicious node send false route reply messages in the network so that other node assumes that it has shortest path towards destination and attacker makes the destination information not available for other nodes in the network [15]. This type of attack is used for playing denial of service type attack. This make destination system unreachable or shutdown in the network.

2) *Denial of Service Attack*:The main motive behind this attack is to make network resource unavailable to the nodes present in the network[11]. On the successful execution of the attack, the network resources will be unreachable. The techniques used by attacker to perform a successful DOS attack in MANET includes jamming of radio signal & making the mobile nodes run out of battery. DOS attack can be classified in the three categories.

a) *Smurf Attack*

b) *Distributed denial of services*

c) *SYN flood attack*

3) *Byzantine Attack*:In this type of attack, [12] there are multiple malicious node which works in conspiracy to create routing loops, transmitting the packet through sub optimal routes as well as dropping of packets .which result in degradation of network performance.

4) *Man- in- the- middle attack*:In this type of attack the attacker node place itself between the source and destination and collects the data transmitted between them on the channel. The attacker nodes use the identity of source to send the data to destination the acts as destination for data transmitted towards sender nodes. It is combination of active and passive attacks.

5) *Grey hole Attack*:It is also known as selective packet drop attack because it drops the packet selectively with assured possibility. The grey hole node works in such a way that for an instance it will act as malicious & then it will switch back to being a normal node.

6) *Wormhole Attack* : In this attack [2] the two attacker nodes that are not in the communication range of each other are connected by a tunnel giving a mistaken belief that they are neighbors. One of the nodes receive route request and topology control messages from the network and send it to the other node via tunnel which will then replay it into the network from there. These nodes are able to declare that they have the shortest path through them by using this tunnel. When the path is established between attacker nodes then they start flooding the network with bogus information by acting as multi relay points. Due to false information all the nodes in network start sending data through them. The attacker nodes then replays that packets in the loop. This induces delay in the data transmission and effects the network performance.

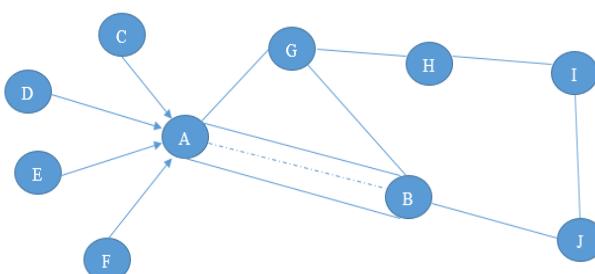


Figure 3: Wormhole Attack with Tunnel

In wormhole a tunnel between two points in the network is created by an attacker. Figure 3 shows A and B are the two end-points in the wormhole tunnel and C, D, E and F are intermediate nodes and J is the destination node. Node A declares that it has direct connection to node J. The all other nodes C, D, E, and F will start transmission using the tunnel created by the attacker. The node B then replay the route requests packets from A to its neighbor nodes. The wormhole attack can be launched using various techniques as using high power transmission, packet relay and encapsulation [22]. When a wormhole attack is launched in AODV, then all the packets will be transmitted through this tunnel and no other route will be discovered. Every node sends RREQ messages by using its neighbor node list to establish path to reach the destination. If the source does not obtain in reverse the RREP message from destination within the specified time, it considers the existence of wormhole attack and adds that route to list. There are two types of wormhole attack:

- Delay sensitive
- Throughput sensitive

In delay sensitive wormhole attack the malicious node either drop packets or forward them to other node which is either mischievous or normal node with the primary concern to divert the packets. In throughput sensitive attack malicious node starts dropping packets making less data available at destination. Wormhole attacks are classified as:

a) *In-band wormhole attack*

It is the attack in which the colluding nodes use encapsulation and protocol deviation methods to perform the attack. The attacker nodes uses the same medium for creating the tunnel. In-band wormhole attacks are further categorized as:

- *Independent Wormhole Attack*: It is the attack where the attack is restricted to the colluding nodes.
- *Extended wormhole attack*: It is the attack where the malicious forces the other victim nodes to pull the whole traffic through them.

b) *Out-of-band Wormhole Attack*: It is the attack in which two colluding nodes connect through physical medium or long range channel which is not used by normal nodes. The attacker nodes may be hidden or exposed nodes in network they use their identity in the network or masquerade the identity of other nodes.

IV. REVIEW OF LITRATURE

A. Based on protocols

Luis Fernando et al., [16] had presented Witness Integration Multipath Protocol that identifies the untrusted nodes behavior related to wormhole nodes. Each legitimate node start neighbor discovery process through temporal leases concept and cryptographic identification is used for authentication between two nodes by use of tamper-proof token. This protocol works fine for open wormhole attacks for only two malicious nodes.

Karthik Raju et al., [13] had offered an algorithm which identifies and eliminate the wormhole attack in the routing

stage. In the purposed scheme the total round trip time is calculated for data transmission from source to destination and also timer values for one hop neighbor route reply messages. As wormhole nodes have high RTT values and they are identified. But there is false positive alarm due to more RTT value due to traffic jam or congestion .The author only consider the malicious nodes present at one-hop neighbors.

Sandiki et al., [6] had identified spoofing attack, and wormhole attack that can be thrown against the QoS-OLSR protocol. To detect the malicious nodes author used improved version of watchdog technique by using cooperative watchdog model and belief function. Watchdog and reputation based concept have disadvantages too. Additional processing delay, packet overhead, false positive alarm were some of the disadvantages in the paper which lead to unsuccessful detection of misbehavior of malicious nodes.

Juhu Biswas et al., [12] had purposed a new method for finding of wormhole links by using modified AODV. To overcome the false detection IP of intermediate node and unique number assigned to it are added in the route reply packet header. After every hour there is increment done by 19 basically a prime number to be used for IP generation. They had assumed that only the legal nodes have this information. The node with unrecognized IP is identified as malicious node. WADP considered exposed wormhole attacks and removed the false positive alarm in WAP.

Vikas Kumar Upadhyay et al., [25] had presented a new detection and prevention technique based on location, neighbor node and hop count methods. If the path discovered by AODV for any two nodes to its next to next nodes is greater than thresholds value than it generates alert then it declares wormhole existence in it's next to next node. Hop-count and neighbor node are two factors considered for threshold value calculation. More control overhead as source node have legitimate the intermediate nodes. It also don't work successfully with large network density.

B. Hop Count and Time Based Mechanisms

Maha Abdelhaq et al., [14] had introduced a new concept in detecting the wormhole attack by using the local network information. The author had purposed the new mechanism in which they detect the malicious nodes by sending the data through different path if there is error in existing path and check existence of wormhole by getting back two acknowledgements. First for path to destination and second for path to previous unreachable node that if the both acknowledgements are received then only data is transferred otherwise there is existence of wormhole. There is still packet overhead and this mechanism considered only for single node attack not for group attack. Also end-to-end delay is not up to satisfactory level.

Aarfa Khan et al., [4] had improved the LID security mechanism by introducing new techniques NWLIDA Normalized Wormhole Local Intrusion Detection Algorithm which is the improved version of local intrusion detection routing security over mobile ad-hoc Network. The concept is same as of LID but there is one other scheme introduced to detect the wormhole by sending the hello packets from node to

next to next node for calculating the peculation value for each node. On receiving the hello packets node calculate the ratio of two values and send the acknowledgement back to sender node. If the value is below 40% then there is wormhole node between the two nodes. More control packets were used which increase the packet overhead and quick capability and bandwidth depletion.

Adel Saeed Alshamrani et al., [2] had introduced an algorithm for identifying wormhole attacks, either in hidden or exposed mode in wireless multi-hop net-works. Author introduces a new mechanism called Packet Travel Time (PTT) based on transmission time-based mechanism. Each single node has to send the main Values (RREQ sending time and RREP receiving time) to the source which will be responsible to make the Round Trip Time (RTT) calculations between a midway node, the destination, and between each pair of successive nodes. To make the discovery of a secure route from a source to destination threshold cryptography is used to prevent illegal node. But there are more delays in processing and increase in mobility which effect the PTT.

Saurabh Gupta et al., [17] had proposed a routing protocol WHOP (Wormhole Attack Detection Protocol using Hound Packet). If ad-hoc network is formed between trusted parties or for private use then security related issues had not been considered hence there is no need to send Hound packet but if network is open and nodes experiences high packet dipping then Hound packet will be send after the path discovery phase. Source node initiates wormhole detection process in the recognized path which counts hop difference between the neighbors of the one hop away nodes in the route. The destination node identifies the wormhole if the hop difference between neighbors of the nodes exceeds the adequate level. Detection and processing delay is higher, hence affect the network performance.

Soo-Young Shin et al., [6] had proposed method by using routes redundancy, routes aggregation and round-trip time (RTT) of all recorded routes. Routes redundancy happens when source sends RREQ using every possible way to reach the destination. All routes that connect source and destination are registered together with the number of hops from every route. Some routes grouped in the same relay point before destination is collected, so all nodes that join the network can be recorded and the behavior of mischievous nodes in can be detected. The RTT and number of hops of all recorded routes are compared in order to detect doubtful route. Nodes with suspicious behavior within network are isolated and will not be considered for transmission.

C. Trust and Reputation Based Mechanism

In mobile ad-hoc network a selfish node starts saving its resources (e.g. battery power and bandwidth) did not cooperate and drops packets which do not belong to it. Due to which cooperative nodes will be overloaded, hence network performance will degrade. Saeed Soltanali et al., [18], had proposed a distributed scheme which was combination of reputation based and currency based schemes to mitigate defects of malicious nodes without use of central control or a priori trust between nodes. The purposed scheme only

considered misbehavior in forward operation and assumes the special scenario not applicable in real life applications.

To find the shortest and trusted path in AODV Jassim et al., [7] had introduced new concept based on trust model which is basically modification of AODV to R-AODV (Re2iant Ad hoc On-demand Distance Vector Routing) by considering the direct and indirect recommendations of trustworthiness of each node in network. There is load misbalancing and higher end-to end delay due to extra processing in choosing the path.

Sudharson Kumar et al., [22] had purposed a fully distributed reputation based mechanism by using Eigen vector & Degree uniqueness for calculation of the individual trust value. More power and memory is used to store the values at each node. A novel trust-enhanced multicast routing protocol (TEMR) had been proposed by Hui Xia et al., [8]. This new protocol introduces the group-shared tree approach, which creates more capable multicast routes since it uses ‘trust’ factor to improve the efficiency and robustness of the forwarding tree. Only route trust and trust value field are added in RREQ and RREP control packets of MODV. Multicasting is done by forwarding hello packets by intermediates nodes at regular intervals. Monitoring and trust value were calculated by using direct observation and recommendations by other nodes for legitimate node .Due to mobility there is much link failure so more processing delay in path reconfiguration.

The mobility based clustering approach had been enhanced by Aida Ben Chehida Douss et al., [1] by covering their earlier work, a reputation-based trust management scheme that detects malicious routing behaviors and isolates them. Clustering environment organized nodes into clusters and elected cluster-heads and extended with a delegation process. The proposed reputation-based trust management scheme was based on cluster heads direct observations as well as alerts exchanged, monitors the behavior of its cluster members and updates reputation values according to events detected. More resources were consumed and malicious member node or detached member node colluded and formed attack.

V. THE COLOR CODING BASED DETECTION AND PREVENTION TECHNIQUE

Out of various attacks in MANET as black hole attack, denial of service attack and gray hole attack are throughput sensitive attacks, these can be easily identified in network using various detection approaches because in these attacks the malicious nodes primary aim is to drop the packets which may be data packets or control packets or both. This makes less data available at destination. These are mostly active attacks but in gray hole it could passive as well. On other hand wormhole attack is delay sensitive attack in which the malicious node perform many attacks by passing the network traffic through it. There may be passive eavesdropping attack, or sending of the data via one malicious node through other malicious nodes. The delay is increased in this attack as data transmitted through wormhole tunnel. The other nodes in the network

could not identify the reason of delay i.e. whether it is due to malicious activity or due to network congestion.

In our proposed work we are introducing novel technique for identifying and isolating the wormhole attack in MANET by using AODV reactive protocol. The reactive protocol works efficiently in terms of throughput and end to end delay in comparison to proactive routing protocol. The AODV is based on Dijkstra algorithm which has low complexity than other reactive protocols like DSR, ABR etc. The methodology is demarcated as following:

- The network is initially formed using various nodes which are categorized as trusted nodes assigned with the green color.
- Because of unpredictable behavior of new nodes within the network, they are initially assumed as untrusted nodes and have been assigned the black color.
- Initial communication in the network would be enabled only through the trusted nodes by using the AODV protocol.
- The nodes will keep monitoring the behavior of its neighbor nodes via watchdog technique for examining the trustworthiness of nodes based on round trip time, number of hop counts, color value, average delay per hop and jitter value. Based on the calculated value of the nodes color of the nodes would be dynamically changed through the timely observations made.
- The nodes would receive color in the ascending order as black (if node is naïve/malicious), red, yellow and green (if node is trusted). The values of color are provided in table 3. The route reply packet header has been slightly modified by inculcating the frame for color value which will capture the color value assigned to each node.

Table 3: Color Values

Color	Value
Green	1
Yellow	.5
Red	.25
Black	0

- During the path formation from the source to destination using the AODV routing protocol the source node would broadcast the Route Request (RREQ) packet to its neighbor nodes to find the path to the destination.
- In AODV protocol the source node chooses the shortest path based upon the first Route Reply (RREP) packet received.

Ticketing Window Time = Round Trip Time of 1st RREP Packet Received.

- As possibly the RREP packet which is received could be from the wormhole; in our technique ticketing window would be used at the source node. Ticketing window will allow the source node to receive the RREP packets from its neighbor nodes other than the first RREP packet for the period of time which will be equal to the round trip time of the first RREP packet.
- Based on the various RREP packets received within the ticketing window the source node will check the header of the RREP packets for trusted path selection on the basis of calculated path value (PV)
- Path cost (PC)* which is equal to the total of *calculated value of the color in the color frame* of the header (CV), *number of hop counts (HC)* and *round trip time (RTT)* and is inversely proportional to the *total number of nodes (N)* which participated in route formation. So,

$$PC = (RTT + HC + CV) / N$$

- As wormhole remains closest to the source node always, the *total number of nodes (N)* would be minimum in this case as compared to other paths alive.

$$PV \propto 1/N$$

- As path value is indirectly proportional to total number of nodes the route with minimum path value would be selected for data transmission in the network.
- As a counter measure credit based mechanism would ensure the delivery of the packets. As wormhole attracts the whole traffic to follow the same path and hence will have high *packet balancing ratio (PBR)* i.e. total number of packets sent by the node upon the total number of packets received by the node. If ideally there is no packet drop and are forwarded then the ratio would be 1 and if packets are only received but not sent then the ratio would start minimum.

$$CV \propto PBR$$

Where, *CV* stands for Credit Value of the Node

- As *CV* is directly proportional to the packet balancing ratio of the node, the node should must maintain its credit value closer to 1, more its closer more its better.
- As this suspicious behavior of the node would be observed by other nodes, they will generate an alert based on *CV* throughout the network about the existence malicious node. Such nodes would be identified and would be excluded from the network.

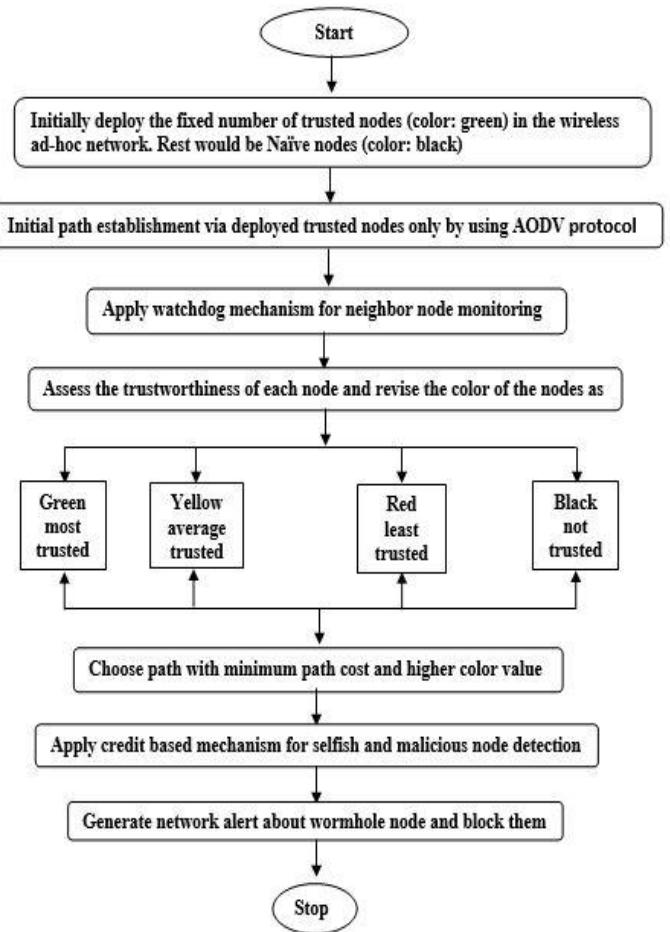


Figure 4: Research Methodology

A. *Expected Outcomes:* The above mentioned methodology will facilitate in:

a) *Trusted path formation:* The color value in the header format used during path discovery process in AODV routing protocol will help the source node choose the most trusted path having lowest path cost among the available paths.

b) *Identifying the wormhole attackers nodes:* Trust mechanism which is based on neighbor node monitoring concept for identifying the suspicious behavior of nodes. As the credits counter value of wormhole nodes will be very low as compared to normal nodes hence would get detected by other nodes.

c) *Providing acceptable level of throughput:* The throughput of the network will increase by isolating the malicious nodes from the network using AODV. Because of trusted path formation the packet delivery ratio will also increase.

d) *Load balancing and Reliable Data Transmission:* The concept of credits will enable reliable data transmission as well as help balance the traffic load and hence encouraging the other nodes to gain the trust.

e) *Punishing malicious and selfish nodes:* Through the use of trust values and credit mechanism the trusted network is formed in which the malicious or selfish nodes will be excluded.

VI. SUMMARY AND CONCLUSION

Wormhole is a delay-sensitive attack. The attacker nodes make destination unreachable and replay the messages by changing headers of the packet by masquerading the identity of other nodes which is member of the network. Due to which messages are not dropped but circulates in loops or tunnels thus end to end delay increases. Out of Hop-Count and Time, Trust and Reputation and Protocol modification based methods, the trust and reputation based techniques can identify and isolate the malicious nodes in network without affecting much of the throughput and network resources. Color Coding initially will help in differentiating between the trusted and naïve nodes and also in discovering and establishing the most trusted path throughout the network. The use of neighbor monitoring technique will help collect information about the behavior of the nodes in the network which will further help in calculating the trust value of the nodes based upon color value of the node, number of hop counts, average delay per hop, jitter value and round trip time. Credit counter will help to check the reliability of data transmission in the network. So both the trust value and credit counter together will detect the malicious nodes based upon their values which possibly should be less in count than other nodes through the network. Thus this novel technique would help to detect malicious nodes and further help eliminate the execution of wormhole attacks consequently improving the performance of the network and ensuring that it is innocuous for communication.

REFERENCES

- [1] Aida Ben Chehida Douss, R. A. ,”A Model for Specification and Validation of a Trust Management based Security Scheme in a MANET Environment”,*IEEE*, pp.341-350, 2015.
- [2] Alshamrani, Adel Saeed. "PTT: packet travel time algorithm in mobile ad hoc networks." In Advanced Information Networking and Applications (WAINA), 2011 IEEE Workshops of International Conference on, pp. 561-568 , 2011.
- [3] Charles E.Perkins , E.M.Royer Ad-hoc on-demand distance vector routing*1999Second IEEE Workshop on Second IEEE Workshop on Mobile Computing Systems and Application 1999*90-100.
- [4] Khan, Ajmal, Shweta Shrivastava, and Vineet Richariya. "Normalized Worm-hole Local Intrusion Detection Algorithm (NWLIDA)." In Computer Communication and Informatics (ICCCI),International Conference on, pp. 1-6 ,2014.
- [5] Halim, Y. S. (2012). "Wormhole Attacks Detection in MANETs using Routes Redundancy and Time-based Hop Calculation. *ICTC,IEEE*, 781-786.
- [6] Hiba Sanadikia, H. O.-M. (2013). Detecting Attacks in QoS-OLSR Protocol. *ieee*, 1126 - 1131.
- [7] Hothefa Sh.Jassim, S. Y. (2009). A Routing Protocol based on Trusted and shortest Path Selection for Mobile Ad hoc Network. *IEEE*, 547-554.
- [8] Hui Xia, J. Y.-y.-g.-k. (2014). Trust-enhanced multicast routing protocol based on node's behavior assessment for MANETs. *IEEE*, 473-480.
- [9] I. Woungang, S. D. (JAN-2012). Detecting Black-hole Attacks on DSR-based Mobile Ad-hoc Networks. *IEEE*, 1-5.
- [10] Isa Maleki1, R. H. (August 2013). SECURITY IN ROUTING PROTOCOLS OF AD-HOC NETWORKS: A REVIEW. *International Journal of Mobile Network Communications & Telematics (IJMNCT)*, vol. 3.
- [11] Jin Guo, Z.-y. L. (2011). “A Kind of Wormhole Attack Defense Strategy of WSN Based on Neighbor Nodes Verification. *IEEE*, 978-1-61284-486-2.
- [12] Juhi Biswas, A. G. (2014). WADP: A Wormhole Attack Detection And prevention Technique in MANET using AODV. *IEEE*, 1-6.
- [13] Ksarthik raju, v. k. (2012). A Simple and Efficient Mechanism to Detect and Avoid Wormhole Attacks in Mobile Ad Hoc Networks. *ICCS(International Conference on, Communication Systems)*, 271-275.
- [14] M. Abdelhaq, S. S. (17 July 2011). A Local Intrusion Detection Routing Security Over MANET Network. *International Conference on Electrical Engineering and Informatics, Indonesia* , 1-6.
- [15] N. Bhalaji, A. S. (2011). “A Trust Based Model to Mitigate Black Hole Attacks in DSR Based MANET. *European Journal of Scientific Research*, Vol.50 No.1, pp.6-15.
- [16] Robert, L. F.-M. (2009). Preventing Layer-3 Wormhole Attacks in Ad-hoc Networks with Multipath DSR. *ieee*, 15-20.
- [17] S. Gupta, S. K. (2011). Wormhole Attack Detection Protocol using Hound Packet. *International Conference on Innovation in Information Technology, IEEE* , 226-231 .
- [18] Saeed Soltanali, S. P. (2007). An Efficient Scheme to Motivate Cooperation in Mobile Ad hoc Networks. *ieee*, 98.
- [19] Sharma, G. M. (2011). A Robust Approach to Detect and Prevent Network Layer Attack in MANETS. *International Journal of Computer Science and Security*, Vol. No.3, pp 276-285.
- [20] Sharma, N. N. (February 2013.). A Novel Approach for Wormhole Detection in MANET. *International Journal of Computer Applications*, (0975 – 8887) Volume 63– No.7.
- [21] Singh, j. (july 2013). A Review Paper on Introduction to Mobile Ad Hoc Networks. *International Journal of Latest Trends in Engineering and Technology*, vol 2.
- [22] Sudharson kumar, p. (2011). SOPE: Self-Organized Protocol for Evaluating Trust in MANET using Eigen Trust Algorithm . *ieee*, vol.2 155-159.
- [23] Vandana C.P, A. F. (2013). Evalution of impact of wormhole attack on AODV. *International Journal of Advanced Networking and Applications*, ISSN 0975-0290 Volume: 04 Issue:04 pp. 1652-1656.
- [24] Vanita Rani, D. R. (march,2013). A Study of Ad-Hoc Network: A Review. *International Journal of Advanced Research in Computer Science and Software Engineering*.
- [25] Vikas Kumar Upadhyayl, R. K. (2014). Detection and prevention of worm holes in mobile ad-hoc networks using Hybrid Methodology. *ieee*, 1-6.

Pragmatic Analysis Based Document Summarization

Ms. Bhakti A. Mukhedkar^{#1}, Mrs. D.Y.Sakhare^{#2}, Mr. Raj Kumar^{*3}

[#]Department of Electronics Engineering
MIT Academy of Engineering, Alandi
Pune, India
^{*}Scientist DRDO, Pune.

Abstract- Automatic Text summarization is the process of reducing a text document to create a summary that relates only important points of the original document. Now a day's huge information available so there is interest in automatic Text summarization. It's very hard for human being to manually summarize large documents of text. Hence we use Text Summarization techniques. Basically Text Summarization Techniques classified in two types 1. Abstraction 2. Extraction. In this Paper We Proposed Abstraction Type of Text Summarizations by using pragmatic analysis. This Summary being generated by Matlab and serially transmitted to PIC microcontroller and displayed on LCD.

Index Terms— POS Tagging, Text Summarization by pragmatic analysis.

I. Introduction

The Purpose of Text Summarization is to represent most important information into reduced version of the original text and keeps its original content as it is which helps the end user to understand large volume of information. Text Summarization focuses both the problem of selecting important section of text and the problem of generating clear summaries. Automatic Text Summarization mainly classified as Extraction &Abstraction [11]

Extraction summary is a selection of sentences from the original text with the higher score and regenerated to new shorter text without changing the original text. But problem with extractive summary is that important or related information spread across the sentences and extractive summaries unable to capture this. For text summarization summary evaluation is very important aspect. Abstraction Summarization tries to develop a knowing the main concepts in clear natural language. It uses linguistic methods to examine and interpret the text then it finds new concepts which describe it by generating new shorter text which conveys the important information from the original text document. The advantage of abstraction method is it gives result as human being thinks. In this paper we propose the summary for article by using abstractive method. In this we want to generate the

summary and same we want to show on LCD by using PIC Microcontroller.

In this paper Text Summarization Technique is designed using Pragmatic analysis [12] The proposed system generates summary by analyzing all the different parts of the documents.

II. RELATED WORK

[1] Extraction types of Summary is a selection of sentences or phrases from the original text with highest score and combine it together to a very new shorter text but it doesn't affect or change our source text.i.e. Our original text.

This paper focuses on Extraction approach. Sentence selection is the goal of text summarization based on extraction approach. In this identification of important features is the first step in summarization by extraction. In this each document is prepared by preprocessing process, sentences segmentation Tokenization removing stop word and word stemming then used 8 features and calculated their score. In this we compared the average precision, recall and frequency measure and score between GSM, Fuzzy summarizer, Microsoft word 2007 summarizer and base line summarizer and result shows that fuzzy method is best for average precision, recall and frequency measure. [2] The primary aim of this paper is to compare summaries which are generated by different automatic text summarization methods and who will generate by human beings. Automatic summarization can reduce the problem of information overloading. In this paper ideal automatic summary and ideal manual summary produced, ideal automatic summary produced by 2 methods, 1.Fuzzy logic, 2.Vector logic. Ideal manual summary produced by several teachers by selecting relevant sentences of the text. In this with the help of ROUGE measures the quality of summary by comparing other summaries. In this manual evaluation of text also done by following, 1. Text flow 2. Understandability 3. Overall impression process and result shows that the score of manually generated summary is high, but it's very close to fuzzy logic. Both manual evaluation and ROUGE evaluation shows that superiority of human summaries over the automatically produced. When we have long text to read that time Fuzzy method is

more economical, appropriate and efficient so automatic text summarization are much faster than human summaries. Fuzzy method is good replacement of human summaries, which can deal a large amount of information faster and easier.

[3] In this paper according to them; a summarization system consists of shorting of a text document to generate a new form which conveys the exact meaning of the contained text. Due to the problem of huge information access to sound and correctly-developed summaries is necessary. In today's world Text summarization is the most challenging task in information retrieval. Limited kind of data helps a user to find required information fastly without wasting time and effort in reading the whole document collection. In this paper presented a combined approach to document and sentence clustering as an extractive technique of summarization.

[4] In this Paper an algorithm using fuzzy logic has been presented. In this new generation, where the lot of information is available on the internet, it is difficult to get the information quickly and most efficiently. There are lot of text materials available on the internet, in order to get the most relevant information from it; we should have a good mechanism. This problem is resolved by the Automatic Text Summarization mechanism. This paper concentrates on the Fuzzy logic Extraction approach for text summarization

[5] This Paper said that the text Summarization is the procedure by which the major portions of a text are retrieved. Lot of approaches perform the summarization based on some hand tagged rules, such as format of the, position of a sentence in the text, writing of a sentence, frequency of few particular words in a sentence etc. But according to different input sources; these predefined constraints heavily affect the result. In this proposed approach evaluate the summarization task by unsupervised learning methodology. The importance of a sentence in an input text is determined by the help of Simplified Lesk algorithm.

Considering the relationship between sentences and words; Xun Wang [7] and Zha [6] this proposes a method for keyword extraction and summary generation by utilizing the sentence-word relationships which shows the impact of sentences on words. Wang et al. [8] improves this method by employing three kinds of relationships: sentence-sentence, sentence-word and word-word. The interconnection between sentences and words is taken into consideration for summarization and keywords selection.

III. METHODOLOGY

In this paper we implemented following block diagram which consist of tokenization, stop word removal, weighted term, POS tagging, Word Sense Disambiguation and Pragmatic analysis

1. Database: it is a source of the system. It consists of files on which we do text summarization.

2. Tokenization: in this we do the separation of each word from sentences. It consists of list of tokens.

3. Stop word removal: it provides less meaning in document

But it appears regularly. So we are removing these words from tokenization and making new file.

Example of stop words: about, and, are at, as do, each, for, from, have, but both, between etc

4. Weighted Term: the words occurring higher times means weighted term. We do this step after stop word removal.

Ex: the term occurring 8 times is important than the word occurring 2 times

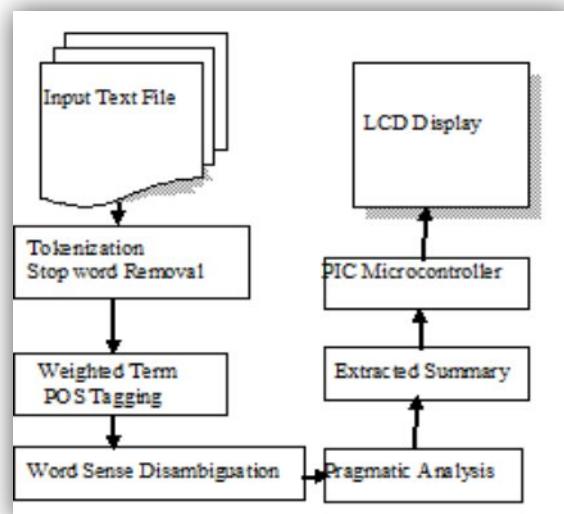


Fig. 1. Block Diagram

5. POS Tagging: [13] In this it takes sentence as input and applies unique tag to each word in the sentence such as noun, verb, adverb, adjective.

6. Word sense disambiguation: in this we identify different senses of word [14] i.e. same word having different meanings. According to our input we decide the meaning of text. There are two approaches 1. Deep approaches 2. Shallow approaches. We follow shallow approach in this as it needs limited knowledge of domain

7. Pragmatic Analysis: it is the study of the meaning in context. By which we get intended meaning of the text [15] it focuses on meaning behind word. It can be done on fixed format articles.

8. Extracted Summary: once pragmatic analysis done summarized sentence will get stored in a database, this is the result of text summarization. In document after pragmatic analysis extracted summary will get in command prompt of MATLAB window and that summary we want to Show on LCD Screen by using PIC microcontroller

The following diagram shows the flowchart of hardware and software of text summarization system.

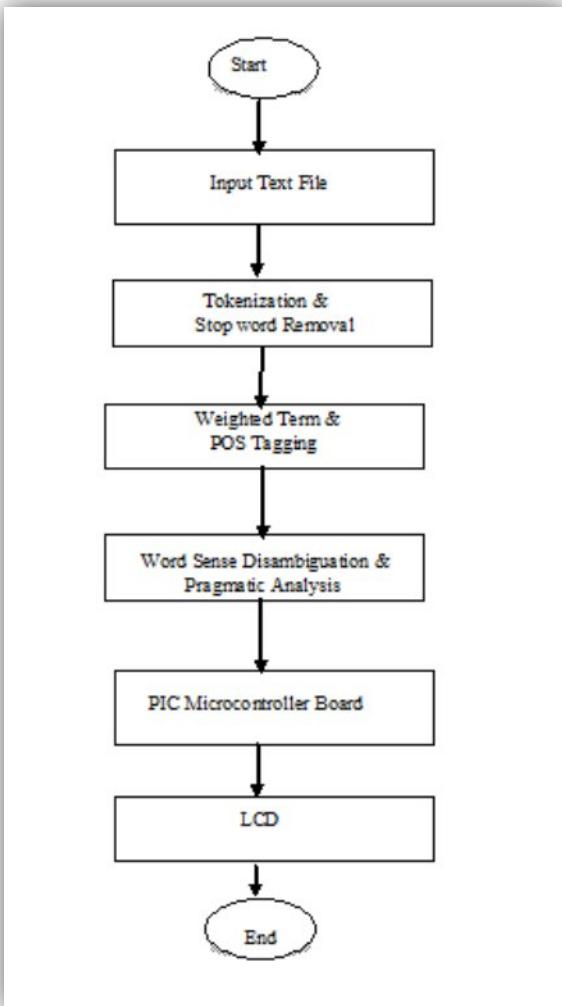


Fig. 2. Flowchart

Here we have interfaced PIC microcontroller with MATLAB and then output of the MATLAB is serially transmitted to LCD(interfaced with PIC).The PIC microcontroller will receive data from the text file and then the received serial data is given to LCD(Liquid Crystal Display) for display purpose.

1) PIC (Peripheral Interface Controller)

PIC is one of the open source platform for designing electronics project.PIC 16F877A is Flash 40 pin 4 MHz, 8KB microcontroller.PIC micro is one of the most popular microcontroller with internal RAM, Flash memory& peripherals. It consists of both a physical programmable circuit board (often referred to as a microcontroller) and a piece of software, or IDE (Integrated Development Environment) that runs on our computer, used to write and upload computer code to the physical board.

2) PIC-Matlab Interfacing

Firstly we store output data in variable, then we write it in the text file (data saved in the form of arrays). After that we will open our COM port by using the command (fopen). Then we write a suitable code (in IDE), which will receive data from text file (via Matlab code).After executing Matlab code output will be stored in PIC.

3) PIC - LCD interface

Now the serially transmitted data is stored in PIC board and further given to LCD for display. We are using 16*2 LCD for display purpose

IV. RESULTS

1) Input

The sun is a huge ball of gases. It can be seen rising everyday along the bank of river. It has a diameter of 1,392,000 km. It is so huge that it can hold millions of planets inside it. The Sun is mainly made up of hydrogen and helium gas. The surface of the Sun is known as the photosphere. The photosphere is surrounded by a thin layer of gas known as the chromosphere. Without the Sun, there would be no life on Earth. There would be no plants, no animals and no human beings. As, all the living things on Earth get their energy from the Sun for their survival. The Moon is a barren, rocky world without air and water. It has dark lava plain on its surface. The Moon is filled with craters. It has no light of its own. It gets its light from the Sun. The Moon keeps changing its shape as it moves round the Earth. The Solar System consists of the Sun Moon and Planets. It also consists of comets, meteoroids and asteroids. The Sun is the largest member of the Solar System. The Sun is at the centre of the Solar System and the planets, asteroids, comets and meteoroids revolve around it.

Fig. 3. Input

2) Output

Above Paragraph is given as an input.i.e. Text files to Matlab. Then as per our block diagram we have done steps such as tokenization, stop word removal, weighted term, post tagging, word sense disambiguation and pragmatic analysis. By using all these steps we get extracted summary on command prompt of Matlab.

We have created our own data set which consists of collection of documents and we have done pragmatic analysis and also we have done manual summarization. According to our result, result obtained by using pragmatic analysis is much better than manual summarization. And it gives Fifty percent reduction of original text.

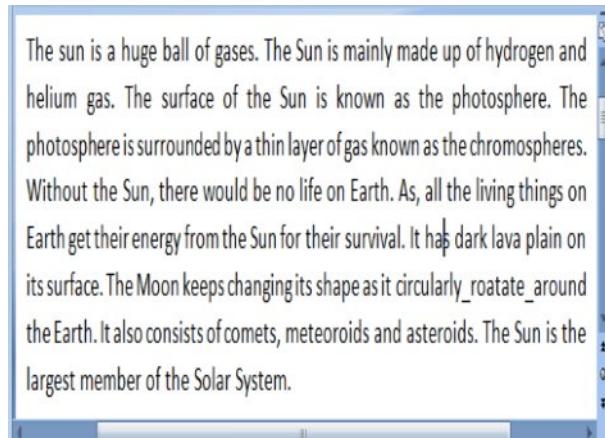


Fig. 4. Output

3) Output on Matlab (GUI)

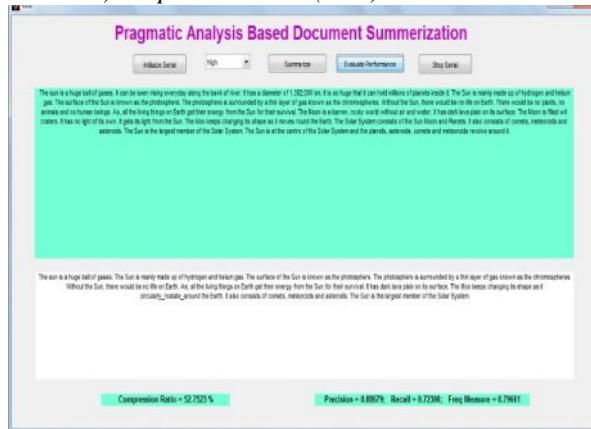


Fig. 5 Output on Matlab (GUI)

A. Output with Hardware

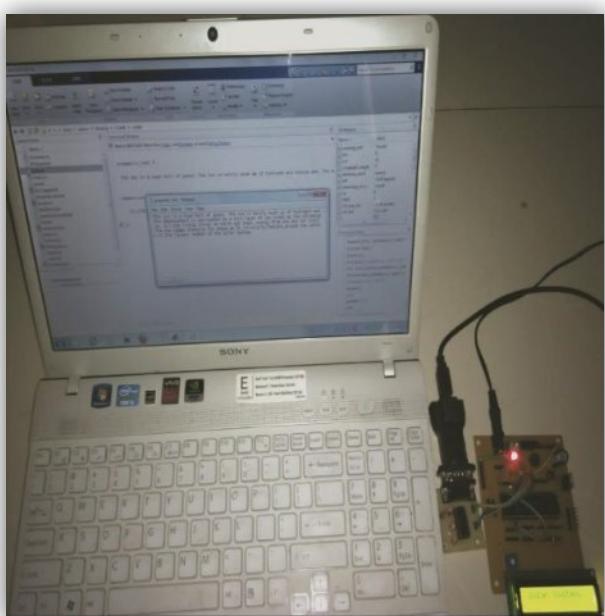


Fig. 6 Output with Hardware

V. Performance Metrics & Graph

There are three parameters by using we can evaluate performance of Text document

1. Precision 2. Recall 3. Fmeasure

If the set of sentences selected by an automatic extraction method has a high Overlap with the human-generated extract, the automatic method should be regarded as effective. Assume that S_{man} is the manual summary and S_{auto} is the automatically-generated Summary, the measurements are defined as [9]

Precision: It can be calculated by using following formula,

$$P = \frac{|S_{manual} \cap S_{automatic}|}{|S_{automatic}|} \quad (1)$$

Recall: It can be calculated by using following formula,

$$R = \frac{|S_{manual} \cap S_{automatic}|}{|S_{manual}|} \quad (2)$$

F-Measure: it can be calculated by following formula,

$$F = \frac{2\text{Precision} * \text{Recall}}{\text{Precision} + \text{Recall}} \quad (3)$$

Comparative Analysis: By using “(1)”, “(2)” and “(3)” presents comparative analysis of proposed system with existing system. The proposed system achieves high Precision, Recall and F-measure as compare with existing system [10]. Table 1 gives the comparison of precision, recall & F-measure.

Table I

Summarization System	Precision	Recall	F-measure
Proposed System	0.72	0.88	0.792
Existing System	0.69	0.56	0.62

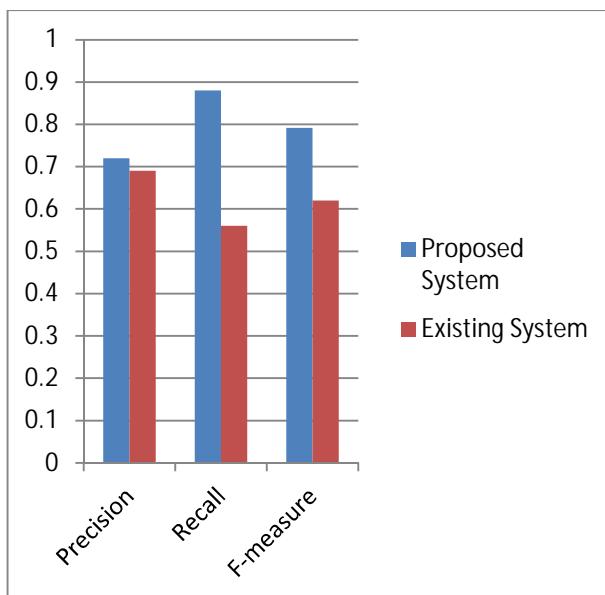


Fig. 7. P,R, & F Graph

Extraction”, ACL2007 [9] Rasim M M. Alguliev Ramiz M. Aliguliyev Appl. Comput. Math. 6 (2007), no.2, pp.278-287

[10] Namita Mittal, Basant Agarwal Himanshu Mantri Rahul Kumar Goyal and Manoj Kumar Jain Department of Computer Engineering, Malaviya National Institute of Technology, Jaipur India.Vol.4, No.2 (April 2014)

[11] Rafeeq Al-Hashemi, Text Summarization Extraction System (TSES) Using Extracted Keywords, International Arab Journal of e-Technology, Vol. 1, No. 4, June 2010 pp 164-168

[12] Manisha Prabhakar,Nidhi Chandra International Journal of Scientific and Research Publications, Volume 2, Issue 5, May 2012 1 ISSN 2250-3153

[13] Chai, Joyce Y. and Biermann, Alan W.: A WordNet based rule generalization engine for meaning extraction, to appear at Tenth International Symposium On Methodologies For Intelligent Systems (1997)

[14] Prabhakar Pande Lakshmi Kashyap Manish Sinha, Mahesh Kumar and Pushpak Bhattacharyya.Hindi word sense disambiguation. In International Symposium on Machine Translation, Natural Language Processing and Translation Support Systems, Delhi, India, November 2004

[15] F. Yetim, “DISCOURSIUM for cooperative examination of information in the context of the pragmatic web,” 2nd International Conference on the Pragmatic Web, Tilburg, The Netherlands, 2007,pp.29-40

VI. CONCLUSION

In this paper we proposed automatic text summarization approach by pragmatic analysis using Abstractive method for text document. By pragmatic analysis intended meaning of text is obtained and generated summary stored in database and same summary to shown on LCD by using PIC microntroller. The system gives better result than manual summarization.

REFERENCES

- [1]Ladda Suanmali1, Naomie Salim2 and Mohammed Salem Binwahlan3 1Faculty of Science and Technology, Suan Dusit Rajabhat University, Bangkok, Thailand 10300,2,3Faculty of Computer Science and Information System, Universiti Teknologi Malaysia 81310. (IJCSIS) International Journal of Computer Science and Information Security, Vol. 2, No. 1, 2009
- [2] Farshad Kiyomarsi Islamic Azad University Shahrekord Branch Iran 1877-0428 2015.
- [3]Anjali R. Deshpande, Lobo L. M. R. J., “Text Summarization using Clustering Technique”, International Journal of Engineering Trends and Technology (IJETT) - Vol.4 Issue8- August 2013
- [4]Ms.Pallavi D.Patil, Prof.N.J.Kulkarni, “Text Summarization Using Fuzzy Logic”, International Journal of Innovative Research in Advanced Engineering (IJIRAE) Volume 1 Issue 3 (May 2014).
- [5]Alok Ranjan Pal, Diganta Saha, “An Approach to Automatic Text Summarization using WordNet”, IEEE International Conference on Advanced Communication Control and Computing Technologies, 978-1-4799- 2572-8/14©2014.
- [6]H. Zha,“Generic summarization and key phrase extraction using mutual reinforcement principle and sentence clustering”, SIGIR2002
- [7]Xun Wang, Lei Wang, Jiwei Li, Sujian Li “Exploring simultaneous keyword and key sentence extraction: improve graph-based ranking using Wikipedia”, ACM, international conference on Information and knowledge management 2012.
- [8] X. Wang, J. Yang, J. Xiao, “Towards an Iterative Reinforcement Approach for Simultaneous Document Summarization and Keyword

Mobility Aware Fault Tolerant Multipath Multicast Routing Protocol for MANET

Channabasayya Mathad¹

Dept. of Electronics & Communication
Engg, Kalpataru Institute of Technology,
Tiptur Karnataka, India.

Paramesha²

Dept. of Electronics &
Communication Engg Govt
Engineering College, Hassan
Karnataka, India.

D Srinivasa Rao³

Dept. of Electronics &
Communication Engg
Jawaharlal Nehru Technological
University, Hyderabad Telangana India.

Abstract— In MANETs, due to the constant mobility of the nodes, the topology is ever changing. Hence, the selection of paths is crucial. So, it is always efficient to select more than one route to the destination, so that even if one path fails, there is always high possibility for the data to reach the destination. In MANETs, since the nodes keep on joining and leaving the network randomly, selecting paths that are less susceptible to turn out faulty is important. Since several disjoint paths are possible, multicasting is economical in MANETs. In this proposed scheme a multipath, multicast routing protocol which works efficiently by selecting route with higher lifetime and it also recovers the lost packets.

Keywords-Multipath,Multicast,Fault Tolerent,LinkLife Time, Hop Count.

I. INTRODUCTION

A. Mobile Ad-hoc Network

MANET is a self-adapting network with mobile topology formed by a set of mobile nodes that are connected to each other through radio links. The nodes in this network are not dependent on any predetermined infrastructure and use wireless communication [1, 7]. As the nodes are randomly moving in and out of the transmission range, the network topology can be constantly varying, thereby increasing the possibility of link or node failure. This can lead to the increased energy consumption while transferring the packets from the source to the destination (i.e. routing), resulting in reduced routing performance [3]. Routing protocols in MANET can be broadly classified into proactive (every node records the update in a periodic manner with a table format), reactive (the paths are found out on demand), and hybrid routing protocols (the characteristics of both proactive and reactive protocols are used) [1].

B. Multipath Routing Protocol for MANET

In wireless networks, owing to the restrained transmission range of the nodes, several hops are needed to transfer the data message from the source to the destination. Therefore, routing protocols are considered to be significant in MANET communication. Multipath routing is a routing protocol in which several paths can be identified between the source and the destination as the nodes are randomly connected to other nodes [2]. In this type of routing, many redundant data packets are transmitted through multiple paths [5]. Therefore, the data can reach the destination node even if there is a single feasible

path. As a result, multipath routing is considered to be more efficient than single-path routing and as a practical way of providing consistent routing services [4].

The aim of the multipath routing is to improve the consistency of the routing method while transferring data packet. Therefore, data can reach the destination through the other route even in case of route failure. However, multipath routing can drastically increases the network traffic [1]. Application of multipath technique is very efficient because it can balance the load and safeguard the data from link failure by sharing of the data traffic in several disjoint paths. In MANETs, the major criteria in developing the routing protocol are:

- Dispersed and light weight
- Ability to be fault tolerant
- Mobile network maintenance
- Simple and easy to implement
- Highly reliable and scalable to large extent [2].

In MANET, data packets are transmitted via several routes to several receivers in the multicast group; it will not transmit to a single receiver via single route. By using this mechanism, two most stable paths to the destination will be chosen. The most stable path is chosen as the primary path to the receiver, whereas the other path is kept for additional purposes. When the primary path breakdown, then the other path will be used instantly for transferring data packet [11].

Some of the issues in multipath routing are as follows:

- After the determining the nodes for data transfer, it is hard to choose appropriate path.
- Determining the number of paths selected for transmitting data packets is difficult [2].
- There are redundant operating overheads [5].

C. Fault-Tolerant Multipath Routing Protocol for MANET

In MANET, failures such as node breakdown, link breakdown, excessive energy usage, network breakdown, excessive power usage, and so are possible. Therefore, fault tolerant mechanism is used for avoiding these failures. Fault tolerance is the capability to respond to unpredicted hardware

and software breakdown. If breakdown occurs, it need be repaired or should be concluded as not repairable. [1, 3] The fault tolerant capability is high in multipath routing as multiple copies of the data packets are transmitted to the destination via all possible routes [5]. Using fault tolerant technique, channel breakdown can be prevented and the source reroutes the data to recover the lost data [4]. In case of undesirable environment with several defective nodes, the fault tolerant-routing protocols determine redundancy in the network by addressing routing [6].

D. Multicast Routing in MANET

Multicast routing is a routing protocol in which same message is transmitted from a single source to several destinations. In the Quality of Service (QoS) based multicast routing, a multicast tree is formed from the source to every destination node. The paths chosen using tree multicasting complies with the transmission QoS requirements [13]. Multicasting is efficient as it minimizes the communication cost, bandwidth utilization by the link, delay in data delivery, and overhead in data transmission with increased data delivery speed at the destination [15].

Multicast routing protocols are divided into two groups, namely, tree-based protocol and mesh-based protocol. In tree-based multicast routing protocol, single path exists between the source and the destination, whereas in mesh-based protocol, multiple paths exist from the source to the destination. Tree-based multicast topology is consistent in terms of efficiency as several paths are accessible. Mesh-based topology is stable in terms of robustness and dependability [14]. Handling the mobile nodes along with data transmission is a challenging task during reliable multicasting. This may result in the loss of contact of intermediate nodes with each other and loss of multicasting data packets [12].

II. RELATED WORKS

The network has several defective nodes; most of the proposed ad hoc protocols consider the fact that the nodes in the network operate in an ideal way. In this protocol [5], network that has faulty nodes is considered in which routing protocol can discover strategies for employing redundancy in data transmission. Under any network circumstances, multicast protocol transfers data with reduced overhead. This protocol [6] manages the data delivery in the mobile and irregular topology change in the network using multicast technique. For this multicasting, there is no requirement to withstand any particular structure such as tree or mesh. This protocol has no need to have a partial or global idea of the network. In addition, this protocol did not require any information of the surrounding nodes and members of the group. This protocol reduces the overhead by evading the redundant data transmission [6].

Multipath OLSR protocol is on the basis of OLSR, in which several paths are selected using multipath Dijkstra algorithm. This algorithm becomes flexible and extensible using several link metrics and cost functions, Route recovery and loop detection are used to obtain higher QoS. However, delay in

packet delivery varies on the basis of node dimension [7].

In a tree-based QoS multicast routing protocol, one source node searches the QoS paths to several destinations by dividing the network area into same-sized hexagonal cells. Moreover, a leader and alternate leader nodes are chosen for recording all the information of the network. Routing is proficiently performed for transmitting the data towards every receiver on the basis of node location. Based on the restricted directional flooding, the lost packet is resent only when the destination node is nearer to the resending node [8].

The routing algorithm uses Spiral Millipede-inspired Routing Algorithm (SMiRA). When this algorithm was weighted against AODV, conventional MANET routing protocol, routing overhead and fault recovery delay are reduced. However, this algorithm has high complexity in computation and energy overhead in its operation [9].

The link breakage prediction in MANETs is performed on the Dynamic Source Routing (DSR) protocol. This technique reduces the data loss and latency and creates several routes to the destination. When the initially used link fails to operate, alternate link will be chosen to the destination. It provides higher delivery rate and less routing overhead. The range for transmission varies when the node moves, thereby increasing overall delay and packet drop [10]. For MANETs, multicast routing protocol called as fuzzy logic-modified AODV routing protocol [11].

In this case, the distinct strategy is used to select stable backbone hosts (BH). The global positioning system estimates the amount of remaining connection time for two neighboring nodes. By using this, stable BHs are chosen with longer remaining connection time to the other hosts. In addition, a new multicast protocol depends on the selected stable BHs for choosing the stable multicast. However, the link quality of vehicular ad hoc networks is affected by some environmental factors, such as, microwaves, wall obstacles, and buildings [13].

In QoS-based multicast routing protocol for MANET, entropy of nodes is considered as an important parameter for determining a stable path. Bandwidth reservation mechanism is used in order to achieve some QoS requirements, and entropy of node and bandwidth reservation policy is used in order to find a stable link with sufficient bandwidth. However, the complexity of QoS-based multicast routing protocol is increased when the part of links is unidirectional [14].

The network coding-based multicast protocol in wireless network provides two schemes: static scheme for repeatedly retransmits one coding packet until all intended receivers receive it and a dynamic scheme to update the coding packet until one or more receivers receive it. This can encode packets with more general coding operations to encode lost packets with common intended receivers together to fully exploit the potential coding opportunities and to have polynomial-time complexity [15]. In order to give multiple optimal paths, the multiple metrics like hop count, battery life, and strength signal are considered with the aid of fuzzy logic. Nodes then stochastically forward data on these multiple paths, thereby performing automatic load balancing and fault tolerance operations [16].

This algorithm exchanges the routing information for some time and then stops working for certain time. But this information is used by each router for making its own routing recovery of the lost data using the Dynamic General-Coding-based (DGC) scheming decisions on the basis of intuitionistic fuzzy logic during this time [17]. The receiver-initiated fuzzy logic control method is mainly utilized for improving the performance of the network. This can be done by balancing the load among nodes [18]. This protocol can efficiently manage the energy weakness node and deliver the packets to destination with less number of dropped packets [19].

Each node gathers the position information of its neighbor's nodes by broadcasting one-hop beacon in a periodic manner. One-hop beacon has node ID and position information. All nodes in the network maintain a neighbor table to store the node ID and position of each neighbor [20].

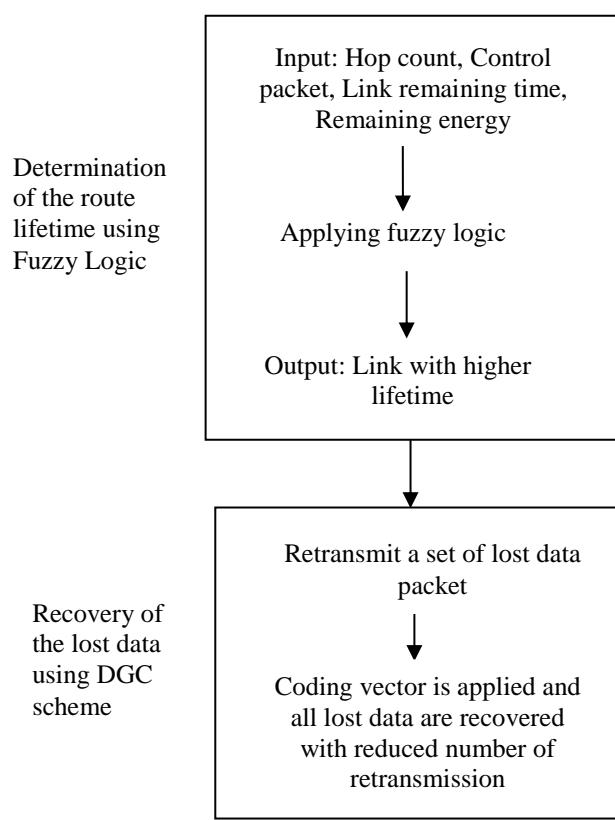


Fig.1. Block Diagram

III. OVERVIEW

The proposed design is a Mobility Aware Fault Tolerant Multipath Multicast Routing (MAFMMR) Protocol for MANET. In this the link remaining time metric is included in addition to the hop count, remaining energy and control message as input to the fuzzy logic [11] for determining the route lifetime. The link remaining time can be determined by the mobility prediction method given in [13]. For recovery of

lost packets, network coding [15] will be applied in selected multicast routes which will encode lost packet and also have polynomial time complexity. This scheme will improve lost packet buffer and number of multicast receivers.

A. Path selection

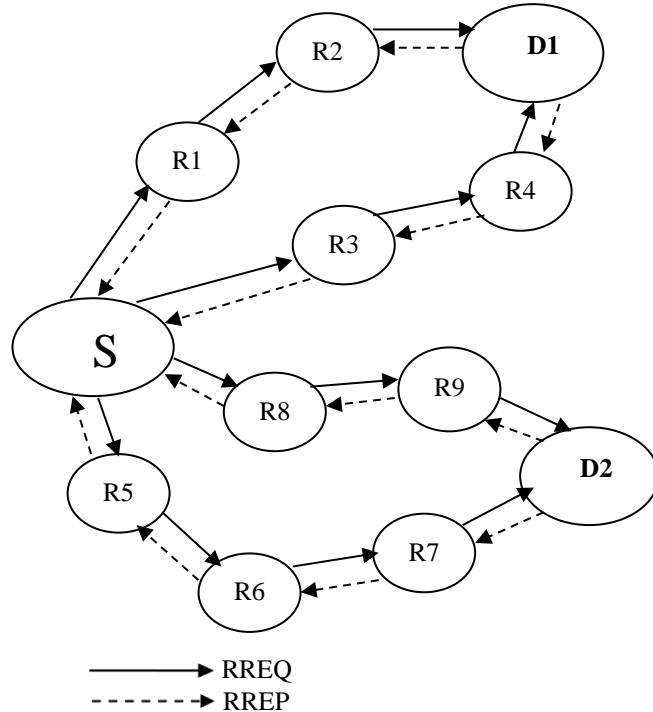


Fig.2. Route Request RREQ flooded by the source node S, forwarded by the intermediate nodes and Route Reply RREP and the two destination nodes D1 and D2.

B. Calculation of Link remaining time

The receivers of mobile nodes are equipped with a GPS, provides location, speed, and direction. Suppose two neighboring nodes are v_i and v_j , the remaining connection time between them is $t_{i,j}$. According to the mobility prediction method in [13], $t_{i,j}$ can be estimated as follows. Define (lx_i, ly_i) ((lx_j, ly_j)) as the location of v_i (v_j), s_i (s_j) as the speed of v_i (v_j), and θ_i (θ_j) as the moving direction of v_i (v_j), ($0 \leq \theta_i \leq 2\pi$, and $0 \leq \theta_j \leq 2\pi$). In addition, let $a = s_i \cos \theta_i - s_j \cos \theta_j$, $b = lx_i - lx_j$, $c = s_i \sin \theta_i - s_j \sin \theta_j$, and $d = ly_i - ly_j$. Then

$$t_{i,j} = \frac{-(ab + cd) + \sqrt{(a^2 + c^2) h^2 - (ad - bc)^2}}{a^2 + c^2} \quad (1)$$

Where h is the transmission range radius [13].

The two comparatively stable disjoint routes are selected by the source with higher remaining connection time $t_{i,j}$.

C. Stable Path Selection

- The source constructs the four basic evaluation criteria as Link Remaining time, Hop Count, SentCtrlPkt and EngyMin from the different routes [11].
- Membership functions for Hop Count and SentCtrlPkt are assigned to each candidate route.
- The membership functions for the rating value (EngyMin) and the converted rating value (RvEngy) are assigned to all candidate routes.
- Using the combined rule-base [11], calculate the combined suitability indices, then find the final fuzzy rating index, with the fuzzy suitability indices, rating of the possible alternative routes will be obtained.

D. Application of fuzzy logic

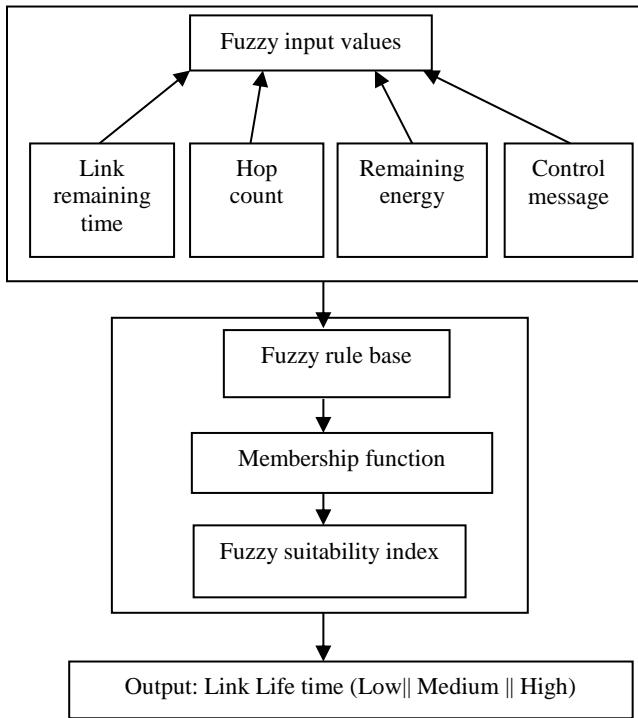


Fig.3. Determination of the route lifetime using the Fuzzy Logic

The membership functions for the input and output variables are shown in figures 4, 5, 6 and 7. The triangulation functions are used because of uncomplicated formulas and computational efficiency which are widely utilized in real-time applications. This design of membership function offers positive impact.

i) The Link Remaining time (LR) calculated is one of the important criteria to be considered, when calculating the Link Life time (LL). When the link remaining time is high, the probability for the link to be stable for longer period of time is

higher. Therefore, the time the path remains (Link Life time – LL) in the routing table will be larger.

The rules should be as follows:

- L1: If LR time is high, then LL is high.
L2: If LR time is medium, then LL is medium.

L3: If LR time is low, then LL is low.

Example: The link remaining time is
Low: 20 ms ~ 40 ms and 30 ms is the center.
Medium: 30 ms ~ 70 ms and 50 ms is the center.
High: 60 ms ~ 90 ms and 75 ms is the center.

Function

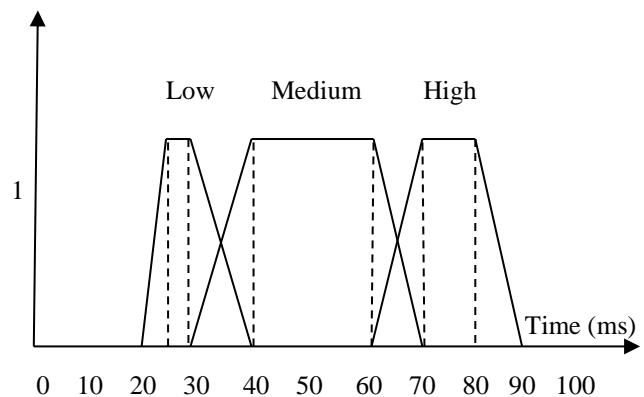


Fig.4. Membership functions for the link remaining time.

ii) Hop Count (HC) is an evaluation criterion (active time to present in the routing table) for Lifetime and is the number rating of nodes along the route between the source and destination. When the HC is high, because of node's mobility the probability of route broken is also high. Therefore, the time in which the path will remain in routing table (the lifetime) and it should be smaller, thus the rating of Lifetime (expressed by LL) will be given small similarly.

Consequently, the rules should be as follows:

H1: If HC is high, then LL is low.

H2: If HC is medium, then LL is medium.

H3: If HC is low, then LL is high.

The membership functions for HC and LL rating value are expressed with dimensionless index within [0, 1]. The LL is an inverse ratio to Hop Count. Example: The hop count is

Low: 0 ~ 10 and 5 is the center.

Medium: 5 ~ 20 and 12.5 is the center.

High: 15 ~ 40 and 27.5 is the center.

The power consumption rate is denoted by PC_i . Since the power consumption of a node is caused by the transmission, reception and overhearing of packet activities, the average energy consumption rate of node i is PC_i given by:

$$PC_i = \frac{(W_r \times M_r + W_s \times M_s + W_o \times M_o)}{T} \quad (2)$$

Function

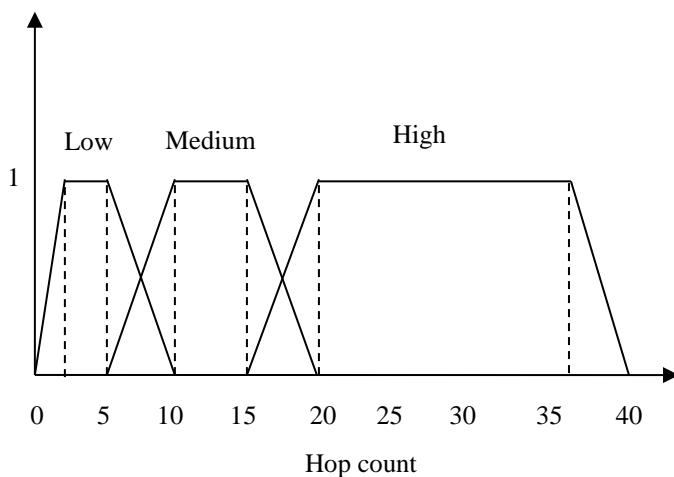


Fig.5. Membership function for the hop count

Where W_r , W_s and W_o are the power consumed by the network interface when the node i receives, sends and overhears a packet; M_r , M_s and M_o are the corresponding sizes of data packets respectively; The node i consumes its energy during the time period T [11]. RT_i is residual time for the node i to consume its energy, is calculated by:

$$RT_i = \frac{RP_i}{PC_i} \quad (3)$$

Where the remaining battery energy of the node i represented by RP_i . The route lifetime has a relationship with the minimum RT_i for all nodes in the path defined. That is if the energy of any node in the path is exhausted, then the complete path would crashes down.

Therefore, the lifetime of the route is related to $\min_{\forall n_i \in P} RT_i$

$$\text{Energy Minimum (EM)} = \min_{\forall n_i \in P} RT_i \quad (4)$$

The function for EM criterion should be considered as the dimensionless index (0, 1).

The link broken probability will be high if the EM as the low value. Thus, the rules for the relationship between Energy Min should be as follows:

- E1: If EM is high, then LL is high
- E2: If EM is medium, then LL is medium
- E3: If EM is low, then LL is low

Example: The remaining energy is

Low: $0.2 \text{ J} \sim 0.7 \text{ J}$ and 0.45 J is the center.
Medium: $0.5 \text{ J} \sim 1.0 \text{ J}$ and 0.75 J is the center.
High: $0.9 \text{ J} \sim 1.3 \text{ J}$ and 1.1 J is the center

Function

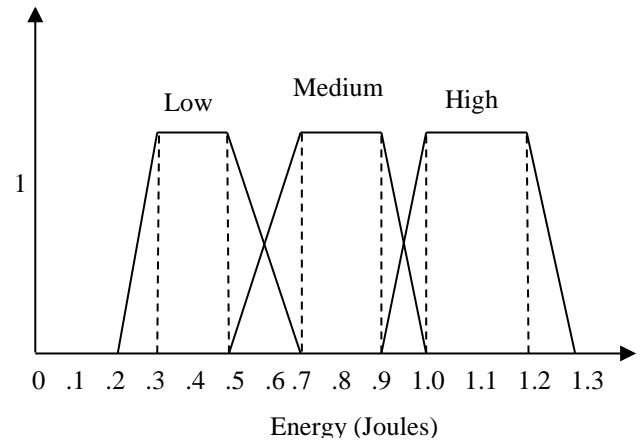


Fig.6. Membership function for the remaining energy

The control packet (CP) SntCtrlPkt is sum of the number of packets sent and packets received. It is also a valid factor for the evaluation of the LL of the route entry in the routing table. The link would probably break if the nodes move frequently beyond the communication range, increases the control packets. The shared bandwidth of channels would be reduced, if route is congested, due to the retransmission of the lost packets route become unstable. The control packets are: HELLO, RREQ, RREP, RERR and RREP_ACK. If the route is probably unstable, RREP packet will records the number of sending control packet to the intermediate nodes, so more number of these recorded control packets means high probability to lose some of its current links or packets.

Function

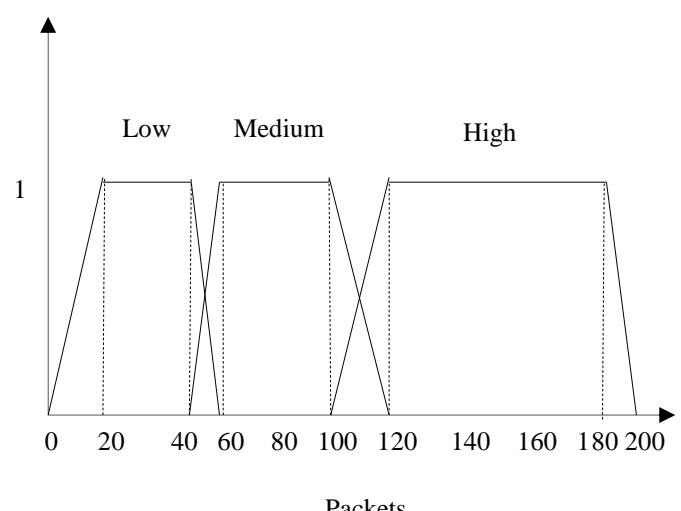


Fig.7. Membership function for the control message

The rules for the relationship between SntCtrlPkt and LL are:

N1: If CP is high, then LL is low.

N2: If CP is medium, then LL is medium.

N3: If CP is low, then LL is high.

Similarly, The CP rating value is expressed within [0, 1] as dimensionless index and the LL value is an inverse ratio to CP value.

Example: The lifetime is

Low: 0 ~ 60, and 30 is the centre.

Medium: 40 ~ 120, and 85 is the centre.

High: 100 ~ 200, and 150 is the centre.

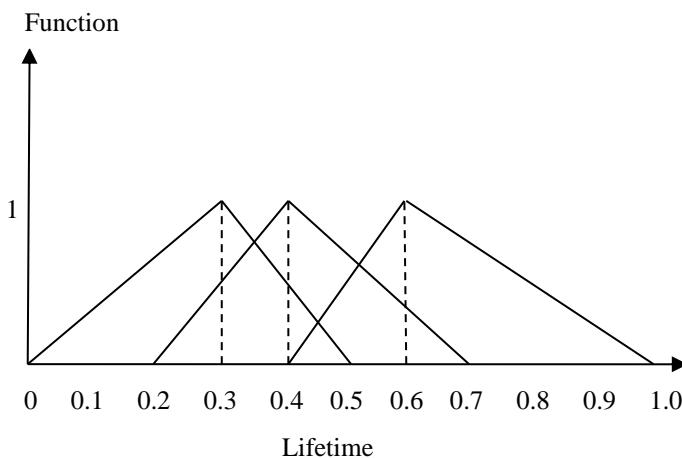


Fig.8.Membership functions for linguistic rating values: Low (0, 0.3, 0.3, 0.5), Medium (0.2, 0.4, 0.4, 0.7) and High (0.4, 0.6, 0.6, 1)

SL No	Hop Count HC	Control Packet CP	Energy Minimum EM	Link Remaining time LR	Link Life time LL
1	L	L	H	H	H
2	M	M	M	M	M
3	H	H	L	L	L
4	L	L	L	L	M
5	H	H	H	H	M
6	L	L	M	M	H M
7	H	H	M	M	L M
8	M	M	L	L	L M
9	M	M	H	H	H M

Table 1.Fuzzy rules for determining the output

The membership functions which corresponds to each element in the linguistic set (link remaining time, Hop Count, SntCtrlPkt, EngyMin and Lifetime) is defined. We have presented the method to design its membership functions. The criteria rating that can be assessed by linguistic terms

(dimensionless index) for example Low (L), Medium (M) and High (H). The linguistic rating scale applied is illustrated in Fig. 4, 5, 6 and 7, and the membership functions of the five linguistic values are shown in Fig. 8.

The selected optimal routes will have higher route lifetime in the routing table. Once the optimal routes are selected, the source node then starts multicasting data packets through these paths. If the data packet gets lost during transmission, then it is recovered using the Dynamic General-Coding-based (DGC) scheme as explained below.

E. Lost Packet Recovery

The Dynamic General-Coding-based (DGC) scheme [15] consists of the transmission phase and retransmission phase. The DGC scheme uses a simple algorithm to find the set of lost packets for encoding. For each retransmission the encoded packet is dynamically updated such that the potential coding opportunities can be exploited more effectively.

- For data recovery, the source retransmits a set of packets, out of all the packets lost.
- At the receiver, it checks whether the coding vector set for the encoded packet is equal to the set of retransmitted packet.
- If it is not equal, then the retransmitted packet set remains unchanged, similar to the previous transmission.
- If it is equal and each packet received belongs to the retransmitted packet set then the record is updated as all the missing packets have been recovered.
- If any packet received belongs to the retransmitted packet set and is also recorded. Then in every receiver, remove the entry corresponding to the packet from the coding vector. If there is no coding vector available, then remove the packet from the retransmitted packet set.
- Each packet in the set of lost packets is checked to see if it has never been recorded as received in any of the receiver, if so then this packet is added into the retransmitting packet set and removed from the set of lost packets and then updated at the receiver. Coding vector is applied at every receiver, whenever the vector set is smaller than the retransmitted packet set.
- Thus all the data packets get recovered eventually with reduced number of retransmissions.

F. Overall steps involved in MAFMMR Protocol

- Source floods Route request packets to determine the possible routes to the destination and based on the received route reply from the destination node, the source records the input parameter information:

- Hop count, remaining energy and control packets.
- The input: link remaining time is calculated based on [11].
- Fuzzy rules are applied to determine the link lifetime.
- Based on the fuzzy logic results, few stable routes to the destination are selected with higher link lifetime. Dynamic General-Coding scheme is used to recovery of lost packet.

IV. SIMULATION RESULTS

A. Simulation Parameters

Mobility Aware Fault-tolerant Multipath Multicast Routing (MAFMMR) Protocol is evaluated using NS-2. We use a bounded region of 1500 m x 300 m, in which nodes are placed using a uniform distribution. The number of nodes is 50. The nodes power levels are assigned in such way that the transmissions range as 250 meters. Simulation time is 50 Sec, packet size as 512 bytes. The channel capacity of mobile hosts is set to 11 Mbps. We use the Distributed Coordination Function (DCF) of IEEE 802.11 for wireless LANs as the Medium Access Control (MAC) layer protocol. The simulated traffic is Constant Bit Rate (CBR).

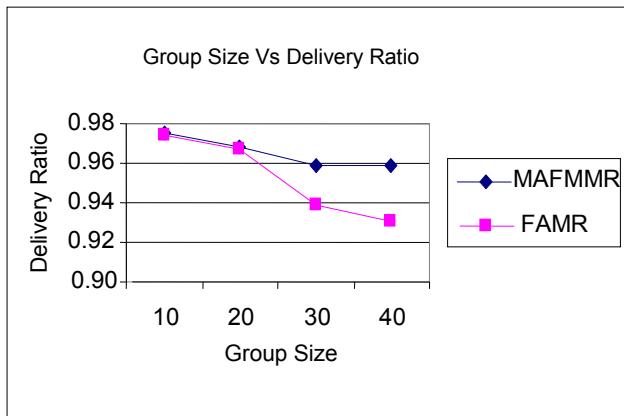


Fig.9. Group Size Vs Delivery Ratio

B. Performance Metrics

The performance of proposed MAFMMR protocol is compared with Fuzzy Logic Modified AODV routing (FAMR) protocol [11]. The evaluation performance is according to the following metrics

C. Results

Based on Group Size

The group size or the numbers of group members is varied from 10 to 40 with speed 10 m/s.

Fig no 9 shows that both MAFMMR and FAMR performance is almost same for only for less number of nodes. Since MAFMMR chooses stable routes by measuring the link remaining time, it minimizes the packet losses due to mobility

and disconnections. Moreover, the packet losses can be recovered by means of network coding, thereby increasing the delivery ratio. Hence MAFMMR outperforms FAMR in terms of delivery ratio by 2%,

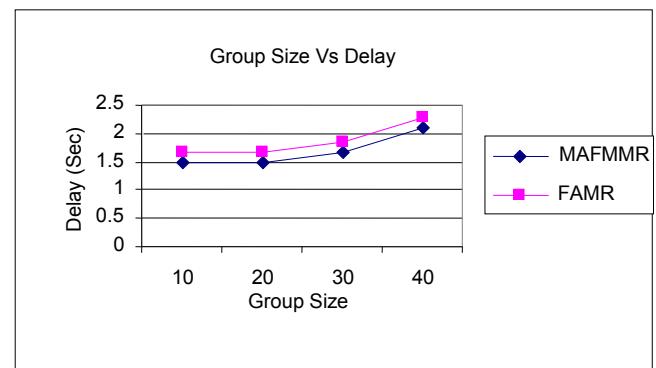


Fig.10. Group Size Vs Delay

Fig 10 represents the delay as a function of group size. It was observed that as the group size increases, the data traffic will be more leading to more congestion and hence the delay increases linearly. However, since MAFMMR chooses stable routes for data transmission, it reduces the rerouting and retransmission delay. Hence it has 10% reduced delay when compared to FAMR.

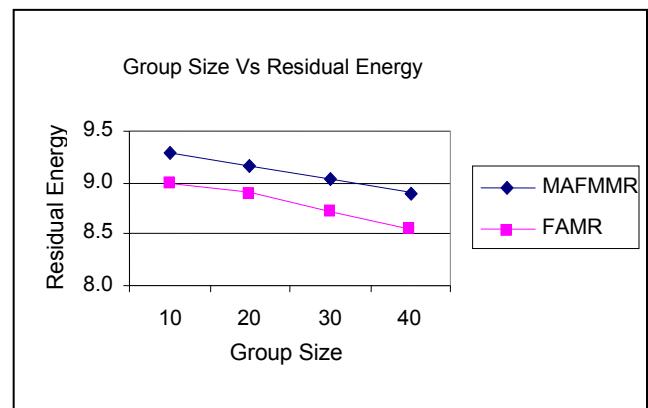


Fig.11. Group Size Vs Residual Energy

Fig no 11 shows that group size as a function of residual energy. Nodes which are having lower remaining energy are not participating at time of communication. The nodes which are selected for routing path have higher remaining energy in MAFMMR than FAMR. The MAFMMR outperforms over the FAMR in terms of residual energy by 3%.

D. Based on Speed

The mobile node speed is varied from 5 m/s to 25 m/s for the group size of 10 members.

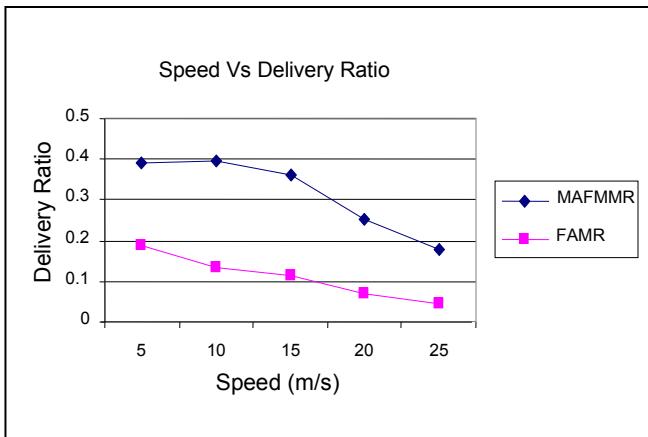


Fig.12. Speed Size Vs Delivery ratio

Fig no 12 shows results of packet delivery ratio when the node speed is increased. If the speed of the nodes increases the delivery ratio decreases, because of the route disconnections due to mobility. Since MAFMMR chooses stable routes by measuring the link remaining time, it minimizes the packet losses due to mobility and disconnections. Moreover, the packet losses can be recovered by means of network coding, thereby increasing the delivery ratio. Hence MAFMMR has 64% higher delivery ratio when compared to FAMR.

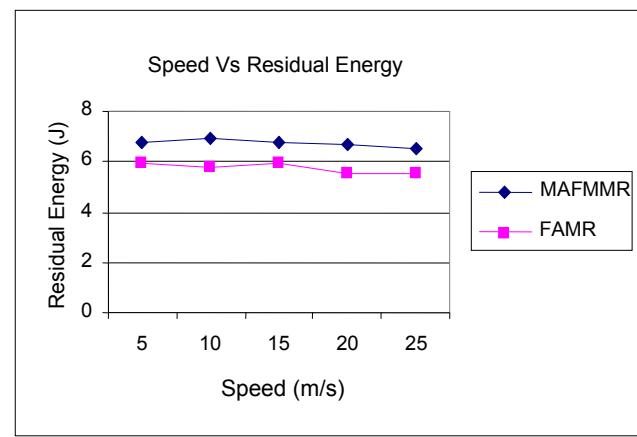


Fig.14. Speed Vs Residual energy

Fig.14 shows the speed is the function of residual energy. The energy left after the packet transmission at every node is the remaining energy. The amount of energy available decreases with increased mobility causes increased number of connection. The nodes which are selected for routing path have higher residual energy in MAFMMR than FAMR. We can see that MAFMMR outperforms FAMR in terms of residual energy by 14%.

V. CONCLUSION

In this paper, we propose to develop a multipath multicast routing protocol for MANETs that works efficiently by selecting more than one path with higher lifetime. This protocol considers the link remaining time, hop count remaining energy and control message in order to determine the route lifetime using the Fuzzy Logic. The link remaining time is determined based on the mobility prediction method. In this paper, we also propose to recover the lost data packet by using the Dynamic General-Coding-based (DGC) scheme. By simulation, results the proposed routing protocol provides fault-tolerance communications in terms of increased packet delivery ratio and reduced delay and energy.

REFERENCES

- [1] Rakesh Kumar Sahu, RekhaSaha and Narendra S. Chaudhari, “Fault Tolerant Reliable Multipath Routing Protocol for Ad hoc Network”, 2012 Fourth IEEE International Conference on Computational Intelligence and Communication Networks, November 2012.
- [2] Ranjeet Kaur, Rajiv Mahajan and Amanpreet Singh, “A Survey on Multipath Routing Protocols for MANETs”, International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 2,ISSN 2278-6856, Issue 2, March – April 2013.
- [3] D.Maheshwari and A.Dhanalakshmi, “Fault Tolerance in Mobile ad hoc Network: A Survey”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, ISSN: 2277 128X,Issue 3, March 2013.
- [4] Yut aka Hat anaka, Masahide Nakamura, Yoshiaki Kakuda and

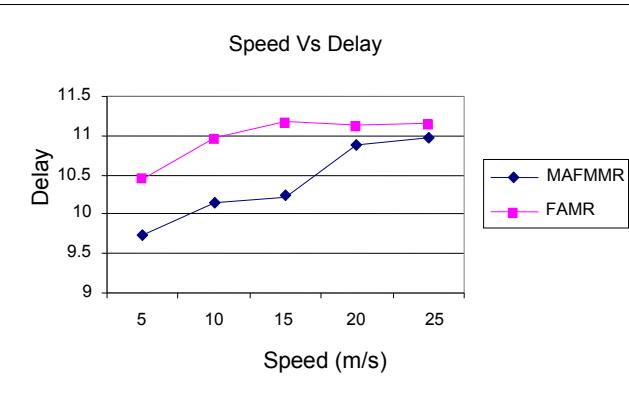


Fig.13. Speed Vs Delay

From fig 13 it is obvious that MAFMMR have lower delay then FAMR. As the mobility decreases the delay also decreases due to less route failures. As the mobility increases route failure increases and have an impact on delay. As the no de speed increases, the delay also increases due to rerouting of packets. since MAFMMR chooses stable routes for data transmission From the figures, the MAFMMR outperforms over the FAMR in terms of delay by 6%.

- TohruKikuno, "A Synthesis Method for Fault-tolerant and Flexible Multipath Routing Protocols", Engineering of Complex Computer Systems, 2007. Proceedings Third IEEE International Conference on 2007.
- [5] B. John Oommen and Sudip Misra, "Fault-Tolerant Routing in Adversarial Mobile Ad hoc Networks: An Efficient Route Estimation Scheme for Non-Stationary Environments", Telecommunication Systems, Volume 44, Issue 1-2, pp 159-169, June 2010.
- [6] Ozsnur Ozkasap a, Zulkuf Genc b and Emre Atsan, "Epidemic-Based Reliable and Adaptive Multicast for Mobile Adhoc Networks", Computer Networks Volume 53, Issue 9, pages: 1409–1430, 2009.
- [7] Jiazi Yi, Asmaa Adnane, Sylvain David and Benoît Parrein, "Multipath Optimized Link State Routing for Mobile Adhoc Networks", Ad Hoc Networks, Volume 9, Issue 1, Pages 28–47, January 2011.
- [8] Mohammad M. Qabajeh, Aisha H. Abdalla, Othman Khalifa and Liana K. Qabajeh, "A Tree-based QoS Multicast Routing Protocol for MANETS", IEEE 4th International Conference on Mechatronics (ICOM), Pages: 17-19, May 2011.
- [9] Olufemi Adeluyi and Jeong-A Lee, "SMiRA: A Bio-Inspired Fault Tolerant Routing Algorithm for MANETs", ICT Convergence (ICTC), 2012, IEEE, International Conference, October 2012.
- [10] Khalid Zahedi and Abdul Samad Ismail, "Route Maintenance Approach for Link Breakage Prediction in Mobile Ad Hoc Networks", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No. 10, 2011.
- [11] Bey-Ling Su, Ming-Shi Wang and Yueh-Ming Huang, "Fuzzy Logic Weighted Multi-Criteria of Dynamic Route Lifetime for Reliable Multicast Routing in Adhoc Networks", Elsevier, Expert Systems with Applications, Volume 35, Issues 1–2, Pages: 476–484, August 2008.
- [12] Tzu-Chiang Chiang, Chan-Yu Hsu and Jia-Lin Chang, "Immediate Group ACK tree (IGA) for Reliable Multicast in Mobile Ad Hoc Networks", IEEE 3rd International Conference on Communication Software and Networks (ICCSN), Page(s): 483 - 487, May 2011.
- [13] Chia-Cheng Hu, Eric Hsiao-Kuang Wu and Gen-Huey Chen, "Stable Backbone Hosts and Stable Multicast Routes in Two-Tier Mobile Ad Hoc Networks", IEEE Transactions on Vehicular Technology, Vol. 58, No. 9, Pages: 5020 - 5036, November 2009.
- [14] Zheng Sihai,Li Layuan and Guo Lin, "QoS-Based Multicast Routing Protocol in MANET", IEEE International Conference on Industrial Control and Electronics Engineering, Pages: 262 - 265, August 2012.
- [15] Kaikai Chi, Xiaohong Jiang and Susumu Horiguchi, "NetworkCoding-Based Reliable Multicast in Wireless Networks", Elsevier, Computer Networks, Volume 54, Issue 11, Pages 1823 -1836, August 2010.
- [16] Raju V Daraskar M M Goswami, "Intelligent Multipath Routing Protocol for Mobile Adhoc Networks", International Journal of Computer Science and Application Vol 2, No 2, Nov/Dec 2009.
- [17] Ashit Kumar Datta and Abdul Rahman Wahab Sait " An Application of Intuitionistic Fuzzy in Routing Networks" International Journal of Advanced Computer Science and Applications Vol,3,No.6,2012,Page; 131-135.
- [18] Ming-Chang Haung, S Hossein Hossini and K Vairan " A Receiver-Initiated Load Balancing Method in Computer Networks Using Fuzzy Logic Control" IEEE International Conference GLOBECOM,2003, Page:4028-4033.
- [19] P. Manickam and D Manimegalai "A Highly adaptive fault tolerant routing Protocol for Energy Constrained Mobile Adhoc Networks" Journal of Theoretical and Applied Information Technology November 2013, Vol 57, No 3 Page; 388-397.
- [20] V Jayalakshmi and R Rameshkumar " Multipath Fault Tolerant Routing Protocol for MANET" International Journal on Adhoc networking Systems Vol, 2 No,1, January 2012 Page; 23-34.
- [21] P. Sander, S. Egner, L. Tolhuizen, Polynomial time algorithms for network information flow, in Proceedings of the 15th ACM Symposium on Parallel Algorithms and Architecture, San Diego, 2003.

Fully homomorphic encryption: state of art and comparison

Ahmed EL-YAHYOUI and Mohamed Dafir ELKETTANI

Information Security Research Team, CEDOC ST2I ENSIAS, Mohammed V University in Rabat, Rabat,
Morocco

Abstract

Fully homomorphic encryption (FHE) is an alternative of cryptography that allows evaluating arbitrary functions on encrypted data without the need for decryption of ciphertexts. In this article we present the state of the art of fully homomorphic encryption schemes. In particular we present a classification of several existent FHE schemes followed by a comparison of performances and complexity of these cryptosystems. Finally we will give different possible axes of research in the conclusion.

Keywords: cryptosystem, fully homomorphic, cloud, bootstrappability, modulus reduction, key changing.

I. INTRODUCTION

The rise of cloud computing and outsourcing of data storage increased the need for privacy and security of sensitive informations. Computing on encrypted data without decryption is a magic solution for this problem. Rivest et al conjectured this way of encryption in 1978 in their article entitled ‘on data bank and privacy homomorphism’ [1]. This new concept is what we call today Fully Homomorphic Encryption (FHE). Their conjecture resisted over three decades and remained the most important dream for all cryptographers. In 2009 Craig Gentry presented a breakthrough work solving the theoretical problem of constructing a FHE scheme [14], his genious idea consist of using a technique of refreshing noisy ciphertexts called ‘bootstrapping’. Ever since its first plausible secure construction, FHE has gained increasing attention from cryptographers.

A faster public key FHE scheme is strongly required today to promote security in cloud computing. The majority of works that followed after have inspired from the Gentry’s framework for designing FHE, other ideas and other frameworks have appeared later, but despite these advances, there remains much work to cryptographers to make these cryptosystems practical.

In this work, we will present the state of art of fully homomorphic encryption schemes that exist today (at the time of writing this article). Firstly, we will start by defining what a FHE is. Secondly, we will present

different noise management techniques used in homomorphic encryption. Thirdly, we will explain the link between symmetric and asymmetric encryption schemes besides we will present a set of mathematical problems that inspire cryptographers to build a FHE scheme. Fourthly, we will detail the body section of our article about the classification and comparison of FHE schemes. After we will give an overview about the implementation and testing of FHE schemes and finally we will finish with a conclusion containing research runways.

II. DEFINITIONS

A. Somewhat homomorphic encryption

Computing on encrypted data is guaranteed by homomorphic encryption cryptosystems. Sometimes we are not able to do any operation on ciphertexts, but just a category or a limited number of computations. These types of cryptosystems are supposed to be somewhat homomorphic encryption schemes (SWHE). We can classify SWHE schemes to three categories as follows:

Additively homomorphic encryption schemes: give ability to do limited or unlimited additions on encrypted data. As an example we can cite Goldwasser-Micali [2], Benaloh[3], Naccache-Stern[4], Okamoto-Uchiyama[5], Paillier[6], Damgård-Jurik[7], and SCHMIDT-SAMOA-TAKAGI[8]’s encryption schemes.

Multiplicatively homomorphic encryption schemes: give ability to do limited or unlimited multiplications on encrypted data. Historically the most famous examples in this sense are: RSA[9], ELGAMAL[10] and Sander-Young-Yung[11]’s encryption schemes.

Pseudo-homomorphic encryption schemes: A cryptosystem is said pseudo-homomorphic if it allows calculating both addition and multiplication on encrypted data, but in a limited way. In specific terms, these schemes

permit an unlimited additions and a bounded number of multiplications on ciphertexts. The BGN[12] cryptosystem was the first algorithm that allows to compute both addition and multiplication on ciphertexts. Addition is allowed a multitude of times while multiplication is possible only once. A second example of pseudo-homomorphic encryption schemes is Melchor-Gaborit-Herranz[13]'s schemes. It allows calculation on ciphertexts through multivariate polynomials of degree d . This is a cryptosystem d -multiplicative fully homomorphic, i.e. it allows d multiplications and an unbounded number of additions on encrypted data.

B. FHE schemes

A FHE scheme is a quadruplet of algorithms (Gen, Enc, Dec, Eval) such that:

- $\text{Gen}(\lambda)$: Is an algorithm of key generation , takes as input a security parameter λ and outputs a public and secret keys (pk, sk) .
- $\text{Enc}(m, pk)$: Is an encryption algorithm, takes as input a plaintext m and a public key pk and outputs a ciphertext c .
- $\text{Dec}(c, sk)$: Is a decryption algorithm, takes as input a ciphertext c and a secret key sk and outputs a plaintext m .

$\text{Eval}(C, c_1, \dots, c_n)$: Is an evaluation algorithm, takes as input a circuit C and ciphertexts c_1, \dots, c_n and verify $\text{Dec}(\text{Eval}(C, c_1, \dots, c_n), sk) = C(m_1, \dots, m_n)$. Anyone can evaluate Eval, since it does not require the secret key sk .

C. Techniques of noise reduction

In order to obtain homomorphic properties, the majority of FHE cryptosystems designed until now add noise to plaintext during encryption. The homomorphic evaluation amplifies noise and increases the margin of error. The error keeps growing until it is impossible to perform any more homomorphic evaluations or makes decryption impossible. To reduce the increased noise in the ciphertext, several techniques exist:

Gentry's bootstrapping

Gentry's bootstrapping [14] is a technique to "refresh", periodically, ciphertexts associated to interior nodes of a circuit, we can update for any number of levels in a circuit, and can therefore evaluate circuits of arbitrary depth.

To refresh a ciphertext which encrypts a plaintext π with a public key pk_i of a scheme \mathcal{E} , we re-encrypt it with pk_{i+1} and we apply, homomorphically, decryption circuit to the result, using the secret key sk_i which is encrypted

by pk_{i+1} , thereby obtaining a ciphertext of π under pk_{i+1} . Homomorphically evaluating the decryption circuit decrypts the inner ciphertext under pk_i , but within homomorphic encryption under pk_{i+1} . The implicit decryption "refreshes" the ciphertext, but the plaintext is never revealed; at least one layer of encryption always covers the plaintext. Now that the ciphertext is refreshed, we can \continue" correctly evaluating the circuit.

Modulus reduction

The bootstrapping technique of Gentry [14] for noise management is very cost in practice, because it must be called after each multiplication. To avoid these disadvantages, Brakerski and Vaikuntanathan introduced a new noise management procedure[21], called modulo reduction. This technique consist of reducing the noise by converting a ciphertext modulo q into another ciphertext modulo q' such that $q' < q$. The noise will be reduced by a factor q/q' .

Key changing

This technique [21] permits to transform a ciphertext c_1 under a key s_1 to another ciphertext c_2 under a second key s_2 such that c_1 and c_2 encrypt the same plaintext.

III. HOMOMORPHIC ENCRYPTION: LINK BETWEEN SYMMETRIC AND ASYMMETRIC SCHEMES

A homomorphic encryption algorithm can be symmetric with one encryption/decryption key, as it can be asymmetric with two keys. The study of the state of the art FHE cryptosystems shows that cryptographers focus on the design of asymmetric FHE more than symmetric FHE. Indeed, the first FHE scheme designed by Gentry was asymmetric [14] and the number of existing asymmetric FHE schemes exceeds it's of symmetric FHE. This favouring of the asymmetric is justified by the importance of such schemes in practice. Moreover, it attracts the attention of researchers to find a link between symmetric FHE scheme and asymmetric FHE scheme.

To switch from a public key FHE scheme to a private key FHE scheme is considered trivial. Intuitively, an asymmetric scheme can became symmetric by keeping secret its two keys.

Concerning the switching from symmetric to asymmetric, Ron Rothblum[34] found a generic transformation which switch a homomorphic private key cryptosystem into a homomorphic public key cryptosystem, this transformation is only valid for cryptosystems whose plaintext space is $\{0,1\}$.

IV. UNDERLYING MATHEMATIC PROBLEMS TO HOMOMORPHIC ENCRYPTION

With the revival of homomorphic encryption, traditional mathematical problems such as factoring, discrete logarithm ... begin to disappear and be used less than before (for this axis of cryptography). Indeed, most robust new assumptions have emerged recently and become very promising. Among these assumptions, we find:

A. Euclidean lattice's problems

An Euclidean lattice is a subgroup of \mathbb{R}^n which is isomorphic to \mathbb{Z}^n , and which spans the real vector space \mathbb{R}^n . Rigorously, for any basis of \mathbb{R}^n , the subgroup of all linear combinations with integer coefficients forms a lattice \mathcal{L} . i.e $\mathcal{L} = \mathbb{Z}b_1 \oplus \mathbb{Z}b_2 \oplus \dots \oplus \mathbb{Z}b_n$ where (b_1, b_2, \dots, b_n) is a basis of \mathbb{R}^n . The most used Euclidean lattice problems in cryptography are:

SVP: the Shortest Vector Problem

Given a basis B of a lattice \mathcal{L} , the SVP problem consist of finding a non-zero vector $v \in \mathcal{L}$ such that $\forall x \in \mathcal{L}\{0\}$ we have $\|v\| \leq \|x\|$.

CVP: the Closest Vector Problem

Given a basis B of a lattice \mathcal{L} and a target vector $t \in Vect(\mathcal{L})$, the CVP problem consist of finding a non-zero vector $v \in \mathcal{L}$ such that $\|v - t\| \leq dist(t, \mathcal{L}(B))$.

SSSP: the Sparse Subset Sum Problem

Given a set S of size $|S| = n$ and a target t , the SSSP problem consist of finding a subset $S' \subset S$ of size $s \ll n$ such that $\sum_{x_i \in S'} x_i = t$.

These problems are proved difficult to resolve. There are other problems on euclidean lattices, but these three are the most applied in homomorphic cryptography.

B. The AGCD (Approximate Greatest Common Divisor) problem and its variants

n is a security parameter.

Given a list of approximate multiples of a hidden odd integer p : $\{b_i = a_i p + e_i : a_i \in \mathbb{Z}_+, e_i \in \mathbb{Z}, |e_i| < 2^{n-1}\}_{i=0}^{\tau}$, find p .

MAGCD is the matrix variant of the problem AGCD, and reads as follows:

Given a list of matrices $\{B_i = AR_i + E_i \in \mathbb{Z}_p^{n \times n} : R_i, E_i \in \mathbb{Z}^{n \times n} \text{ and } \det(A) = p, \|p \cdot A^{-1} E_i\|_{\infty} < p/2\}_{i=0}^{\tau}$, find A .

C. The GLWE (General Learning with Error) problem

λ Is a security parameter, $n = n(\lambda)$ is an integer dimension, $f(x) = x^d + 1, d = 2^k$ is a cyclotomique polynomial such that $k \in \mathbb{N}$, $q = q(\lambda) \geq 2$ is a prime modulo, $\mathcal{R} = \mathbb{Z}[x]/f(x)$, $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$ and $\chi = \chi(\lambda)$ is a distribution on \mathcal{R} of standard deviation σ .

The GLWE problem is to distinguish distributions $(a_i, b_i = \langle a_i, s \rangle + e_i) \in \mathcal{R}_q^{n+1}$ and $(a_i, r) \in \mathcal{R}_q^{n+1}$ such that $a_i, s \in \mathcal{R}_q^n, e_i \leftarrow \chi$ and $b_i \in \mathcal{R}_q$.

The LWE problem is corresponding to GLWE problem instantiated with $d = 1$, while for Ring-LWE, we choose $n=1$.

V. CLASSIFICATION AND COMPARISON OF FULLY HOMOMORPHIC CRYPTOSYSTEMS

A. Schemes based on Euclidean lattices problems

Gentry's scheme:

In 2009, Gentry's thesis [14] gave rise to the first FHE scheme. Its security is based on the Euclidean lattices. This cryptosystem encrypts messages belonging to the clear space $\{0, 1\}$, by adding noise (error), while decryption consist of removing the error. The ciphertext of a cleartext is $c = m + kI$ where I is an ideal of a ring R and $e = kI$ is a noise associated to the clear. Homomorphic properties are trivial, given tow ciphertexts $c_1 = m_1 + k_1 I$ and $c_2 = m_2 + k_2 I$, we have $c_1 + c_2 = m_1 + m_2 + (k_1 + k_2)I$ and $c_1 \cdot c_2 = m_1 \cdot m_2 + (m_2 \cdot k_1 + m_1 \cdot k_2 + k_1 \cdot k_2)I$.

Gentry's scheme can be summarized into three main stages:

- Somewhat Homomorphic Encryption Scheme (SWHE): Gentry started from a scheme said SWHE or simply homomorphic which supports a limited number of homomorphic multiplications.
- Squashing the decryption circuit: Gentry reduces the complexity of the decryption circuit by issuing a set of vectors whose sum of a part of them is equal to the secret key. This scheme called 'squashed' can evaluate, in addition to its SWHE capacity, a NAND gate. This step cost him a security assumption: is the assumption of the robustness of the SSSP problem.
- Bootstrapping: This procedure involves the evaluation of the decryption circuit plus the NAND port to obtain a scheme called 'levelled' FHE for evaluating any circuit with a depth defines the circuit at the start. The scheme becomes bootstrappable and therefore it can be converted easily into a cryptosystem FHE.

Smart-Vercautern's scheme :

By following the same steps as Gentry, Smart and Vercautern have designed a new cryptosystem based on euclidean lattices [15], this scheme uses the same cleartext space as Gentry's (ie {0,1}) and also gives the possibility of extending the space such that the cleartext will have a size N instead of a single bit. The advantage of this cryptosystem is its small key and ciphertexts sizes compared to Gentry's scheme, but there's always the problem of accumulation of noise in ciphertexts and the slowness of the scheme.

Chunsheng's version:

In [20], Chunsheng started from the same algorithm as Smart and Vercautern and built a new refreshment algorithm by following Gentry's framework but without making use of the SSSP assumption.

Improved Gentry's scheme:

Stehle and Steinfeld [35] presented two improvements of Gentry's scheme: first they posed other conditions when selecting SSSP settings to enhance the semantic security of the algorithm, secondly They introduced a probabilistic decryption algorithm which can be implemented with a small multiplicative degree of algebraic circuit. Combined together, these improvements lead to a faster fully homomorphic scheme.

SIMD Gentry, 2011:

The Gentry's scheme [14] performs operations on a clear of 1-bit length. Therefore, it is intuitive to think that some operations may be performed on several bits in parallel to reduce the runtime. In [15], Smart and Vercautern indicated that the style of SIMD operations (Single Instruction, Multiple Data) on the data can be supported by their scheme. In [36], Smart and Vercautern show how to select parameters for the implementation of SIMD operations for the Gentry and Halevi's scheme [37]. The main point is that the SIMD version is 2.4 times faster than the standard FHE pattern and the ciphertext size is reduced by a factor of 1/72. Thus, by exploiting the parallelism in algorithms constituent we can ameliorate the efficiency of a scheme.

Gentry-Halevi's scheme:

This scheme [37] uses a hybrid approach to design a FHE scheme. This method is based on the use of a SWHE algorithm and another algorithm MHE (multiplicatively homomorphic Encryption) as ElGamal to evaluate the multiplication, provided that they are chimerically

compatible. This approach eliminates the concern for squashing step that costs an assumption more (the SSSP assumption).

Gentry-Helevi-Smart 2011:

In this article [38], the authors present a simple approach to bypass the homomorphic evaluation of the reduction of an integer modulo another, using a modulus very close to a power of two. This method is easier to describe and implement and seems to be faster in practice. In some cases, it also stores the encryption of the secret key as an encrypted text only, thereby reducing the public key size. This method can also be combined with homomorphic SIMD computation techniques.

B. Schemes based on the AGCD problem

The DGHV's scheme 2010:

Based on the Gentry's bootstrappability technique, van Dijk, Gentry, Halevi and Vaikuntanathan presented a new approach [16] to construct a FHE. The major contribution of this scheme is its simplicity: its operations are done on integers instead of euclidean lattices. However, because of the size of adopted parameters, it isn't applicable in its original version. Its security is based on the AGCD problem.

Coron-Mandal-Naccache-Tibouch's improvement:

In 2011, Coron et al [26] gave a method to reduce the key size of SWHE from $\tilde{O}(\lambda^{10})$ to $\tilde{O}(\lambda^7)$. The idea is to store only a small subset of the public key, and then generate a complete public key by combining, multiplicatively, the elements of the small subset. The new scheme is also semantically secure, but under a stronger variant of the AGCD hypothesis.

Chunsheng's scheme:

In [17] Chunsheng presented a FHE scheme based on the MAGCD problem. It is a new framework for designing robust FHE cryptosystems but remains an open problem.

Batch DGHV:

In 2013, Coron et al [39] extended the DGHV scheme to support encryption and homomorphic processing on bit-vectors of cleartext. It's done in a single ciphertext, this is called batch DGHV. The batch DGHV scheme can encrypt $l = \tilde{O}(\lambda^2)$ bits in a single ciphertext. The semantic security is maintained in this scheme. In addition, given the ciphertext and the public key, it allows arbitrary permutations on the underlying cleartext vector. Although

there is no significant progress in efficiency at this cryptosystem, it presents a new approach to obtain the characteristics of LWE-based FHE in an AGCD-based scheme.

Kim-Lee-Yun-Cheon's scheme:

Based on the Chinese remainder theorem and drawing from [1] and [16], Kim et al [30] have developed a FHE scheme that deals with cleartext $m = (m_1, \dots, m_k)$ such that $m_i \in \mathbb{Z}_{Q_i}$, which allows to support SIMD operations and reduces the runtime. Furthermore, this scheme is very simple.

C. Schemes based on the LWE problem

The BV's scheme:

In [21], the authors introduce a new approach to construct FHE schemes, it's the re-linearization technique. This technique allows making fully homomorphic a SWHE scheme, while the noise is managed by the modulus switching technique, so we will never need to use the Gentry's bootstrapping technique. This scheme reduces the size of ciphertexts and the decryption complexity, its security is based on the LWE problem.

The BGV's scheme:

Following the same ideas of [21], Brakerski et al [22] designed the BGV scheme. The major contribution of this cryptosystem is the refinement of the technique of modulus reduction to better manage noise in ciphertexts. Also this contribution allows them to get rid of the evaluation key used in [21]. This cryptosystem no longer requires the bootstrapping technique, but its authors introduce it at the end of the article as a kind of optimization.

Brakerski's scheme:

Based on the Regev's cryptosystem [40], Brakerski proposed a new FHE scheme [23]. This cryptosystem allows encrypting messages from the most significant bit of the ciphertext, rather than least significant as in previous homomorphic schemes. The resulting scheme has a number of interesting properties:

- Scale invariance.
- It does not require modulus switching.
- There is no restriction on the modulus.
- There is no restriction on the secret key distribution.
- There is a classical reduction from GapSVP.

Fan-Vercautern's scheme:

Vercauteren and fan [24] have taken over the scheme of Brakerski [23] and transposeed the underlying problem from LWE Ring-LW proven more secure. The authors also introduced two optimized versions for ciphertext's relinéarisation that allow obtaining a small relinéarisation key and a quick computation.

Gentry-Sahai-Waters's scheme:

The major drawback of previous schemes, based on the LWE problem, lies in the multiplication operation. In fact the step of relinéarisation used at this level is very expensive. This cryptosystem [25] reduces the complexity of this operation through the use of a new technique, called "approximate eigenvector." The homomorphic operations in this scheme are matrix additions and multiplications and don't require an evaluation key, giving an asymptotically faster scheme and permit to design the first homomorphic identity based encryption scheme (see [25]).

Brakerski-Vaikuntanathan's scheme:

Starting from the GSW's[25] cryptosystem, Brakerski and Vaikuntanathan[29] developed a new FHE scheme that can be as secure as any other lattice-based public-key encryption scheme. Their approach is based on three main ideas:

- Noise-bounded sequential evaluation of high fan-in operations.
- Circuit sequentialization using Barrington's Theorem.
- Successive dimension-modulus reduction.

YASHE's scheme:

Naehrig et al use the ideas of Stehle and Steinfeld [35] to design the YASHE [27] FHE scheme, this cryptosystem is based on the RLWE problem and uses the tensorial product technique of Brakerski [23] to manage the noise resulting from the homomorphic multiplication. For a diagram FHE authors apply the bootstrappabilité Gentry technique.

Chen-Wang-Zhang-Song's scheme :

This cryptosystem [42] is based on a new variant of LWE problem called binary-LWE (bLWE). To reduce the size of the noise the authors choose the secret key from $\{0,1\}^n$ rather than using the binary decomposition of this key as in the Brakerski's scheme [23]. The advantage of this scheme compared to the scheme [23], is its best key size, its best size of the key switching matrix as well as its smallest resulting ciphertext from tensorial product.

Tanping-Xiaoyuan-Wei-Liqiang's scheme :

Based on the same security assumption as [42], the bLWE problem, Tanping et al [28] have developed a FHE scheme using both modulus reduction and key switching to obtain a FHE. This cryptosystem has the advantage to have a very small secret key, to be the first circularly secure key switching algorithm and to have a fast homomorphic addition operation in comparison with the BGV scheme. But the performance of this algorithm always remains to be demonstrated.

D. Noise-free FHE schemes

From the Gentry's breakthrough [14] until now, most of the current design of FHE schemes are noise-based constructions. To decrypt we should remove this noise from ciphertext. To cut down the noise on the ciphertexts, these cryptosystems rely on one of the techniques of managing noise cited above. The refreshment techniques impact negatively the performances of FHE schemes after implementation. In order to improve these performances a second category of FHE schemes is appeared currently. It is free-noise FHE schemes. In this section we show the most important free-noise FHE schemes in the literature.

The Xiao-Bastani-Yen's scheme

In 2012 [43] Xiao et al, proposed the first noise-free FHE scheme. This is a symmetric encryption scheme. Its security is based on the factoring problem. Homomorphic properties are obtained via matrices operations. Using this cryptosystem we can encrypt a cleartext $m \in \mathbb{Z}_N$. But this system is not IND-CPA secure; at least it can withstand a set number n of selected cleartext attack.

MORE&PORE schemes

Kipnis and Hibshoush published two isomorphic methods [44]; each method randomizes and encrypts a single input element $m \in \mathbb{Z}_N$ without adding noise to it. The basic methods are a matrix-based method, MORE (Matrix Operation for Randomization or Encryption), and a polynomial-based method, PORE (Polynomial Operation for Randomization or Encryption). These two schemes were quickly proven insecure [45].

Li-Wang's scheme

Using non-commutative rings, Li and Wang [46] proposed a free-noise FHE scheme. The scheme is very similar to the Xiao-Bastani-Yen's and MORE schemes. The purpose of using non-commutative rings was to overcome the attack suffered by its similar previous cryptosystems.

Recently in February 2016, Gjosteen and Strand published a new attack [55] on this scheme. This means that it is not secure today.

Yagisawa's schemes

Masahiro Yagisawa published a sequence of FHE schemes using non-associative octonion ring over finite field [56], [57], [58], [59] and [60]. In [56] the author proposed a FHE scheme which security is based on computational difficulty to solve the multivariate algebraic equations of high degree. This scheme has the weak point in the enciphering function which suffers from the “p and -p attack” (p is the plaintext) and was cryptanalyzed in [61]. In [57] Masahiro adopted the enciphering function such that we can't easily distinguish the ciphertexts of “p and -p” and constructed the composition of the plaintext p with two sub-plaintexts u and v. The same approach was followed by the author in [58] to secure his cryptosystem, but this time the composition of the plaintext p is three plaintexts u, v and w and the octonion was chosen over finite ring with composite number modulus instead of finite field. A third amelioration of Yagisawa's scheme was introduced in [59]. In this paper the author proposed a FHE scheme with composite number modulus where the complexity required for encryption and decryption is smaller than the same modulus in the RSA scheme. Recently in 2016 Masahiro published a new FHE scheme based on octonion ring. This is a public key cryptosystem based on discrete logarithm assumption and Diffie-Hellman assumption of multivariate polynomials on octonion ring. Despite of this scheme is shown to be immune from “p and -p attack”, it should be revisited by cryptologists.

Wang's scheme

Recently in January 2016, Yongge Wang proposed a symmetric FHE scheme [62], it is octonion based. Homomorphic operations are obtained via regular matrix operations. This scheme is not secure against adversaries who have access to sufficiently many linearly independent ciphertexts with known plaintexts and session randomness. Furthermore it is not secure in the ciphertext only attack security model, but it is secure in the weak ciphertext-only security model.

VI. COMPARISON AND SYNTHESIS

In the table [1] we analyse the complexity of FHE schemes described above. The table below gives an overview of the performance of these algorithms. . (λ, n : security parameters, q: modulo, Θ, O, \tilde{O} : Landau's notations[53])

Table 1 : Comparison of the performance of FHE schemes

Category	ID	Algorithm	Public key	Secret key	Ciphertext
Noise-based	1	Gentry[14]	n^7	n^3	$n^{1.5}$
	2	Smart-Verc[15]	$O(n^3)$	n^3	$O(n^{1.5})$
	3	Chunsheng [20]	$O(2^{n\eta+1})$	$O(2^{n\eta})$	$O(2^{n\eta})$
	4	Improved Gentry[35]	$\tilde{O}(\lambda^{3.5})$	$\Theta(\lambda^{1.5})$	$\tilde{O}(\lambda^{3.5})$
	5	SIMD Gentry[36]	$N^N 2^{t.N}$	$O(2^t)$	$O(2^{t.N})$
	6	DGHV[16]	$\tilde{O}(\lambda^{10})$	$\tilde{O}(\lambda^2)$	$\tilde{O}(\lambda^5)$
	7	CMNT[26]	$\tilde{O}(\lambda^7)$	$\tilde{O}(\lambda^2)$	$\tilde{O}(\lambda^5)$
	8	Chunsheng[17]	$O(\lambda^5)$	$O(\lambda^3)$	$O(\lambda^2)$
	9	Chunsheng[18]	$O(n^3)$	$O(n)$	$O(n^2)$
	10	Chunsheng[19]	$O(n^3 \log n)$	$O(n \log n)$	$O(n^2 \log n)$
	11	Batch DGHV[39]	$\tilde{O}(\lambda^7)$	$l \cdot \tilde{O}(\lambda^2)$	$l \cdot \tilde{O}(\lambda^5)$
	12	KSYC[30]	$\tilde{O}(\lambda^{10})$	$\tilde{O}(\lambda^5)$	$\tilde{O}(\lambda^5)$
	13	BV[21]	$O(n^2 \log^2 q)$	$n \cdot \log q$	$(n + 1) \cdot \log q$
	14	BGV[22]	$2dn \cdot \log q$	$2d \cdot \log q$	$2d \cdot \log q$
	15	Brakerski[23]	$O(\lambda^2 \log^2 q)$	$\lambda \cdot \log q$	$(\lambda + 1) \cdot \log q$
	16	Fan-Verc[24]	$2d \cdot \log q$	d	$2d \cdot \log q$
	17	GSW[25]	$O(n^2 \log^2 q)$	$(n + 1) \cdot \log q$	$(n + 1)^2 \cdot \log^3 q$
	18	BV[29]	$(n + 1)^2 O(\log q)$	$n \cdot \log q$	$(n + 1)^2 \log^2 q$
	19	CWZS[42]	$O(n^2 \log q)$	$n + 1$	$(n + 1) \log q$
	20	TXWW[28]	$O(n^2 \log^2 q)$	$(n + 1) \log q$	$(n + 1) \log q$
Free-noise	21	XBY[43]	NA	$O(\lambda m)$	$O(\lambda m)$
	22	MORE [44]	NA	$O(2\lambda)$	$O(2\lambda)$
	23	LI-WANG[46]	NA	$O(3\lambda)$	$O(3\lambda)$
	24	Yagisawa[60]	$64 \cdot \log q$	$O(1)$	$O(q)$
	25	Wang[62]	q	$O(q)$	$O(64q)$

The results of this table show that the keys and ciphertexts of noise-based FHE schemes, currently known, are gigantic sizes. This was expected, because the homomorphy in these cryptosystems is obtained by adding huge noise to cleartexts. These larger sizes have a major impact on the performance of FHE algorithms in terms of memory and runtime. On the other hand, the complexity of ciphertexts in free-noise FHE schemes is acceptable compared to noise-based FHE schemes. But the security of this category of schemes is weak and the majority of these schemes was broken.

VII. IMPLEMENTATION AND TESTING OF FHE SCHEMES

Different implementations of FHE schemes exist today, but are only test implementations and are not for effective use. The first attempt to implement a scheme dates from 2009 FHE with Smart and Vercautern [15], the two cryptologists were able to implement the Gentry's SWHE scheme but remained unable to implement bootstrappability that is required for full functionality of this FHE cryptosystem. In [49], Gentry and Halevi have overcome this problem by implementing the bootstrappability operation; the runtime of a single

operation (on a machine with a large capacity memory) varies between 30s and 30min, for different public key sizes (between 70 megabytes and 2.3 megabytes). In April 2013, [51] Halevi and Shoup described a design of HElib library that implements the BGV encryption scheme focusing on the technique of packaging of ciphertexts of Smart and Vercautern [15] and Gentry-Halevi-Smart's optimizations[50] for a faster homomorphic evaluation. This design was implemented in C++ and got out to use, including also the bootstrappability, in December 2014 [47]. Recently in 2015[48], Varia et al have published an open source testing framework, called Hetest, to assess the correctness and performance of homomorphic encryption software and libraries. Hetest automates all processes of a test: data generation for testing (such as circuits and inputs), the execution of a test, comparing performance to a reference level of insecurity, statistical analysis of the test results and producing a report.

VIII. CONCLUSION AND OUTLOOKS

In this article we did a study of the state of the art of FHE schemes. The study shows that there are different frameworks for building a FHE scheme. Despite the existence of these different frameworks and despite the efforts of cryptologists to build a practical FHE scheme, there is still much work to do to move from theory to practice.

After the detailed study of the state of the art of homomorphic encryption, different axes of research, which we can follow to continue our thesis, appear:

- Improve the runtime of FHE schemes.
- Find other alternative of frameworks to design FHE schemes.
- Boost cryptanalysis of FHE algorithms to enhance the design of FHE schemes.

REFERENCES

- [1] R. Rivest, L. Adleman, and M. Dertouzos. "On data banks and privacy homomorphisms", Foundations of Secure Computation, pp 169-180, 1978.
- [2] S. Goldwasser and S. Micali: Probabilistic encryption. Journal of Computer and System Sciences 28(2) (1984) 270-299
- [3] Benaloh, J. Dense probabilistic encryption. In In Proceedings of the Workshop on Selected Areas of Cryptography (1994), pp. 120–128.
- [4] Naccache, D., and Stern, J. A new public-key cryptosystem. In EUROCRYPT (1997), pp. 27–36.
- [5] Okamoto, T., and Uchiyama, S. A new public-key cryptosystem as secure as factoring. In In Eurocrypt '98, LNCS 1403 (1998), Springer-Verlag, pp. 308–318.
- [6] Paillier, P.: Public-key cryptosystems based on composite degree residuosity classes. In: 18th Annual Eurocrypt Conference (EUROCRYPT'99), Prague, Czech Republic. Volume 1592 of Lecture Notes in Computer Science., Springer (1999) 223-238.
- [7] Damgård, I., and Jurik, M. A generalisation, a simplification and some applications of paillier's probabilistic public-key system. In Proceedings of the 4th International Workshop on Practice and Theory in Public Key Cryptography : Public Key Cryptography (London, UK, UK, 2001), PKC '01, Springer-Verlag, pp. 119–136.
- [8] Schmidt-Samoa, K., and Takagi, T. Paillier's cryptosystem modulo p2q and its applications to trapdoor commitment schemes. In Proceedings of the 1st international conference on Progress in Cryptology in Malaysia (Berlin, Heidelberg, 2005), Mycrypt'05, Springer-Verlag, pp. 296–313.
- [9] R.L. Rivest, A. Shamir and L. Adleman, 'A Method for Obtaining Digital Signatures and Public Key Cryptosystems," Communications of ACM, Vol. 21, pp. 120-126, April 1978.
- [10] ElGamal, T.: A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory 31(4) (1985) 469-472.
- [11] Sander, T., Young, A. L., and Yung, M. Non-interactive cryptocomputing for nc1. In FOCS (1999), pp. 554–567.
- [12] Boneh, D., Goh, E.J., Nissim, K.: Evaluating 2-DNF formulas on ciphertexts. In Kilian, J., ed.: Theory of Cryptography, Second Theory of Cryptography Conference, TCC 2005, Cambridge, MA, USA, February 10-12, 2005, Proceedings. Volume 3378 of Lecture Notes in Computer Science., Springer (2005) 325-341
- [13] Aguilar Melchor, C., Gaborit, P., Herranz, J.: Additively homomorphic encryption with d-operand multiplications. Cryptology ePrint Archive, Report 2008/378 (2008) <http://eprint.iacr.org/>.
- [14] Gentry, C. A fully homomorphic encryption scheme. PhD thesis, Stanford University, 2009. <http://crypto.stanford.edu/craig>.
- [15] Smart, N.P., Vercauteren, F. Fully Homomorphic Encryption with Relatively Small Key and Ciphertext Sizes. Cryptology ePrint Archive, Report 2009/571, 2009. <http://eprint.iacr.org/>.
- [16] van Dijk, M., Gentry, C., Halevi, S., and Vaikuntanathan, V. Fully homomorphic encryption over the integers. Cryptology ePrint Archive, Report 2009/616, 2009. <http://eprint.iacr.org/>.
- [17] G. Chunsheng. " Fully Homomorphic Encryption Based on Approximate Matrix GCD ". Available at eprint.iacr.org/2011/645.
- [18] G. Chunsheng. " Fully Homomorphic Encryption, Approximate Lattice Problem and LWE ". Available at <http://eprint.iacr.org/2011/114>
- [19] G. Chunsheng. " New Fully Homomorphic Encryption over the Integers ". Available at <http://eprint.iacr.org/2011/118>
- [20] G. Chunsheng. " More practical Fully Homomorphic Encryption ". Available at <http://eprint.iacr.org/2011/121>.
- [21] Z. Brakerski, V. Vaikuntanathan. " Efficient Fully Homomorphic Encryption from (Standard) LWE". Available at <http://eprint.iacr.org/2011/344>.
- [22] Z. Brakerski, C. Gentry, V. Vaikuntanathan. "Fully Homomorphic Encryption without Bootstrapping". Available at <http://eprint.iacr.org/2011/277>.

- [23] Z. Brakerski, "Fully Homomorphic Encryption without Modulus Switching from Classical GapSVP". Available at <http://eprint.iacr.org/2012/78>.
- [24] J. Fan, F. Vercauteren, "Somewhat Practical Fully Homomorphic Encryption". Available at <http://eprint.iacr.org/2012/144>.
- [25] C. Gentry, A. Sahai, B. Waters, "Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based ". Available at <http://eprint.iacr.org/2013/340>.
- [26] J. Coron, A. Mandal, D. Naccache, M. Tibouchi, "Fully Homomorphic Encryption over the Integers with Shorter Public Keys". Available at <http://eprint.iacr.org/2011/441>.
- [27] J.W. Bos, K. Lauter, J. Loftus, M. Naehrig, "Improved Security for a Ring-Based Fully Homomorphic Encryption Scheme". Available at <http://eprint.iacr.org/2013/075>.
- [28] Z. Tanping, Y. Xiaoyuan, Z. Wei, W. Wiqiang, "Efficient Fully Homomorphic Encryption with Circularly Secure Key Switching Process". Available at <http://eprint.iacr.org/2015/466>.
- [29] Z. Brakerski, V. Vaikuntanathan. " Lattice-Based FHE as Secure as PKE". Available at <http://eprint.iacr.org/2013/541>
- [30] J. Kim, M. Sung Lee, A. Yun, J. Hee Cheon. " CRT-based Fully Homomorphic Encryption over the Integers". Available at <http://eprint.iacr.org/2013/057>
- [31] Xiao, L., Bastani, O., and Yen, I.-L. « An efficient homomorphic encryption protocol for multi-user systems ». Cryptology ePrint Archive, Report 2012/193.
- [32] A. Kipnis and E. Hibshoosh, « Efficient Methods for Practical Fully Homomorphic Symmetric-key Encrypton, Randomization and Verification », Cryptology ePrint Archive, Report 2012/637.
- [33] J. Li, L. Wang. " Noise-free Symmetric Fully Homomorphic Encryption based on noncommutative rings". Available at eprint.iacr.org/2015/641
- [34] R. Rothblum, 'homomorphic encryption: from private-key to public-key' electronic colloquium on computational complexity, report No. 146 (2010).
- [35] D. Stehle and R. Steinfeld. "Faster fully homomorphic encryption." Cryptology ePrint Archive Report 2010/299.
- [36] N. P. Smart and F. Vercauteren, "Fully homomorphic SIMD operations", IACR Cryptology ePrint Archive, Report 2011/133.
- [37] C. Gentry and S. Halevi, "Fully homomorphic encryption without squashing using depth-3 arithmetic circuits", Cryptology ePrint Archive, Report 2011/279.
- [38] C. Gentry, S. Halevi and N.P. Smart, "Better bootstrapping in fully homomorphic encryption", Cryptology ePrint Archive, Report 2011/680.
- [39] J. Coron, T. Lepoint and M. Tibouchi. "Batch fully homomorphic encryption over the integers." 2012. Available at eprint.iacr.org/2013/36.
- [40] Regev, O. On lattices, learning with errors, random linear codes, and cryptography. In STOC (2005), pp. 84–93.
- [41] David A. Mix Barrington. Bounded-width polynomial-size branching programs recognize exactly those languages in nc^1 . J. Comput. Syst. Sci., 38(1):150{164, 1989}
- [42] Z. Chen, J. Wang, ZN. Zhang, X. Song, "A Fully Homomorphic Encryption Scheme with Better Key Size". available at <https://eprint.iacr.org/2014/697.pdf>
- [43] Xiao, L., Bastani, O., and Yen, I.-L. « An efficient homomorphic encryption protocol for multi-user systems ». Cryptology ePrint Archive, Report 2012/193.
- [44] A. Kipnis and E. Hibshoosh, « Efficient Methods for Practical Fully Homomorphic Symmetric-key Encrypton, Randomization and Verification », Cryptology ePrint Archive, Report 2012/637.
- [45] B. Tsaban and N. Lifshitz,"Cryptanalysis of the MORE symmetric key fully homomorphic encryption scheme ", Cryptology ePrint Archive, Report 2013/250.
- [46] J. Li and L. Wang, "Noise-free Symmetric Fully Homomorphic Encryption based on noncommutative rings", Cryptology ePrint Archive, Report 2015/641.
- [47] <https://github.com/shaikh/HElib>
- [48] M. Varia, S. Yakoubov, Y. Yang, "HETest: A Homomorphic Encryption Testing Framework". available at <https://eprint.iacr.org/2015/416.pdf>
- [49] C. Gentry, S. Halevi, "Implementing Gentry's Fully-Homomorphic Encryption Scheme". available at <https://eprint.iacr.org/2010/520.pdf>
- [50] C. Gentry, S. Halevi, N. Smart "Homomorphic Evaluation of the AES Circuit". available at <https://eprint.iacr.org/2012/099.pdf>
- [51] <http://researcher.ibm.com/researcher/files/us-shaikh/he-library.pdf>
- [52] Howgrave-Graham, N. Approximate integer common divisors. In CaLC (2001), pp. 51–66
- [53] https://en.wikipedia.org/wiki/Big_O_notation.
- [54] A. Jounaidi, L. Henri, "Méthodes matricielles Introduction à la complexité algébrique"
- [55] K. Gjosteen, M. Strand. Fully homomorphic encryption must be fat or ugly?. Cryptology ePrint Archive, Report 2016/105, 2016. <http://eprint.iacr.org/>.
- [56] M. Yagisawa " Fully homomorphic encryption without bootstrapping" Cryptology ePrint Archive, Report 2015/474, 2015. <http://eprint.iacr.org/>.
- [57] Masahiro Yagisawa " Fully homomorphic encryption on octonion ring" Cryptology ePrint Archive, Report 2015/733, 2015. <http://eprint.iacr.org/>.
- [58] Masahiro Yagisawa," Fully Homomorphic Encryption with composite number modulus", Cryptology ePrint Archive, Report 2015/1040, 2015. <http://eprint.iacr.org/>.
- [59] M. Yagisawa " Improved fully homomorphic encryption with composite number modulus" Cryptology ePrint Archive, Report 2016/50, 2016. <http://eprint.iacr.org/>.
- [60] M. Yagisawa " Fully homomorphic public-key encryption based on discrete logarithm problem" Cryptology ePrint Archive, Report 2016/54, 2016. <http://eprint.iacr.org/>.
- [61] Yongge Wang. Notes on two fully homomorphic encryption schemes without bootstrapping. Cryptology ePrint Archive, Report 2015/519, 2015. <http://eprint.iacr.org/>.
- [62] Yongge Wang. Octonion algebra and noise-free fully homomorphic encryption (FHE) schemes. Cryptology ePrint Archive, Report 2016/068, 2016. <http://eprint.iacr.org/>.

Autoregressive Model based Segmentation of Overlapped region

Vidyadevi G Biradar
Department of ISE
NMIT
Bangalore, India

H Sarojadevi
Department of CSE
NMAMIT
Bangalore, India

H C Nagaraj
Department of ECE
NMIT
Bangalore, India

Abstract—Overlapped fingerprints occur due to multiple impressions of fingerprints on the same object at same place. This is natural in uncontrolled environments, or they are the residual fingerprints left over on fingerprints scanner. Overlapped fingerprints need to be separated into individual fingerprints for recognition. Separation of overlapped fingerprints involves steps, segmentation of image regions, feature extraction and classification. State of the art algorithms for separation of overlapped fingerprints adopts region wise processing approach to feature extraction. Therefore segmentation of overlapped region is an essential step for robust feature extraction. This paper presents a new algorithm for segmentation of overlapped region using time series two dimensional Autoregressive (2D AR) model. AR model parameters are estimated using Least Squares (LS) method which ensures minimum mean square error. The performance of the algorithm is evaluated using a standard database of 100 overlapped fingerprints images. The results are compared with ground truth results and are found satisfactory. Segmentation accuracy achieved is between 80% to 90%.

Keywords- Segmentation, AR model, overlapped fingerprints, texture, separation

I. INTRODUCTION

Fingerprints based personal recognition systems are successfully deployed both in civilian and law enforcement organizations [1]. However, existing fingerprints recognition systems pose limited ability in their performance for recognition of fingerprints with complex backgrounds which are very challenging. Overlapped fingerprints are the typical challenged fingerprints which contain specifically another fingerprint as background. Fig.1 shows an example of overlapped fingerprints. These fingerprints occur due to multiple impressions of fingerprints in the same position or they are the residual fingerprints left over on fingerprints scanner. Existing fingerprint recognition systems can be tuned to work for overlapped fingerprints by essentially separating overlapped fingerprints into individual fingerprints.

A number of approaches exists in the literature for the separation of overlapped fingerprints [2][3][4][5]. Typical steps for fingerprint separation include 1.Segmentation of overlapped fingerprints into overlapped and non overlapped regions, 2.Extraction of fingerprint ridge orientations, 3. Classification of fingerprints orientation fields followed

separation. Extraction of fingerprint ridge orientations in non overlapped region is straightforward as it contains orientation field of individual fingerprints, most widely used methods for ridge orientation extraction are Gradient based methods [6]. Overlapped region contains mixture of orientation fields of both the fingerprints, therefore robust and efficient algorithms such as ridge orientation modelling using Fourier expansion (FOMFE) and Dictionary based techniques are utilized. These methods are highly complex and applying these on entire image leads to both time and space complexity. Therefore there is a need to identify overlapped and non overlapped regions to selectively apply methods. Existing algorithms for fingerprints separation are dependent on manual marking of overlapped regions by fingerprints experts. The process of manual marking becomes tedious and unrealistic especially when a lot of overlapped fingerprints need to be analysed. Also, human intervention in the separation process becomes a bottleneck in developing completely automated fingerprints separation systems. Therefore there is a need for developing an algorithm for automatic segmentation of regions of overlapped fingerprint.

Earlier work on segmentation of overlapped fingerprints is presented in papers [7][8], former presents method for identifying regions of overlapped fingerprints using morphological connectivity and later, gives a method based on fractal analysis. In this paper a novel approach to segmentation is proposed which is based on two dimensional time series Autoregressive (2D AR) model.



Figure 1. Example of overlapped fingerprint

Fingerprints exhibit texture patterns due to ridges and furrows. Overlapped fingerprints shows observable distinct texture patterns in overlapped and non overlapped regions. Two dimensional Time series autoregressive models are very useful in representing image texture [9]. Therefore autoregressive model is explored in this work to identify regions of overlapped fingerprint and results are presented in section V.

Paper is organized into following sections, Section II presents related work on AR model for modelling overlapped fingerprints image texture and analysis, Section III focuses AR model coefficients estimation, Section IV provides a method for segmentation using AR model, Section V provides results and discussion, Section VI presents conclusion.

II. RELATED WORK

Time series autoregressive model is widely applied for processing one dimensional (1-D) signal such as speech, ECG [10], [11]. The advantage of AR model is the possibility of predicting the current value using previous signal sample values and this model is an effective tool in capturing texture content from an image. Regions of a texture image are differentiated in terms of AR model coefficients. There are different approaches to compute AR model coefficients such as least squares method, Maximum likelihood method, Yule Walker and Burg's method etc. AR models are categorized into different types depending upon the pattern of neighbourhood and number of lag pixels used for the prediction of current pixel value. One approach to this is considering all the pixels that belong to top rows and left column of current pixel as lag variables.

2 D Autoregressive model is widely used for image processing applications, they include texture analysis, texture synthesis, texture segmentation and image retrieval [12][13][14][15][16][17][18][19]. Earlier work on segmentation using time series autoregressive modelling is as follows, in paper [12] a non causal type AR model is used for synthesis and analysis of texture where model coefficients are computed using maximum likelihood algorithm. Paper [13], presents design of AR model for image texture analysis and model parameters are computed using neural network. Paper [14] presents a method of selecting adaptive neighbourhood for two dimensional bidirectional AR model to analyse image texture.

Paper [15] suggests a method for deciding a set of lag variables using partial autocorrelation coefficients. Paper [16] presents another method for selecting neighbourhood patterns for AR model based on auto and partial correlation coefficients. In paper [17] AR model is applied for modelling of rock surface texture and identification of fractures in rock which occur due to overload.

Paper [18] implements a 2D Quarter Plane AR model which incorporates four prediction supports to model texture for image segmentation. In paper [19], AR model is developed with causal neighbours for modelling image texture in image retrieval application. AR model identifies regions of image based on model coefficients. AR methods use region growing method for image segmentation. In the proposed work two dimensional (2-D) time series model is used for segmentation of overlapped fingerprints into overlapped and non overlapped regions.

III. AUTOREGRESSIVE MODELLING FOR OVERLAPPED FINGERPRINTS

Autoregressive modeling is an approach to digital signal processing which is based on standard probability and statistics concepts. An AR model is considered as all pole infinite impulse response filter which predicts current value of the signal as a linear weighted combination of previous signals.

An AR (P) model with order p is represented as given in equation (1).

$$X_t = C + \sum_{i=1}^p \varphi_i X_{t-i} + \epsilon_t \quad . \quad (1)$$

Where, X_t is the estimated current value of the signal and X_{t-i} is previous value. $\varphi_1, \dots, \varphi_p$ are the AR model coefficients, C is constant and ϵ_t is the white noise.

In analogy with a one dimensional signal, time series two dimensional (2-D) autoregressive model assumes that image $I(x, y)$ is a set of random variables which are spatially related. Image analysis using autoregressive model utilizes pixel neighbourhood information for predicting grey value of current pixel, it is the weighted sum of neighbour pixel values and noise.

In first order AR (1) model, grey value of the current pixel is computed using equation (2).

$$I(x, y) = A * B [I(x-1, y) + I(x, y-1)] + n(x, y) \quad (2)$$

Where, A and B are AR model coefficients, $n(x, y)$ is the Gaussian white noise.

By applying linear regression method, AR parameters are computed as, assume

$$z(x, y) = I(x-1, y) + I(x, y-1)$$

$$\text{Numerator} = \sum_{x=1}^M \sum_{y=1}^N z(x,y) * I(x,y) - M * N * L \quad (3)$$

Where, $L = E[z(x,y)] * E[I(x,y)]$

$$\text{Denominator} = \sum_{x=1}^M \sum_{y=1}^N [z(x,y)]^2 - M * N * K^2 \quad (4)$$

$$K = E(z(x,y))$$

M is total region growing sample row pixels number, N is total region growing sample column pixels number.

$$\hat{z} = \frac{\text{Numerator}}{\text{Denominator}}$$

$$\hat{z} = E(I(x,y)) - \hat{z} * E(z(x,y)) \quad (5)$$

$E(I(x,y))$ denotes expected value.

Intuitively, first order AR model is not sufficient for prediction as the number of pixels used to predict current pixel are only top and left neighbours. Therefore second order AR model is considered in this work.

Second order AR (2) model – grey value of current pixel is calculated using equation (6).

$$I(x,y) = A + BI(x-1,y) + CI(x,y-1) + DI(x-1,y-1) + N(x,y) \quad (6)$$

Where, A, B, C and D are the AR model coefficients and N(x,y) is Gaussian noise. In second order AR model, for predicting the current value of pixel top, left and top-left diagonal neighbours are considered as significant pixels to influence current pixel value.

Let $\hat{I}(x,y)$ is a predicted value of $I(x,y)$ using AR (2) model, AR model coefficients are calculated using least squares method which ensures minimum value of mean square error (MSE) between the actual data and the predicted data[20][21][22]. MSE is given by equation (7).

$$MSE = \sum_{x=1}^M \sum_{y=1}^N E\{(I(x,y) - \hat{I}(x,y))^2\} \quad (7)$$

Equation (8) gives the conditions to be satisfied to achieve minimum value of MSE.

$$\begin{aligned} \frac{\partial(MSE)}{\partial A} &= 0, & \frac{\partial(MSE)}{\partial B} &= 0 \\ \frac{\partial(MSE)}{\partial C} &= 0, & \frac{\partial(MSE)}{\partial D} &= 0 \end{aligned} \quad (8)$$

Through the method of linear regression, AR coefficients are estimated using following matrix operation as shown in equation (9).

$$P * T = Q \quad (9)$$

Where P and Q are given as,

$$\begin{aligned} P &= \begin{bmatrix} p_{11} & p_{12} & p_{13} & p_{14} \\ p_{21} & p_{22} & p_{23} & p_{24} \\ p_{31} & p_{32} & p_{33} & p_{34} \\ p_{41} & p_{42} & p_{43} & p_{44} \end{bmatrix} \\ Q &= \begin{bmatrix} q_{11} \\ q_{21} \\ q_{31} \\ q_{41} \end{bmatrix} \\ T &= \begin{bmatrix} \hat{A} \\ \hat{B} \\ \hat{C} \\ \hat{D} \end{bmatrix} \end{aligned}$$

$\hat{A}, \hat{B}, \hat{C}, \hat{D}$ are calculated using T .

Predicted image is computed using equation (10), and the error between actual and predicted image is given by equation (11).

$$\hat{I}(x,y) = \hat{A} + \hat{B}(x-1,y) + \hat{C}(x,y-1) + \hat{D}(x-1,y-1) \quad (10)$$

$$e(x,y) = \hat{I}(x,y) - I(x,y) \quad (11)$$

IV. SEGMENTATION USING AUTOREGRESSION MODEL

Segmentation of overlapped fingerprints into overlapped and non overlapped regions is done using region growing segmentation method. It starts with seed point and grows region by merging to seed point with those neighborhood pixels that have similar AR coefficients. The algorithm for region growing is depicted in the flowchart shown in fig. 2, it shows initial values for AR model coefficients A, B, C and D. Other parameters are threshold T, and mean square error MSE. Fig.2 also shows steps for region growing segmentation method. In overlapped fingerprints feature patterns correspond to overlapped and non overlapped regions, thus it is a two class pattern classification problem. The criterion for classification is as below.

- 1) Set class label = 1,

If $e(i,j) < \text{Threshold} = \sqrt{MSE(\text{Optimal})}$

2) Set class label = 0, Otherwise.

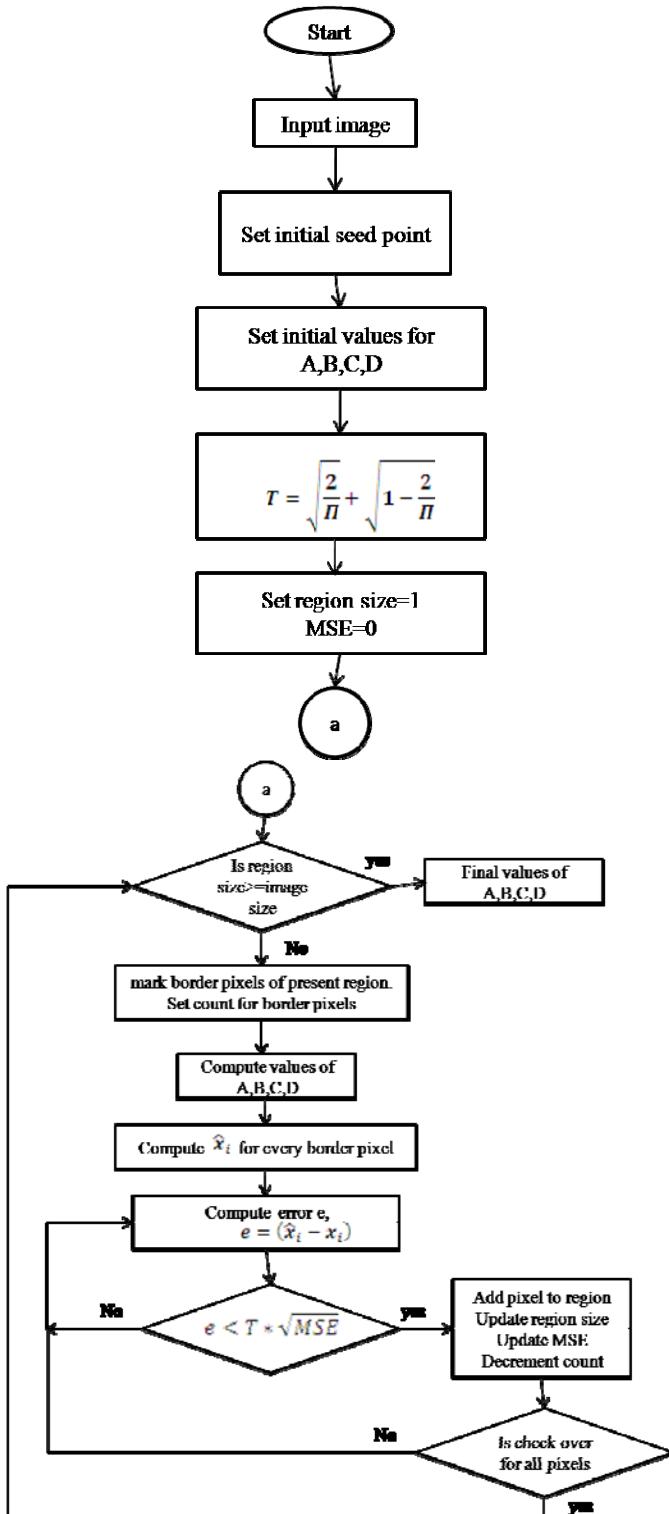


Figure 2. Segmentation using region growing

MSE is the mean square error that changes in each iteration while region is growing. Based on sampling theory properties

and statistical hypotheses and distribution nature of error pixels, the 95% confidence interval threshold T, can be found as:

$$T = \left(\sqrt{\frac{2}{\pi}} + \sqrt{1 - \frac{2}{\pi}} \right) \quad (15)$$

Threshold T with square root of MSE determines whether the pixel is grouped for overlapped region as given in flow chart shown in figure 2.

V. RESULTS AND DISCUSSION

Autoregressive model parameters are computed using least squares method and implemented using Matlab2010a. Segmentation of regions into overlapped and non overlapped regions is experimented with AR model by varying its order and results are presented in this section.

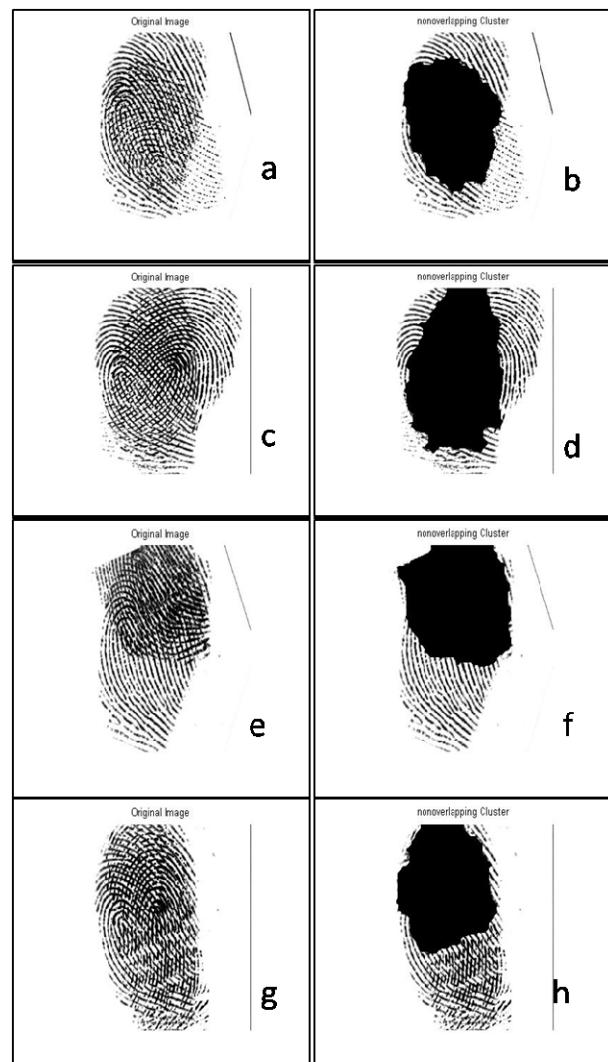


Figure 3(a),(c),(e) and (g) are the input overlapped fingerprints (b), (d),(f) and (h) are segmented images

First order AR model, AR(1) is not satisfactory for segmentation of overlapped region, as the number of neighbours used for prediction of current pixel value is not sufficient. Therefore, Second order AR model, AR(2) model is adopted for segmentation of overlapped fingerprint into overlapped region and non overlapped regions. The performance of AR model is evaluated by testing it on overlapped fingerprints from a standard database and satisfactory results are achieved.

The standard database contains a set of 100 overlapped fingerprints with varied conditions. These include fingerprints with unclear ridges, noise, different extent of overlap, and different overlap angle. The model is also tested on a set of locally generated overlapped fingerprints from ink impressions. Both the databases contain overlapped fingerprints with only two fingerprints overlapped. In this work, for the sake of simplicity, it is assumed that there are only two fingerprints overlapped in the overlapped region.

Fig. 3 shows segmentation results for some images from the standard database, Fig. 3(a), (c), (e) and (f) are the input overlapped fingerprints. The segmentation results are satisfactory as interpreted from the results shown in Fig. 3(b), (d), (f) and (h).

Fig. 4 shows segmentation results for few poor quality overlapped fingerprints images, Fig. 4(i), (k), (m) and (o) are the input overlapped fingerprints and Fig. 4(j), (l), (n) and (p) shows segmented images. It is clear from these outputs that AR is indeed satisfactory for poor quality fingerprints.

Segmentation results obtained from AR model are evaluated quantitatively through comparison with ground truth results of segmentation. A database of masks that represents overlapped region for all overlapped fingerprints is prepared through manual segmentation and this is considered as ground truth information. The number of pixels in the overlapped region is used for comparison. The average accuracy of AR model achieved is 80 to 90%. Table 1 shows model accuracy for few overlapped fingerprints.

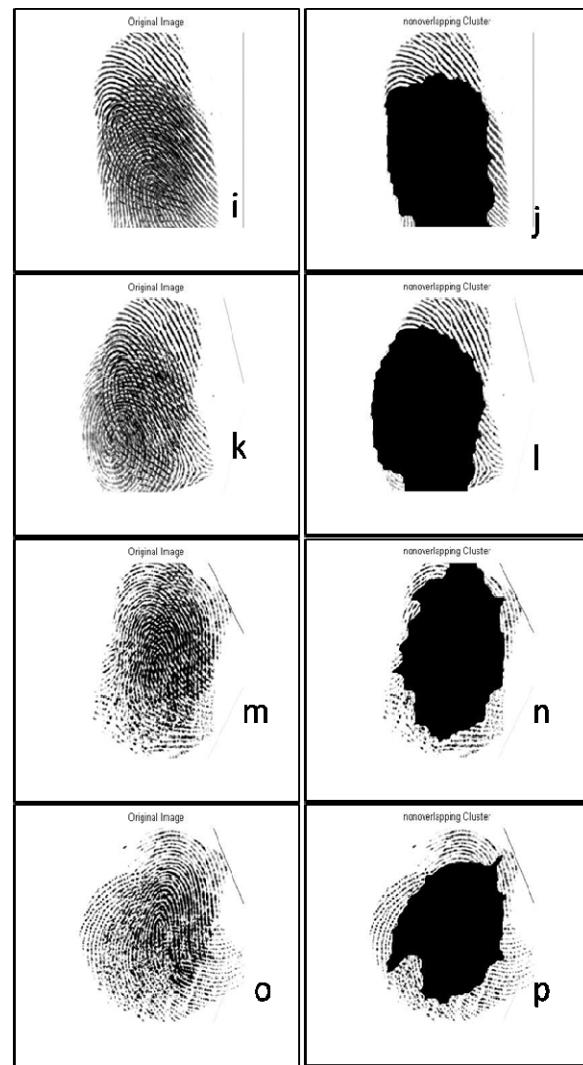


Figure 4(i),(k),(m) and (o) are the input overlapped fingerprints (j), (l),(n) and (p) are segmented images

TABLE I. SEGMENTATION ACCURACY FOR DIFFERENT OVERLAPPED FINGERPRINTS

<i>Overlapped fingerprints</i>	<i>Accuracy of segmentation</i>
1	90.29
2	92.75
3	90.43
4	63.66
5	91.96
6	54.59
7	96.64
8	67.00
9	75.71
10	96.53
11	60.09

<i>Overlapped fingerprints</i>	<i>Accuracy of segmentation</i>
12	30.06
13	96.78
14	74.50
15	85.31
16	87.78
17	99.51
18	82.05
19	60.25
20	67.23

VI. CONCLUSIONS

Time series two dimensional AR model is used for segmentation of overlapped region in overlapped fingerprints. AR model parameters are computed using least squares method, which ensures minimum mean square error between given input image and predicted image. Second order AR model is found satisfactory for the segmentation of overlapped region in overlapped fingerprints. AR model performance is evaluated on a standard database of overlapped fingerprints and the results obtained are satisfactory. There is no improvement in the segmentation results as the model order is increased. The prediction power of AR model is not enhanced by increasing the number of neighboring pixels due to the presence of redundant information about pixel neighborhood. The results of segmentation are compared with the ground truth information and the percentage of accuracy achieved is between 80% to 90%.

ACKNOWLEDGMENT

Authors wish to thank the management, Nitte Meenakshi Institute of Technology, for encouraging the research work and providing kind support.

REFERENCES

- [1] Davide Maltoni, Dario Maio, Anil K. Jain, Salil Prabhakar, Handbook of Fingerprint Recognition, Springer Professional Computing 2nd Ed. 2009.
- [2] F. Chen, J. Feng, and J. Zhou, "On separating overlapped fingerprints," in Proc. Fourth IEEE Int. Conf. Biometrics: Theory Applications and Systems (BTAS), pp. 1–6, 2010.
- [3] Fanglin Chen, Jianjiang Feng, Anil K. Jain, Jie Zhou, and Jin Zhang, "Separating Overlapped Fingerprints", *IEEE Transactions on Information Forensics and Security*, vol. 6, pp.346-359, 2011.
- [4] Q. Zhao and A. K. Jain, "Model-based separation of overlapping latent fingerprints," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 3, pp. 904–918, 2012.
- [5] Jianjiang Feng, Member, Yuan Shi, and Jie Zhou, "Robust and Efficient Algorithms for Separating Latent Overlapped Fingerprints", *IEEE Transactions on Information Forensics and Security*, vol. 7, No. 5, pp. 1498-1510, 2012.
- [6] S. Yoon J. Feng, A. Jain, "Latent fingerprint enhancement via robust orientation field estimation". International Joint Conference on Biometrics, pp.1-8, 2011.
- [7] Vidyadevi G. Biradar, H.Sarojadevi, "Segmentation of overlapped region using morphological processing", IJCSI International Journal of Computer Science Issues, vol. 11, pp.66-71, 2014.
- [8] Biradar V G,Sarojadevi H,Nagaraj H C, "Fractal analysis for classification of regions in overlapped fingerprints", *Journal of Signal and Image Processing*, vol.5, pp.-149-152, 2015.
- [9] Pei-Gee Peter Ho, Image Segmentation, Tech Janeza Trdine 9, 51000 Rijeka, Croatia, 2011.
- [10] GE Ding-Fei HOU Bei-Ping XIANG Xin-Jian, "Study of feature extraction based on autoregressive modeling in ECG automatic diagnosis", vol. 33, ACTA,Automation sinica, vol.33, pp.462-466, 2007.
- [11] J. Hernando and C. Nadeu, "AR modelling of the speech autocorrelation to improve noisy speech recognition," SPAC, pp. 107-110, November 1992.
- [12] Koichiro Deguchi, "Two dimensional auto-regressive model for analysis and synthesis of gray level textures", proceedings of first international symposium for science on form, pp.441-449.1986.
- [13] SiWei Lu and He Xu, "Textured image segmentation using, Autoregressive model and artificial neural network", journal of pattern recognition, vol 28 12, pp.1807-1817, 1995.
- [14] I. Claude and A. Smolarz, "A new textured image segmentation algorithm by autoregressive modelling and multiscale block classification", 6th International Conference on Image Processing and its Applications (CP443), pp.586-590, 1997.
- [15] Anjan Sarkar, K. M. S. Sharma, and Rajesh V. Sonak, "A new approach for subset 2D AR model identification for describing textures", *IEEE transactions on image processing*, vol 6, pp.407-413 ,1997.
- [16] Isabelle claude and andre smolarz, "An identification method for texture AR modeling based on auto-and partial correlation measures", *Signal processing conference*, pp.1-4, 1998.
- [17] Seetal , N. Natarajan, "Image Segmentation for rock fractures based on ARMA model", *International Journal of engineering science and technology*,vol. 2, pp.1155-1159, 2010 .
- [18] Olivier alata, Clarisse Ramananjarasoa, "Unsupervised textured image segmentation using 2D quarter plane autoregressive model with four prediction supports", *Pattern recognition Letters*, vol.26,pp.1067-1081, 2005.
- [19] Noureddine abbadeni, texture representation and retrieval using the causal autoregressive model, *J.Vis. Commun. Image*, vol.21, pp. 651-664, 2010.
- [20] Wei Xing Zhang, "A least square based method for autoregressive signals in the presence of noise", *Circuits and Systems II: Analog and Digital Signal Processing*, *IEEE Transactions*, vol.46, pp.81-85, 1995.
- [21] Bo Bao, Yingoin Xu, jie Sheng, Ruifeng Ding, "Least squares based iterative parameters estimation algorithm for multivariable controlled ARMA system modeling with finite measurement data", *Mathematical and Computer modeling*, vol 53, pp.1664-1669, 2011.

- [22] Proakis, Digital Signal Processing: Principles, Algorithms, And Applications, 2006.

AUTHORS PROFILE

Vidyadevi G Biradar is working as an Associate professor in the department of Information Science and Engineering, Nitte Meenakshi institute of technology and currently pusuing her Phd. She has 19 years of tecahing experince. She has published about 12 papers in national and international journals. Her research interests include image processing, database management systems and software engineering.

Dr. Sarojadevi H. is Professor & Head of the dept. of CSE, NMAMIT, Nitte. She is a PhD graduate from the Indian Institute of Science(IISc). She has received her BE and ME qualification from UVCE, Bangalore. She has more than 22 years of experience in teaching, research and industry. Her research interests include Computer architecture, High Performance Computing, and Image processing. She has more than 35 national and international publications. She is a member of the technical committees for various journals and IEEE/ other conferences at national and international level. She is life member of IISc Alumni Association, CSI and ISTE.

Dr. H C Nagaraj, obtained his B.E degree in E&CE from university of Mysore. He obtained his ME in Communication Systems from P.S.G College of Technology, Coimbatore. He has obtained his Doctoral degree in the area of Biomedical Signal Processing and Instrumentation from Indian Institute of Technology, Madras. He has about 32 years of experience in Teaching, Research and Administration. He is presently serving as the principal, Nitte Meenakshi Institute of Technology, Bangalore, India. He has published more than 30 research papers in National and International journals. He has delivered several invited talks in the field of Biomedical Signal Processing, Image Processing and Mobile Communication etc. He is the author of the Book titled "VLSI Circuits" in 2006. His research interests include Biomedical Signal Processing, Image Processing, Soft Computing, Biometrics and Computer Vision. He is a Fellow of the IETE, Life member of Biomedical Engineering Society of India and Member of Global Engineering Deans Council India Chapter (GEDCIC) and also Member of Karnataka State Innovation Council, Government of Karnataka.

A Hybrid Hashing Security Algorithm for Data Storage on Cloud Computing

Noha MM. AbdElnapi

Computer science department

Nahda University

Beni Suef, Egypt

Fatma A. Omara

Computer science department

Cairo University

Cairo, Egypt

Nahla F.Omran

Mathematics department

South Valley University

Qena, Egypt

Abstract— In today's modern IT everything is possible on the web by cloud computing, it allows us to create, configure, use and customize the applications, services, and storage online. The Cloud Computing is a kind of Internet-based computing, where shared data, information and resources are provided with computers and other devices on-demand. The Cloud Computing offers several advantages to the organizations such as scalability, low cost, and flexibility. In spite of these advantages, there is a major problem of cloud computing, which is the security of cloud storage. There are a lot of mechanisms that is used to realize the security of data in the cloud storage. Cryptography is the most used mechanism. The science of designing ciphers, block ciphers, stream ciphers and hash functions is called cryptography. Cryptographic techniques in the cloud must enable security services such as authorization, availability, confidentiality, integrity, and non-repudiation. To ensure these services of security, we propose an effective mechanism with a significant feature of the data. This paper is to show how to improve the security of the Cloud storage using the implementation of a hybrid encryption algorithm and hash functions. It proposes the implementation of two algorithms, Rivest-Shamir-Adleman (RSA) and Advanced Encryption Standard (AES) with a secure hashing algorithm (SHA256) by using Netbeans IDE 8.0.2, JDK 1.7 tool and EyeOS2.5 as a cloud platform on ubuntu14.04.

Keywords— Cloud Computing, Security, Advanced Encryption Standard (AES), Rivest-Shamir-Adleman (RSA), Hybrid Algorithm, Hash functions, Secure Hash Algorithm (SHA256), Encryption, Cryptography, availability, confidentiality, integrity, authorization, and non-repudiation.

I. INTRODUCTION

Cloud computing is the concept of internet based technology, which offers a variety of remote services over the internet such as infrastructure, data storage, software, and hardware. Which mean that applying a broad set of policies, technologies, and controls to protect data, applications, and the associated infrastructure of Cloud Computing technology. The essential principles of the cloud computing are; on-demand computing resources, founding a pay-as-you-go business model for computing and information technology services that you will use, elastic scaling, and elimination of up-front capital and operational expenses. [1]. Security plays the most important role in the cloud and the major concern over the internet in order to serve all the services and benefits of it. Secrecy of the data over the network can be achieved by using cryptography technique which is the process of encryption and hash functions [2].

Converting plain text into a cipher text by using special key is a technique called encryption [3]. There are three common types of encryption algorithms are the implementation of symmetric, asymmetric, and hybrid algorithms that can be used to encrypt data in the cloud computing storage. In symmetric and asymmetric encryption schemes, the data that will be encrypted referred to as plaintext, using an encryption algorithm and generating decrypted text (ciphertext) [4]. A cryptographic hash function takes a message of arbitrary length and creates a message digest of fixed length. A hash function produces short and fixed length message digest, which is unique for each message [5, 6].

Moreover, to enhance Security in the cloud data storage; a hash function with a hybrid encryption algorithm can be used. It is a technique that proposes a concept of the digital signature with the hybrid algorithm, for encrypting the data while it is being transferred over the network.

II. CRYPTOGRAPHY

The science of designing ciphers, block ciphers, stream ciphers and hash functions is called cryptography. Cryptography is critical for the security and integrity of the data that is stored in the cloud. The essential objective of using cryptography is to fulfill the following fundamental information security services:

A. Confidentiality

It aims to avoid unauthorized disclosure of the protected data. Since, various devices and applications can access cloud storage that may cause an increase in the number of access points, which accordingly adds to the threat of unauthorized disclosure [6]. Therefore, to maintain the confidentiality of the data stored in the cloud storage; some methods must be introduced such as encryption [7, 8].

B. Integrity

Integrity is a key component of cloud data storage security, which means that data will be protected against illegal modification and deletion [9]. It is a serious issue in the cloud environment so that authorization mechanisms are applied [10]. The authorization specifies the access rights for every authenticated user to block the unauthorized users. However, due to the increase in access points and system entities, it is essential to be ensured that only authorized entities are allowed to access the protected data [11]. The digital signature is a common method used for ensuring the data integrity on cloud environment [12].

C. Availability

It refers to data, software, but also storage being available to authorized users upon demand at cloud computing environment. Availability includes a cloud system's ability to carry on operations even when some authorities misbehave [13].

D. Authorization

It means to identify who can access information and other computing services. It begins with some specific procedures and administrative policies. The policies recommend what information and computing services can be accessed, by whom, and under what conditions [14].

E. Non-repudiation

It means the ability to ensure that a sender cannot deny the authenticity of his signature on a document or the sending of a message that he originated. In other

words, a sender should not be able to falsely deny later that he sent a message [15].

Cryptography provides different stronger tools and techniques can be used to provide these security services. These techniques are encryption algorithms, digital signature, and hash functions

III. ENCRYPTION ALGORITHMS

A. Symmetric Algorithms

Symmetric key cryptography (private key); uses a common key for both encryption and decryption of data, as shown in figure 1. The most common symmetric key algorithms are: Data Encryption Standard (DES), Triple-DES, International Data Encryption Algorithm (IDEA), Rivest Cipher 4 (RC4), and Advanced Encryption Standard (AES) [16].

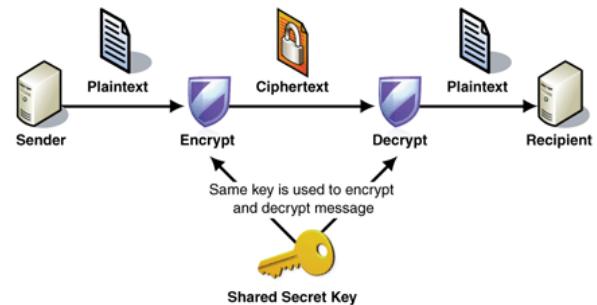


Fig. 1. Symmetric Private Key Cryptography [17].

B. Asymmetric Algorithms

Asymmetric-key cryptography is also known as Public-key cryptography, uses different two keys for encryption and decryption, as shown in figure 2. There are different types of asymmetric algorithms (public key algorithms) such as: RSA, Diffie-Hellman, ElGamal, and so on [18].

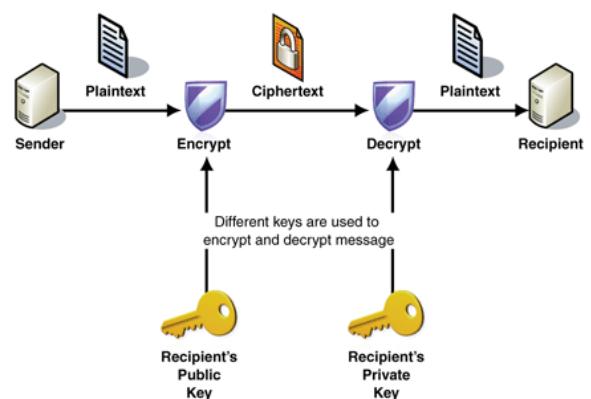


Fig. 2. Symmetric Private Key Cryptography [19].

C. Hybrid Algorithms

Hybrid encryption is a type of encryption that combines two or more encryption algorithms. In other words, it is the process of using either the same or a

different algorithm for encrypting an already encrypted message one or more times. Encryption and decryption provide an easy possibility to use multiple encryptions. Top reasons to use multiple encryptions for most information security and to prevent Brute Force attacks; you can encrypt the same text or file multiple times. Multiple encryptions provide good protection from plaintext attacks, making ciphering stronger [20]. A good example of hybrid encryption/decryption algorithm is that consists of symmetric algorithm such as (AES) and asymmetric algorithm such as (RSA).

IV. LITERATURE REVIEW

A lot of studies and researches have been done to enhance the security of cloud computing storage and environment using encryption and other techniques. The researchers have found the following studies and literature as relevant to the security of cloud computing being proposed.

Vanishreeprasad. S and Mrs. K N Pushpalatha (2015) have improved the data security by proposing an architecture that integrates the cryptographic algorithms, Advanced Encryption Standard (AES) algorithm and the Hash function, SHA-2 [21]. Bernd Gastermann, Markus Stopper, Anja Kossik, and Branko Katalinic (2015) have proposed and implemented a secure cloud storage solution for small and medium-sized enterprises (SMEs) [22]. M. Meenakumari and G. Athisha (2014) have introduced to achieve data integrity and confidentiality during sending data in the cloud by using the technique of combining encryption algorithm (AES) with the hash function (MD5) [23]. B. Sowmya Sri (2013) has proposed a technique for sending data securely in a cloud storage system by using Erasure coding for encoding and RSA, AES algorithms for encryption [24]. Uma Somani, Kanika Lakhani, and Manish Mundra (2010) have Implemented Cloud Storage Methodology to assess Data in the cloud by the Implementation of digital signature with RSA algorithm in a secure manner [25]. Kamara et al. (2010) presented secure cloud storage by using encryption techniques. Using these techniques at first, the data will be indexed then by using symmetric algorithms (AES) with a unique key it will be encrypted. Then by using attribute-encryption scheme and searchable encryption, the unique key and index are encrypted [26].

A. Rivest-Shamir-Adleman (RSA)

The RSA is an algorithm used by modern computers to encrypt and decrypt data stored in the cloud storage. It is a type of an asymmetric cryptographic algorithm. RSA algorithm includes two keys a public key and a private key. The public key is distributed to all so will be known to everyone, it is used to encrypt messages. Messages encrypted with public key only decrypted with private key [27]. RSA can be used for digital signatures, key exchange, or encryption of small block data. The size of the key that is used by RSA algorithm is variable not fixed and also the size of the encryption block. RSA has

been widely used for establishing a secure communications channel and for authentication and the identity of the service provider over insecure communication medium [34]. In proposed scheme RSA algorithm is used to find out the key pair for both mobile user and third party auditor. These keys are used to encrypt and decrypt the file [35]. The following procedures describe the encryption and decryption of RSA [28]:

- Choose random “large” prime integers p and q roughly the same size, but not too close together.
 - Choose a random encryption exponent e less than n that has no factors in common with either $p - 1$ or $q - 1$.
 - Calculate the product $n = p \cdot q$.
 - Calculate $\Phi(n) = (p - 1) * (q - 1)$.
 - Calculate $d = e^{-1} \pmod{\Phi(n)}$.
 - The encryption function is $E(m) = m^e \pmod{n}$, for any message m.
 - The decryption function is $D(c) = c^d \pmod{n}$, where c is the ciphertext.
 - The public key (published with all) is the pair of integers (n, e) .
 - The private key (kept secret) is the triple of integers (p, q, d) .

B. Advanced Encryption Standard (AES)

AES is a symmetric encryption algorithm block cipher that uses cipher keys with lengths of 128, 192, and 256 bits to encrypt data [29]. To use this algorithm for encrypting data; this encryption process consists of 10 rounds for 128 bit keys. All rounds are same except the final round as shown in figure 3. There are four phases are formed each round except the final [30].

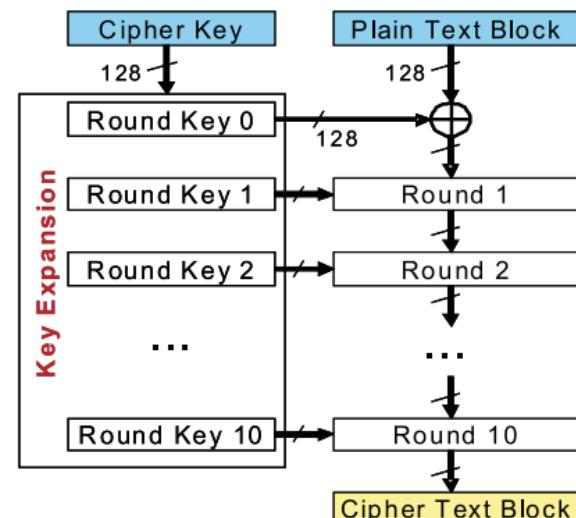


Fig. 3. Structure of AES Algorithm [31]

- SubBytes
- ShiftRows
- MixColumns
- AddRoundKey

C. Secure Hash Algorithm (SHA256)

Hash functions are used in many applications for digital signatures, data integrity, password protection, message authentication, pseudo-random number generation, key derivation, and cryptography protocols [32]. The hash function algorithms compute a fixed length cryptography hash for a given data called the message digest.

V. METHODOLOGY

Such data storage provided by cloud service providers must ensure the main criteria of security which are: confidentiality, privacy, integrity and availability. Confidentiality states to keep data private. Privacy is meant as data leaves the boundaries of the holder. Integrity is a degree of confidence that refers to protect data in the cloud from being modified by unauthorized parties. Availability means that cloud user can able to use the system as predictable.

According to this paper, using combination cryptography encryption algorithms such as the hybrid algorithm (RSA and AES), and hash functions are one of the possible protection solutions for securing cloud storage. The proposed mechanism provides the three security primitives – confidentiality, integrity, and authentication.

The hybrid algorithm proposes/provides more security, scalability and speed which can be provided by a secure system. Performance improvement of AES and RSA has been achieved by implementing the hybrid algorithm. The hybrid encryption algorithm has the advantages of the strength of each form of encryption, which are: the safety of the asymmetric encryption and the speed of the symmetric encryption as well. In addition, using SHA256 to generate a signature with the hybrid algorithm; will achieve the integrity to improve the level of security in the cloud data storage.

The proposed mechanism is taken for implementing hybrid encryption Algorithm with hashing function by using Netbeans IDE 8.0.2, JDK 1.7 tool and EyeOS2.5 as a cloud platform on ubuntu14.04 as follow:

A. Generate the public key using a symmetric algorithm (AES)

This algorithm generates a public key used for encrypting data in the cloud as shown in Figure 4.

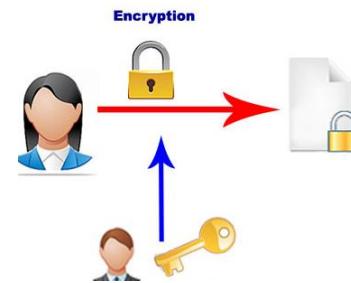


Fig. 4. Encrypt data using AES algorithm [33].

B. Using an asymmetric algorithm (RSA) to generate the secret key

The secret key is used for encrypting the public key as shown in figure 5.



Fig. 5. Encrypt public key using the RSA algorithm.

C. Generating the signature

Secure Hash Algorithm (SHA256) will be used to generate the signature, which will be sent to the recipient with the encrypted file as shown in figure 6.

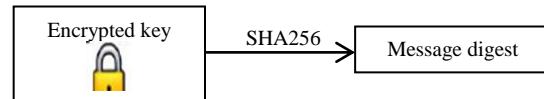


Fig.6. Generating the Signature

D. Signature verification and decryption

The following steps should be done by the recipient to verify the signature and decrypt the file

1) Extracts the message digest of the key file information by using the same hash function.

2) Compute the message digest of the information that has been signed

3) If both message digests are matching, the signature is valid and then he can decrypt the file.

VI. THE IMPLEMENTATION RESULTS

Using different data input sizes (34, 67, and 93) kb, the execution time of encryption for Hybrid and Hybrid-SHA256 algorithms are listed in Table I and presented in Figure 7 and the execution time of decryption is listed in Table II and illustrated Figure 8.

As shown in the experimental results listed in Table I & II, and illustrated in Figure7 and 8; it is found that the encryption and decryption phases using the proposed hybrid-SHA256 algorithm outperforms the Hybrid algorithm in security but it consumes more time than the other.

The computational overhead time is the yardstick in measuring the performance of the mentioned method. The overhead time is defined as the ratio between hybrid-SHA256 to hybrid (AES, RSA) algorithm while measuring its performance with respect to hybrid (AES, RSA) algorithm.

The optimum result obtained from encryption phase is approximately 32% with respect to hybrid (AES, RSA) algorithm, and the optimum results obtained for decryption phase is nearly 33% with respect to hybrid (AES, RSA) algorithm.

The figures show a comparison of total time between hybrid algorithm and new proposed hybrid-SHA256. When comparing with hybrid, proposed model requires more time for encryption and decryption. Whereas proposed model is more secure encryption algorithm than hybrid, because the proposed model includes hashing and digital signature concept, which is more difficult for the intruder to find the plain text from the secret message. Moreover, proposed model provides the three security primitives -- confidentiality, integrity, and non-repudiation.

TABLE I. COMPARISON PERFORMANCE OF ENCRYPTION EXECUTION TIME OF HYBRID (AES, RSA) AND PROPOSED HYBRID-SHA256

Input data size (kb)	Time of execution (ms)		
	Hybrid (AES, RSA)	Hybrid-SHA256	Computation overheads with respect to Hybrid (AES, RSA)
34	365	579	58.63013699 %
67	493	726	47.26166329 %
93	600	801	31.5 %

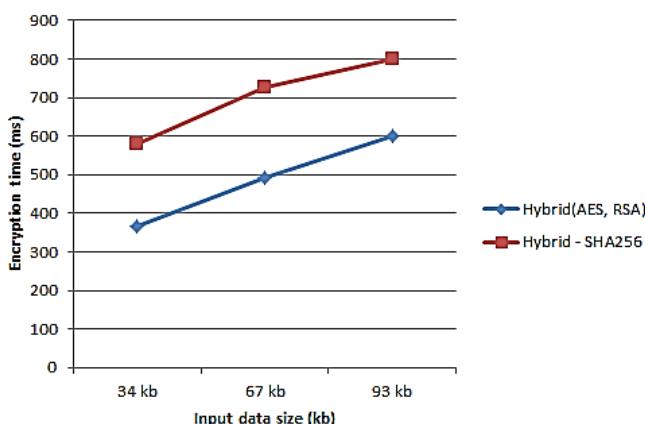


Fig. 7. Encryption execution time of hybrid (AES, RSA) and proposed hybrid-SHA256.

TABLE II. COMPARISON PERFORMANCE OF DECRYPTION EXECUTION TIME OF HYBRID AND PROPOSED HYBRID-SHA256

Input data size (kb)	Time of execution (ms)		
	Hybrid (AES, RSA)	Hybrid-SHA256	Computation overheads with respect to Hybrid
34	270	484	79.25925926 %
67	317	540	70.34700315 %
93	440	577	33.13636364 %

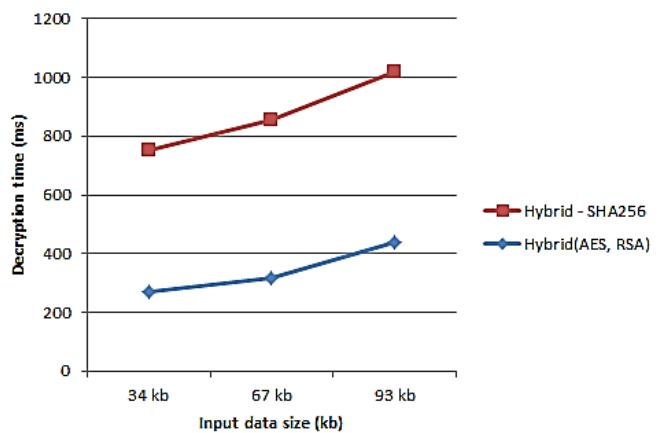


Fig. 8. Decryption execution time of hybrid (AES, RSA) and proposed hybrid-SHA256.

VII. CONCLUSION

Encryption algorithms; symmetric (AES), asymmetric (RSA) and hybrid algorithms are the most algorithms used to encrypt data in the cloud storage in order to make the data more secure from theft. A hash function is the best way to achieve the integrity of data in the cloud environment. Using a combination of cryptography encryption algorithms such as AES and RSA with SHA256 is one of secure and convenient technique for secure data via cloud storage services and achieve the confidentiality, integrity and non-repudiation. In the future, we will try to apply this method using GPU scheduling concepts to reduce the execution time for encryption and decryption phases.

REFERENCES

- [1] Ms. D. Gayatri, Mr. K. B. Rajnish, Mr. N. Kapil, and Mrs. S.N. zaware, "3-D (Dimensional) security in Cloud Computing," International Journal of Computer Science and Information Technology Research, Vol. 2, Issue 2, PP. 47-52, April-June 2014.
- [2] J. , R. , and S. Ajit. "Design and Implementation of New Encryption algorithm to Enhance Performance Parameters." 2278-0661.
- [3] M. , and G. , "Improving Data Storage Security in Cloud using Hadoop," Vol. 4, Issue 9, pp.133-138, September 2014.
- [4] S. , N. , and k. D. Pankaj. "A Hybrid Approach for Encrypting Data on Cloud to prevent DoS Attacks" International Journal of Database Theory and Application Vol. 8.3, pp. 145-154 , 2015.
- [5] P. Suresh, and M. N. Varun Kumar "An efficient model and security framework for data storage in mobile cloud computing using RSA algorithm and hash function," International Journal of Research In Science & Engineering, Vol. 1 ,Issue 2, 2013
- [6] M. , Z. . "Continued Rise of the Cloud". Springer, 2014.
- [7] A. Arasu, K. Eguro, R. Kaushik, R. Ramamurthy "Querying encrypted data". In: IEEE 29th International conference on data engineering (ICDE), Brisbane, 8–12, pp. 1262–1263, April 2013.
- [8] M. Kantarcioğlu, C. Clifton "Security issues in querying encrypted data". In: Jajodia S, Wijesekera D (eds) Data and Applications Security XIX, vol 3654. Springer, Berlin, pp. 325–337, 2005.
- [9] PCI SSC Data Security Standards Overview. https://www.pcisecuritystandards.org/security_standards/.
- [10] N. Santos, KP. Gummadi, R. Rodrigues "Towards trusted cloud computing". In: Proceedings of the 2009 conference on hot topics in cloud computing, USENIX Association, Berkeley, pp. 3–8(2009, June).
- [11] S. Subashini, V. Kavitha "A survey on security issues in service delivery models of cloud computing". J Netw Comput Appl 34(1), pp.1–11, 2011.
- [12] K. Ohta, K. Koyama "Meet-in-the-middle attack on digital signature schemes". In: Seberry J, Pieprzyk J (eds) Advances in cryptology—AUSCRYPT'90. Springer, Berlin, pp. 140–154, (1990, January).
- [13] Z., D. , and L. Dimitrios. "Addressing cloud computing security issues." Future Generation computer systems 28.3, pp. 583-592, 2012.
- [14] C. , M. , A. Jose, et al. "Toward a multi-tenancy authorization system for cloud services." IEEE Security & Privacy vol. 6, pp 48-55, 2010.
- [15] F. , J. , et al. "Analysis of integrity vulnerabilities and a non-repudiation protocol for cloud data storage platforms." Parallel Processing Workshops (ICPPW), 2010 39th International Conference on. IEEE, 2010.
- [16] Zhang, Qi, Lu Cheng, and Raouf Boutaba. "Cloud computing: state-of-the-art and research challenges," Journal of internet services and applications, Vol. 1.1, pp. 7-18, 2010.
- [17] T. , J., and K .Nagesh. "DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis."
- [18] <https://msdn.microsoft.com/en-us/library/ff650720.aspx>
- [19] R. , V. Krishna, B. Thirumala Rao, and L. S. S. Reddy. "Research issues in cloud computing." Global Journal of Computer Science and Technology 11.11, (2011).
- [20] <http://resources.infosecinstitute.com/role-of-cryptography/>
- [21] J. M., et al. " On technical security issues in cloud computing." Cloud Computing, 2009. CLOUD'09. IEEE International Conference on. IEEE, 2009.
- [22] S. Vanishreeprasad , Mrs. K. N. Pushpalatha, " Design and Implementation of Hybrid Cryptosystem using AES and Hash Function "IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) e-ISSN: 2278-2834.p- ISSN: 2278-8735.VOLUME 10, ISSUE 3, Ver. II, PP 18-24 (May - Jun.2015).
- [23] G. , B., et al. "Secure Implementation of an On-premises Cloud Storage Service for Small and Medium-sized Enterprises." Procedia Engineering, Vol. 100, pp. 574-583 ,2015.
- [24] M. , M., and G. Athisha. " Improving Message Authentication by Integrating Encryption with Hash function and its VLSI Implementation." International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering 2.1 (2014).
- [25] B. Sowmya Sri, "A Secure Way for Data Storage and Forwarding in Cloud, "International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue 9, PP. 829-833, September 2013.
- [26] S.Uma, L. Kanika, M. Manish, "Implementing Digital Signature with RSA Encryption to Enhance Data Security of Cloud in Cloud Computing," Parallel Distributed and Grid Computing (PDGC), 1st International Conference, IEEE, 2010.
- [27] S. Kamara, and K. Lauter, "Cryptographic cloud storage", Financial Cryptography and Data Security, Springer Berlin Heidelberg, pp. 136-149, 2010.
- [28] D.Welsh, "Codes and Cryptography, Oxfors Science Publication." (1988).
- [29] Standard, Advance Encryption. "Federal Information Processing Standards Publication 197." FIPS PUB , pp.46-3 ,(2001).
- [30] B. J. , and S. Jean-Pierre. "Fault based cryptanalysis of the advanced encryption standard (AES)." Financial Cryptography. Springer Berlin Heidelberg, 2003.
- [31] H., S. . "Advanced encryption standard (AES)." Network Security, Vol .12 , pp.8-12 , 2009.
- [32] S. , M., and M. Monica. "Enhanced security framework to ensure data security in cloud computing using cryptography." Advances in Computer Science and its Applications, Vol. 1.1, pp. 32-7, 2012.
- [33] <https://www.digicert.com/ssl-cryptography.htm>
- [34] K., Dr Ch., and S. Yogesh. "Enhanced Security Architecture for Cloud Data Security." International Journal of Advanced Research in

International journal of emerging technology and advanced engineering
Vol.1. 2, pp.6-12, 2011.

<https://msdn.microsoft.com/en-us/library/ff650720.aspx>

[19] R. , V. Krishna, B. Thirumala Rao, and L. S. S. Reddy. "Research issues in cloud computing." Global Journal of Computer Science and Technology 11.11, (2011).

[20] <http://resources.infosecinstitute.com/role-of-cryptography/>

[21] J. M., et al. " On technical security issues in cloud computing." Cloud Computing, 2009. CLOUD'09. IEEE International Conference on. IEEE, 2009.

[22] S. Vanishreeprasad , Mrs. K. N. Pushpalatha, " Design and Implementation of Hybrid Cryptosystem using AES and Hash Function "IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) e-ISSN: 2278-2834.p- ISSN: 2278-8735.VOLUME 10, ISSUE 3, Ver. II, PP 18-24 (May - Jun.2015).

[23] G. , B., et al. "Secure Implementation of an On-premises Cloud Storage Service for Small and Medium-sized Enterprises." Procedia Engineering, Vol. 100, pp. 574-583 ,2015.

[24] M. , M., and G. Athisha. " Improving Message Authentication by Integrating Encryption with Hash function and its VLSI Implementation." International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering 2.1 (2014).

[25] B. Sowmya Sri, "A Secure Way for Data Storage and Forwarding in Cloud, "International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue 9, PP. 829-833, September 2013.

[26] S.Uma, L. Kanika, M. Manish, "Implementing Digital Signature with RSA Encryption to Enhance Data Security of Cloud in Cloud Computing," Parallel Distributed and Grid Computing (PDGC), 1st International Conference, IEEE, 2010.

[27] S. Kamara, and K. Lauter, "Cryptographic cloud storage", Financial Cryptography and Data Security, Springer Berlin Heidelberg, pp. 136-149, 2010.

[28] D.Welsh, "Codes and Cryptography, Oxfors Science Publication." (1988).

[29] Standard, Advance Encryption. "Federal Information Processing Standards Publication 197." FIPS PUB , pp.46-3 ,(2001).

[30] B. J. , and S. Jean-Pierre. "Fault based cryptanalysis of the advanced encryption standard (AES)." Financial Cryptography. Springer Berlin Heidelberg, 2003.

[31] H., S. . "Advanced encryption standard (AES)." Network Security, Vol .12 , pp.8-12 , 2009.

[32] S. , M., and M. Monica. "Enhanced security framework to ensure data security in cloud computing using cryptography." Advances in Computer Science and its Applications, Vol. 1.1, pp. 32-7, 2012.

[33] <https://www.digicert.com/ssl-cryptography.htm>

[34] K., Dr Ch., and S. Yogesh. "Enhanced Security Architecture for Cloud Data Security." International Journal of Advanced Research in

Computer Science and Software Engineering, Vol. 3.5, pp. 571-575 ,
2013.

- [35] W. , C. , et al. "Privacy-preserving public auditing for data storage security in cloud computing." INFOCOM, 2010 Proceedings IEEE. Ieee, 2010.

8-neighborhood variant for a better Container Code Extraction and Recognition

Wassim Al-Khawand, Seifedine Kadry, Riccardo Bozzo, Khaled Smaili

Abstract—In this paper, we will present a new variant of the 8-neighborhood connectivity; our approach remedies the segmentation problem related to scratched container code digits. Our approach is highly suitable for real-time automatic container code recognition applications because it treats many special cases, its average response time is equal to 21 milliseconds, and it improves the container code extraction and recognition by 0.89%; due to our contribution in enhancing the segmentation phase, the container code extraction accuracy reached 98.7%.

Keywords— *binary image, 8-neighborhood connectivity, segmentation, Container code.*

I. Introduction

As container ships represent the most dominant transportation mode in the globalized supply chain networks [1] and because the majority of goods is transported via containers, this paper presents a vital approach to extract the container code digits by improving the 8-neighborhood connectivity in order to achieve a faster, more robust, with a higher accuracy for Automatic Container Code Recognition (ACCR) applications.

II. Recent Related Works

In the marine shipping industry, the expected annual container traffic growth is from 4.7% to 7.6% [2], and because ACCR based on computer vision is vital to efficiently manage containers, many researches have recently tackled this subject and emphasized the high importance of the container code digits extraction because it is the cornerstone of the ACCR results; to this end, we will briefly shed the light on some of these recent researches; Sharma and Lee [3] proposed a container code localization method based on object clustering and in order to detect objects in an image, their algorithm used the threshold

binary function to identify white color objects and morphological bot-hat operation for distinguishing black color objects because they assumed that the container code is always printed in black or white color. Chen, Zeng and Wang approach [4] was based on container code localization which consists on the contrast between the container code characters and the background, they applied Otsu's threshold to produce the binary image, and next they used the vertical projection to segment every character within the container-code regions then, they applied refined splitting on the segmented characters, and finally they used pattern recognition based on attribute grid computing. Wu et Al. [5] detailed their two contributions where the first one is the scanline-based algorithm to extract text-line regions which combines the vertical character edges in addition to the spatial relationship between successive characters and their second contribution is a two-step approach in the isolation module to tackle the severity of non-uniform illumination; for segmentation, they suggested using projection method or connected component analysis (in their paper they used vertical projection) and finally, they recognized the container code by converting the segmented character images into characters. Koo and Cha [6] approach consists of a system triggered by cameras and movement detectors in the aim of capturing container images and from these images, they determined the vertical edges using white and black top-hat morphology after Gaussian smoothing and next, they generated seven types of structure windows and they found the position and structure of the ISO-Code through the movement of the spatial structure windows; after that, their system rearranged each part of the ISO-Code into rows and they segmented the characters from the reunion image using binarization and K-Means clustering where they divided the cropped image into three channels and each image is clustered into three classes and finally, the normalized individual characters are recognized using a Back-propagation neural network. Shetty, Caceres, Pastrana, and Rabelo [7] described the advanced container optical character recognition as being composed of three important steps where the first one is the localization of the region of interest for finding and isolating the region on the picture and the second step consists of character segmentation and the final step is the optical character recognition that identifies each character. Chen et Al. [8] proposed a method that consists of a model construction and code recognition stages; in the model construction stage, they started by segmenting the code characters from a training set of container images by incorporating a locally thresholding method with prior knowledge of code character geometry and subsequently, they constructed an Eigen-feature model for each code character based on its segmentation results on the training images; given a container image in the code recognition stage, they segmented the container code characters using the previously mentioned segmentation protocol, then each segmented character is recognized by finding the best matched Eigen-feature model that maintains the minimal reconstruction error of character appearance.

Wassim Al-Khawand
School of Engineering, Sciences and Technologies - University of Genoa
Italy

Seifedine Kadry
School of Engineering – American University of the Middle East
Kuwait

Riccardo Bozzo
Dept. of Electrical, Electronic, Telecommunications Engineering and Naval
Architecture - University of Genoa
Italy

Khaled Smaili
Faculty of Sciences – Lebanese University
Lebanon

K.B. Kim, S. Kim, and Woo [9] proposed a container identifier recognition method via five phases where the first one consists of the container identifier areas extraction, then fuzzy-based noise detection phase is applied which will be followed by the binarization of the container identifier areas phase and next, the 8-directional contour tracking phase is utilized to extract the individual identifiers before the fifth phase that consists of the container identifiers recognition using ART2-based self-organizing supervised learning algorithm.

III. Segmentation

A. Segmentation Overview

Segmentation is one of the main phases for any pattern recognition, ACCR, Optical Character Recognition (OCR), and image analysis and interpretation applications because it partitions an image into different regions where each region contains pixels with similar attributes related to the depicted objects or features of interest; to be more precise, the process of image segmentation assigns a label to every pixel in an image in a way that pixels with the same label share certain characteristics.

Image segmentation can be grouped into contextual or non-contextual techniques where non-contextual techniques don't take into account the spatial relationships between the features of an image but group the pixels on some global attribute basis while, contextual techniques additionally take into account the spatial relationships; worthwhile mentioning that contextual segmentation is better in separating objects because it relies on the closeness of pixels that belong to the object; one of the widely used contextual segmentation technique is the 8-neighborhood pixel connectivity.

B. 8-neighborhood connectivity

The best way to describe the 8-neighborhood region identification is to present its algorithm which is detailed in [10].

First pass: Search the entire image, row by row, and assign a non-zero value to each non-zero pixel $f(i, j)$.

1. If all the neighbors are background pixels (i.e., pixel value zero), $f(i, j)$ is assigned a new (and as yet) unused label.
2. If there is just one neighboring pixel with a non-zero label, assign this label to the pixel $f(i, j)$.

N.B.: Please refer to fig. 1 for neighboring pixels of $f(i, j)$.

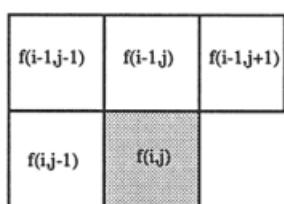


Figure 1. Masks for 8-neighborhood connectivity region identification.

3. If there is more than one non-zero pixel among neighbors (i.e., label collision as showed in fig.

2), assign the label of any one to the labelled pixel and store the label pair in an equivalence matrix.

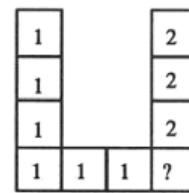


Figure 2. Label collision.

Second pass: The whole image is scanned again, and pixels are re-labelled using the equivalence matrix (i.e., all equivalent labels are replaced by a unique label).

IV. Proposed Method

Before delving into our proposed method, it is worthy to note that neither de-skewing nor binarization of container image techniques will be described in this article because they were previously detailed in the following three papers: Reading skewed images without image rotation [11], A novel skew estimation approach based on same height grouping [12] and, Accurate, swift and noiseless image binarization [13] and this paper is a continuation of them; therefore, we will focus on our contribution to enhance the 8-neighborhood connectivity for a better ACCR results.

A. Challenges

Since our paper is dedicated to container code digits extraction subject to a later recognition, it is worthy to note that container code digits are printed on the external surface of containers and thus, the shapes of digits are often impaired by environmental factors during their transportation by sea and the damage to a container surface, add to it the different noise that may incur, may lead to a distortion of the container code digit shapes [9].

Fig. 3 shows distorted characters by fluid leakage, mud, dust, etc.



Figure 3. Container images taken from real-life scenes.

N.B.: The container code in fig. 3 is located in the first line of each container image (e.g., the container code of the upper left image is MRKU0350091 and the container code of the lower right image is GLDU7531761) and according to ISO-6346 [14], it is composed of 11 digits where the leftmost 4 digits are always capital letters from the Latin alphabet and the rightmost 7 digits are always Hindu-Arabic numerals.

B. Our Work and Contribution

In order to accelerate the 8-neighborhood connectivity, we implemented its second pass by:

1. Avoiding the whole image scanning by creating in the first pass a matrix having the same dimension as the image and which contains the labels assigned in the first pass;
2. Regarding the equivalence matrix: (a) we sort it by ascending order according to the labels to be replaced, (b) we apply transitivity to the equivalence matrix (in our implementation, the highest label value related to the same object will win), (c) we update the label matrix according to the equivalence matrix.

Example: After applying the first pass to the image that only contains the letter W (fig. 4), the label matrix will contain 1 for the cells relative to the left part of the red rectangle, 2 for the cells inside the red rectangle and 3 for the cells relative to the right part of the red rectangle and thus, the equivalence table will contain the two rows: 1-2 and 2-3 which means that the labels 1 should be replaced by 2 and the labels 2 should be replaced by 3 but after applying transitivity, the two rows becomes: 1-3 and 2-3 because the labels 1, 2 and 3 all belongs to the same object W and since 3 is the highest label value related to the same object.



Figure 4. Image containing one object.

Because we were working with real-life images, we had to face the fact that there is a probability that the container code digits will be scratched and thus, the 8-neiborhood segmentation may split any scratched digit; to clarify the problem, let's work on the below two figures (i.e., fig. 5 and fig. 6) where each one is composed of three images (i.e., the leftmost one is the original image, the middle one is the binarized image and the rightmost one is the 8-neighborhood segmentation result image where for readability, each segment is colored differently than its adjacent ones); the sharp eyed reader will notice that the segment related to the rightmost digit 2 of the container code in the fig. 5 is distorted (i.e., split into 2 segments) and the segment related to the digit S related to the container code of the fig. 6 is distorted (i.e., split into 2 segments).



Figure 5. Distorted rightmost digit 2.

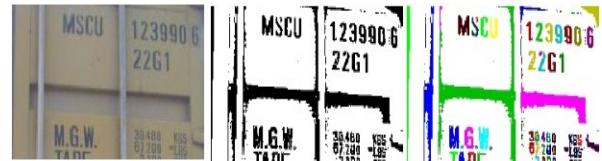


Figure 6. Distorted digit S.

To be more accurate in highlighting the problem, in the:

1. Fig. 5, the two segments that correspond to the rightmost digit 2 are and (actually, the foreground is black and the background is white) so, the first segment will not be recognized by the OCR application as being the number 2 and the second segment will be discarded in the extraction phase because its height is below the minimum required threshold;
2. Fig. 6, the two segments that correspond to the digit S are and (actually, the foreground is black and the background is white) so, the first segment will not be recognized by the OCR application as being the letter S and the second segment will be discarded in the extraction phase because its height is below the minimum required threshold.

To conclude, our contribution, which is ACCR oriented, consists of extending the 8-neighborhood segmentation in a way that the extracted digit will be the surface that elapses from the upper left corner (X_{min}, Y_{min}) of the segment selected as being part of the container code till its lower right corner (X_{max}, Y_{max}) and thus the selected segments will be closer to the reality which consists on the fact that the capital Latin alphabets and Hindu-Arabic numerals have a rectangular shape; to fix the ideas, we will take the same examples of fig. 5 and fig. 6 and the result of the scratched characters will be in respectively and which will be easily recognized by any ACCR application.

Actually, we have also implemented another extension to the 8-neighborhood segmentation which consists of merging two superimposed segments in case the number of the container code segments is lower than eleven (ISO-6346 [14]) or in case the height of the container code digit segment is lower than the other digits, and as long as the height and width of the new segment fall within the required thresholds; to be practical, in case the first superimposed segment has the coordinates $(X^1_{min}, Y^1_{min}, X^1_{max}, Y^1_{max})$ and the second superimposed segment has the coordinates $(X^2_{min}, Y^2_{min}, X^2_{max}, Y^2_{max})$, the merged segment will have the coordinates $(\min(X^1_{min}, X^2_{min}), \min(Y^1_{min}, Y^2_{min}), \max(X^1_{max}, X^2_{max}), \max(Y^1_{max}, Y^2_{max}))$; for example, in the fig. 7 the letter E is scratched and thus the 8-neighborhood segmentation will return the two superimposed segments and while our contribution returns and in the fig. 8, the number 3 is scratched and thus the 8-neighborhood segmentation will return the two superimposed segments and while our contribution returns .

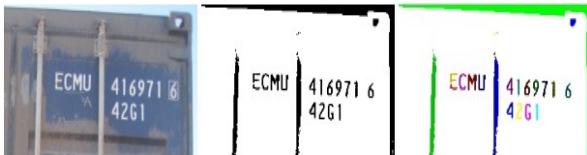


Figure 7. Distorted digit E.



Figure 8. Distorted digit 3.

Remark: As illustrated in the fig. 9, it is essential to highlight that our proposed method also covers the case where the container code color is identical to the container color.

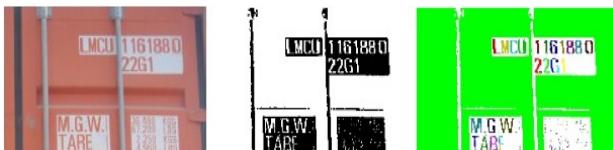


Figure 9. Container code color identical to the container color.

V. Experiments

Our proposed method was tested on 485 images showing the backside of the container images and which belong to 63 different shipping companies; our contribution succeeded to return very good results regarding its accuracy, performance and robustness.

The results of our experiments showed an average response time equals to 21 milliseconds (from a binary image to the container code digits extraction) and complemented the 8-neighborhood connectivity by 0.89% by merging disconnected segments subject to scratched digits.

Fig. 10 illustrates some samples taken from our experimental results where, the first column contains the binary image and the second column contains the eleven segmented container code digits placed one next to the other.

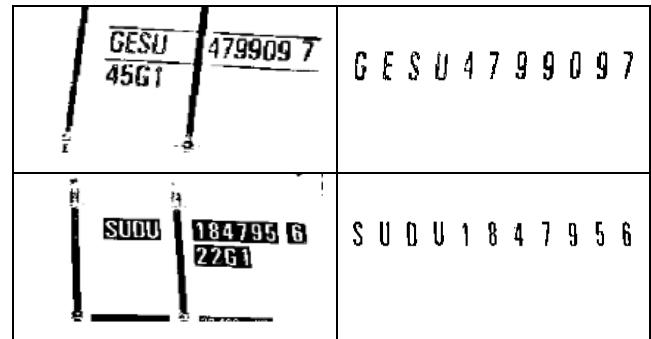
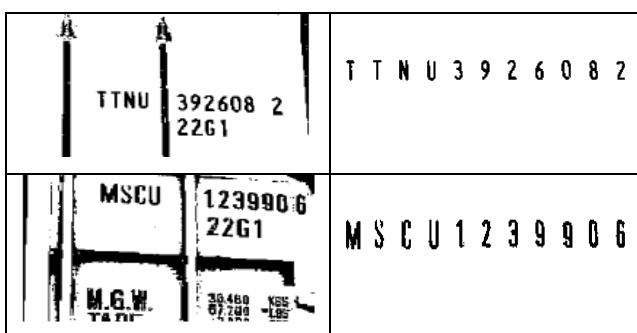


Figure 10. Experiment results.

VI. Application field

Although this paper is intended to enhance the 8-neighborhood connectivity when applied to extract the container code digits for images taken for the back side of the container, but it can also be implemented to extract many other type of images (e.g., container owner name –fig. 11- and vehicle plate –fig. 12-)



Figure 11. Container owner name.



Figure 12. Vehicle plate.

VII. Comparative Study

In the context of container code digits segmentation and extraction, our contribution has many advantages over the recent publications, among them:

1. It doesn't need neither noise removal nor image filtering, while [5, 6, 8, 9] need;
2. It doesn't need a container code region detection independent phase, while [4, 5] need;
3. It isn't disrupted by the presence of parallel lines above and below the container code –fig. 10, third row-, while [4, 5] are disrupted;
4. It doesn't need any image de-skewing, while [3, 4, 5, 8] need;
5. It recognizes the container code even if it is written with the same color as the container background (Fig. 9), while [3, 4, 6, 8] couldn't.

On the other hand, it is worthy to point out some statistical information (e.g., number of container images, system accuracy and response time) concerning our approach versus the other published papers:

1. In our approach 485 damaged or dirty container images were used, while 388 images in [3], 34

- images in [4], 1214 images in [5], 3090 images in [6], 94 images in [8], 79 images in [9];
2. Our approach average container code extraction accuracy is equal to 98.7% , while in [3] 96.16% is the container code region location average accuracy, in [4] 97.97% is the total recognition rate, in [5] 97.94% is the location accuracy and 95.71% is the character extraction accuracy, in [6] 92.15% is the character extraction accuracy, in [8] 88.3% is the segmentation accuracy, in [9] 91.1% is the identifier area extraction accuracy;
 3. Our approach average response time is equal to 21 ms and 92 ms to recognize one container image when using a laptop having a 2.00 GHz processor with 2 GB of RAM, while in [3] 200 ms is the average time of the container code localization with a dual core 4GHz processor having 3GB RAM, in [5] less than 110ms is the average time to recognize a container code when using a Pentium IV 2.4GHz with 1GB RAM, in [6] 240 ms is the average time to recognize one container image when using a dual core 3GHz processor with 4GB RAM, in [8] less than 1 second is the average computational recognition time when using a 3GHz core DUO E8400 processor with 2GB RAM.

VIII. Future Works

Our future works will mainly focus on:

1. Extracting container code digits from videos when one or several containers are passing;
2. Extracting container code digits from infrared images taken during nighttime;
3. Working on a post-segmentation phase in order to solve the attached segment problems due to the mud, fluid leakage, shadows, uneven illumination, etc.; we expect that this phase will improve the whole system accuracy by a minimum of 1% (i.e., the whole system will reach a minimum of 99.7% accuracy with a minimal response time overhead) .

References

- [1] D. Folinas, D. Aidonis, I. Mallidis, and M. Papadopoulou, "Identification of container handling procedures", 2nd Logistics International Conference, 2015.
- [2] Takehara et Al., "Method and apparatus of automated optical container code recognition with positional identification for a transfer container crane", United States Patent No. US 7961911 B2, 2011.
- [3] R. Sharma, and S.R. Lee, "A novel ISO code localization using an object clustering method with OpenCV and Visual Studio application", Modern Education & Computer Science Publisher, DOI:10.5815/ijgsp.2013.07.08, 2013.
- [4] L.D. Chen, W.M. Zeng, and N.Z. Wang, "Container-code pattern recognition based on attribute grid computing", IEEE International Conference on Granular Computing (GrC), 2013.
- [5] W. Wu, et Al., "An automated vision system for container-code recognition", Elsevier, Expert Systems with Applications, Vol. 39, Issue 3, Pages 2842-2855, 2012.
- [6] K.M. Koo, and E.Y. Cha, "A novel container ISO-code recognition method using texture clustering with a spatial structure window",

- International Journal of Advanced Science and Technology, Vol. 41, 2012.
- [7] R. Shetty, R. Caceres, J. Pastrana, and L. Rabelo, "Optical container code recognition and its impact on the maritime supply chain", Math and Engineering Journals, proceedings of the Industrial and Systems Engineering Research Conference, 2012.
 - [8] H.C. Chen, et Al., "A computer vision system for automated container code recognition", Proceedings of the International Multi Conference of Engineers and Computer Scientists, Vol I, 2011.
 - [9] K.B. Kim, S. Kim, and Y.W. Woo, "An intelligent system for container image recognition using ART2-based self-organizing supervised learning algorithm", New Advances in Machine Learning, ISBN 978-953-307-034-6, 2010.
 - [10] M. Sonka, V. Hlavac, and R. Boyle, "Image Processing, Analysis and Machine Vision", ISBN-13: 978-1133593607, 2014.
 - [11] W. Al-Khawand, S. Kadry, R. Bozzo, and K. Smaili, "Reading Skewed Images Without Image Rotation", British Journal of Mathematics & Computer Science, ISSN: 2231-0851, Vol.: 4, Issue.: 7, 2014.
 - [12] W. Al-Khawand, S. Kadry, R. Bozzo, and K. Smaili, "A Novel Skew Estimation Approach Based on Same Height Grouping", International Journal of Signal Processing, Image Processing and Pattern Recognition, Vol.7, No.3, pp.421-432, 2014.
 - [13] W. Al-Khawand, S. Kadry, R. Bozzo, and K. Smaili, "Accurate, swift and noiseless image binarization", IEEE World Symposium on Computer Applications & Research, Italy, 2015.
 - [14] http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=59778

Notification System Based on Face Detection and Recognition: A Novel Approach

Ahmed AbdulQader Al-Bakeri

Faculty of Computing and Information Technology
King Abdulaziz University
Jeddah, Saudi Arabia

Abdullah Ahmad Basuhail

Faculty of Computing and Information Technology
King Abdulaziz University
Jeddah, Saudi Arabia

Abstract— Nowadays, many applications implemented for face detection and recognition are used to achieve different types of projects, whether they are to be used for attendance systems in schools or for the check-in and check-out of employees in an organization. The purpose of this paper is to propose a new notification system using face detection and recognition to notify the house owner of visitors by using the SMTP to send an email containing the names and phone numbers of those visitors. In this system, the camera detects and recognizes the persons in front of the door and then sends their personal information to the host. The theoretical and practical aspects of this system are provided as follows.

Keywords- *Face, Biometric, SMTP, Notification, Face recognition*

I. INTRODUCTION

The human face is an essential part of the human perception system, and is used for practical applications such as surveillance, access control, and criminal identification. Face recognition is considered the most significant part in computer vision and image analysis, and thus it receives much more research in its different components such as the enhancement of its algorithms or new approaches created to better detect and organize the face. The statistical approach is used for calculating the eigenfaces, and the database is presented as a weighted vector. The process of face detection and recognition is performed by converting the face image to the preprocessing image to reduce noise or for any operation of enhancement to image. Then there is selection from the image, which is the first training set of faces. This process is known as Principle Component Analysis (PCA). The second part is recognition, which is performed by projection of a new face after selecting its features into subspace. Classification is used to help determine if it's the actual person, and this is done by comparing the information recorded at that moment with previously stored information. When there is a match, the system will record the name and number of the visitor and send them to the house owner using the SMTP protocol. The faces of persons are used to identify them for security issues or for monitoring the house.

II. PROBLEM STATEMENT

Currently, the topic of security issues has extensively been researched in several branches of computer vision. However, there are different notification systems where doorbells or smart doorbells are used to notify the host about their guests. The use of computer vision equipment is more efficient than the classical method as face recognition is an efficient system in which there is more sufficient contact with the host. This equipment is convenient and based on reliable kits.

III. RELATED WORK

A. Face Recognition

Relying on this technology, many organizations have started using the system of face recognition to effectively manage their employees. In this process, the employee's picture is acquired in front of the camera and the times of attendance are registered. The same process takes place when the employee leaves. In addition, this technology is used to retrieve the person's information by searching for his/her face in the database. Now for operating systems (such as Windows), there are programs that allow users to log on to their computers using (VeriFace-Face Recognition [1]) program with no need to a password.

Face recognition is a kind of biometric application for automatically identifying a person in front of a digital camera. It is essentially used in three major domains: the first use is in attendance systems and management of employee; the second is in visitor-notifying systems; and the third use is in access control systems. This field is one of the most important fields in computer vision, and is used in many applications such as security and access control systems used in high risk areas, right permission in access control systems, and surveillance systems. The recognition process is achieved by comparing the selected features from the face with previous facial information stored in the database.

Geometric or photometric algorithms are the main algorithms used in recognition approaches. The photometric algorithm is a statistical method that extracts image values and compares the obtained values with stored template to

reduce the variances. The popular face recognition algorithm is Principle Component Analysis which uses eigenfaces, Elastic Bunch Graph, Linear Discriminate Analysis, Hidden Markov model and the Multilinear Subspace Learning. Face recognition standard is shown in figure 1 for the access control system for authentication purpose; the use of a database to store facial characteristics of users [2].

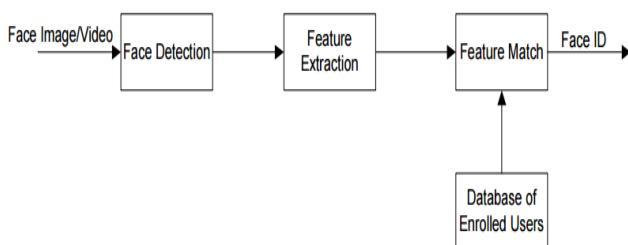


Figure 1: Face Recognition Model [2].

B. Emgu CV

The platform of Emgu CV is .NET to wrap the OpenCV library. The compiled Emgu CV can be opened in Visual Studio and run on Linux, Android and Windows. The latest version of Emgu CV is in 205-05-17; it is available on the website in sourceforge.com, and it has supported the Windows Phone. The code of Emgu is written completely on the basis of C# language and through extensive efforts to have a pure C# application [3].

C. Implementation of Classroom Attendance System Based on Face Recognition in Class

The research in this paper is based on using the method of face detection and recognition to identify a person based on physical attributes of face. This method is used to construct an attendance schedule based on facial features, rather than the traditional time-consuming approach. If the class is about 50 minutes long and traditional recording of attendance takes 5 to 10 minutes, the class instructors and students lose 5 to 10 minutes of class time. To reduce the time it takes to record attendance or to even avoid any time loss from this process, we can use an automatic process to call the roll, a process that is based on face detection and recognition. This part of the database will save the student's name, image, and roll number. This method of taking attendance is convenient and handles the attendance process in a straightforward manner [4].

D. Motion Detection Camera Security System with Email Notification and Live Streaming Using Raspberry Pi

In this paper, the researcher is using the Raspberry Pi, a tiny and affordable computer, developed in UK by Raspberry Pi foundation for the purpose of teaching the basics of computer sciences in schools [5]. The default language supported by Raspberry Pi is Python, but there are other languages that can be used for programming, such as the

java, C, and C++. The Raspberry Pi features the use of camera security in board of Raspberry Pi in the facility. Raspberry Pi's camera security contains motion detection software, where the camera detects the motion and saves the image of person detected. In this paper, the programming is done by using the python script, then the Pi will send email notification messages every time there is a motion detected in front of the camera.

To send an Email notification alert, the SSMTPLib needs to be installed in the OS to allow the sending of emails. The SSMTPLib is a package that grants a system the ability to deliver a message through email from a local computer (mailhost). It is installed by using this command (sudo apt-get install ssmtplib) [6]. System with Face Recognition, SMS Alert and Embedded Network Video Monitoring Terminal. Security

E. Security System with Face Recognition, SMS Alert and Embedded Network Video Monitoring Terminal

The purpose of this paper is to discuss the use of facial recognition technology to allow authorized people to have access to certain areas. If an unauthorized person enters a restricted area, the system will capture a video through the camera. The recognition of person's ID is done by using the PCA algorithm. In the External Sub-sub-system (ESS) the recognition of the face is done by using the MATLAB and two 8-bit micro-controllers for control. The camera captures the person waiting out the door for access and sends their face recognition segment. The ESS architecture involves four components of hardware: the external sensor is used to detect a person in front of the door to have access; the output signal from the external sensor is read through an 8bit Microcontroller; the Principle Component Analysis is used for face recognition based on Eigen-face depending on the MATLAB and OpenCV tools; the camera is located in suitable places to get an accurate image of the individual [7].

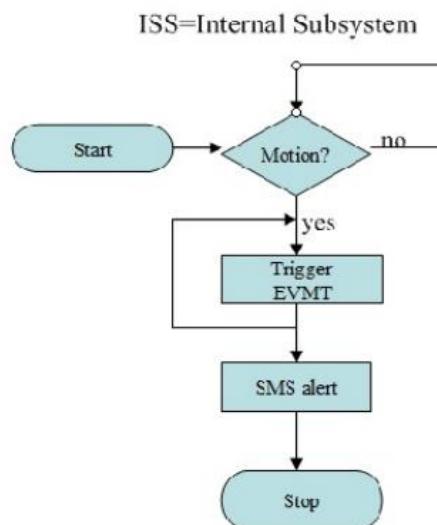


Figure 2: Software Implementation of ISS [7].

IV. METHODOLOGY

A. Proposed System

The aim of this system is to define a new automatic notification system for house owners. Once the system detects and recognizes the face of person in front of the door, the information is directly sent via email to the house owner to notify him about that person. The video is captured by the use of a camera device with suing its ports in the programming part as zero number. The library of Emgu CV is used to wrap the OpenCV in the Environments of C# programming. The process is used to register a person's face in the database as shown in figure 3.

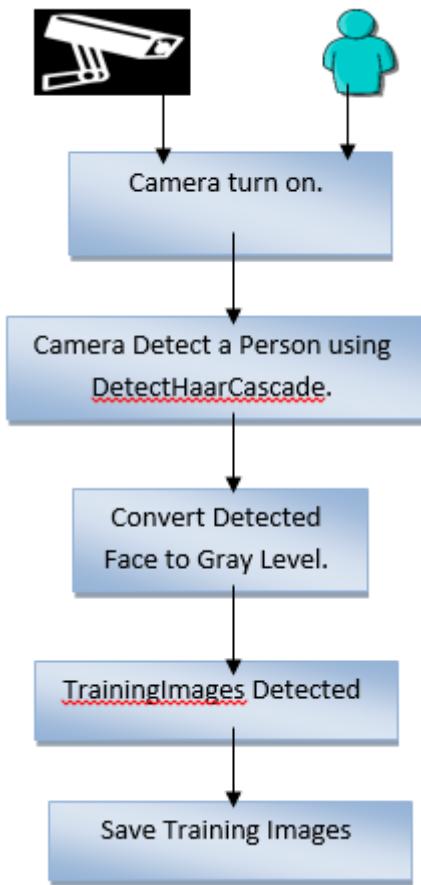


Figure 3: Process of Register the Face.

In the process of recognition the class of Emgu.CV. EigenObjectRecognizer is an object recognizer using PCA (Principle Components Analysis). The person's face is saved in the database. To recognize a newly detected face with the use of a projection against a training image in the database, both images are compared to find similarity. If the person in front of camera is recognized, then the information recorded will be sent to the house owner to notify him of his visitor so that he can know who is in front of his house. This atomic system allows individuals to monitor their house

through their Email. Figure 4 shows how the process is done. The algorithm used in this system is the PCA, which computes:

1- Mean. 2- Covariance Matrix. 3. Eigenvectors v_i and eigenvalues λ_i . 4. Descending Eigenvector by their eigenvalue.

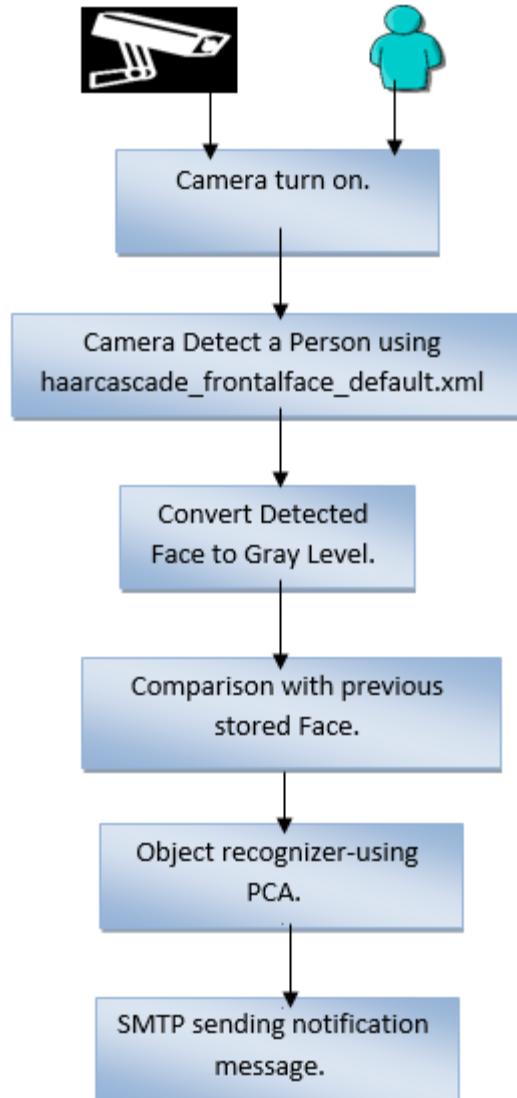


Figure 4: Sending a notification message.

V. SYSTEM DESIGN

A. System Architecture

This architecture consists of computer devices used by the house owner, LAN or MAN network and a face recognition notification application that analyzes stored faces in the database to match the detected face.

B. SMS Architecture

Figure 5 provides an architectural overview for SMS to send notification messages that inform the host of the house about his visitors.

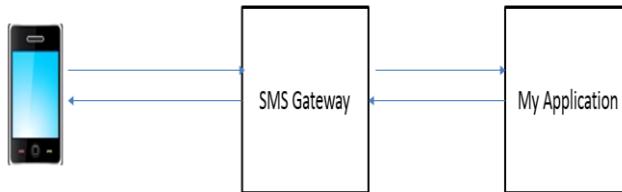


Figure 5: SMS Architecture.

C. Main Interface

Figure 6 shows the system login form. The house owner has the username and password to enter the application. The username and password are connected with the database through the configuration files and uses tableAdabter and the DataSet to reduce the load of connection with the database so the speed of the program is increased.

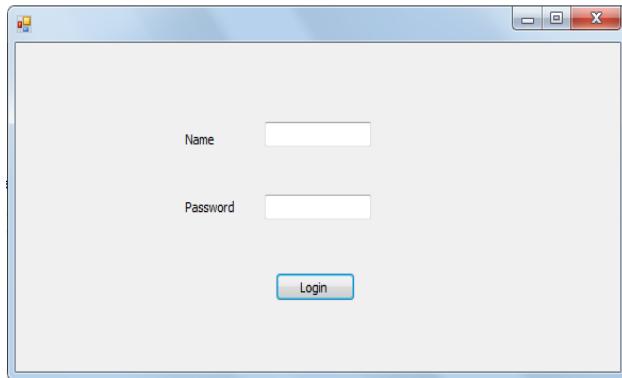


Figure 6: Login Form.

D. Adding Faces to The Database

This interface has the main minus of implementation. The registration of the person in the system is presented in figure 7. First, the camera is turned on to detect the person and then the Add button is pressed to add the detected face to the database.

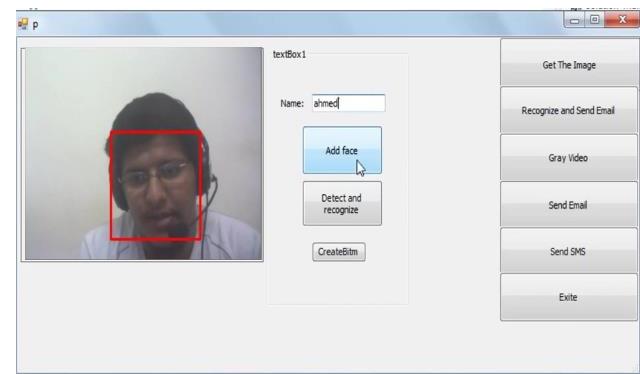


Figure 7: Training the face.

E. Sending Face Detection and Recognition to Email

In the figure 8, the system detects a person in front of the camera and if the person is recognized, his name is shown in the message box. Now this information will be sent to the host's email.

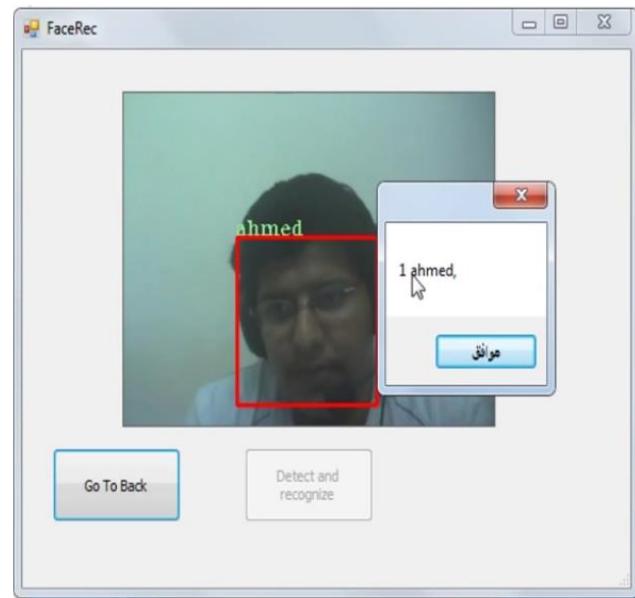


Figure 8: Face Detection and Recognition.

F. Received Message

In figure 9, the notification message is sent to host, using the class of `SmtpClient` `client = new SmtpClient()` to assign the information of the house owner who receives an email message.

The memory stream is used to avoid the use of a disk or to load the information on it.



Figure 9: Notification Message.

G. Gray Level Face Detection

In figure 10, the face captured is in the right side. This form detects the face in front of the door and keeps it until a new face is detected, in which case the last face the camera detected is saved.

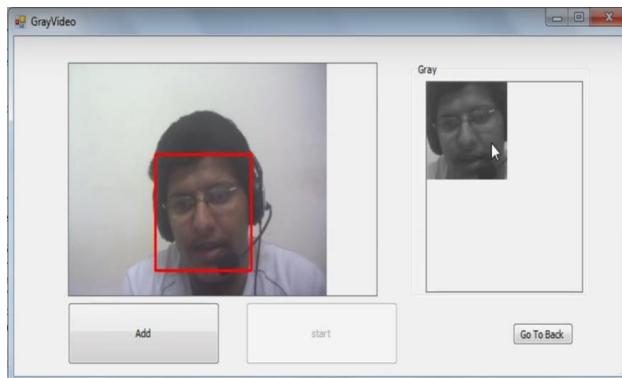


Figure 10: Gray Face Detection.

VI. CONCLUSION

In this paper, we construct a system to help the host know more about the visitor who is outside his house. We provide a new styles form, which based on a useful technique such as OpenCV, Emgu CV, and SMTP. The idea of using face recognition is to achieve an interactive system so that any future maintenance or manipulation of the system architecture can be achieved in a convenient way. This is better than a system that is not based on biometric identification. The gateway in the system works as an outer server to send an SMS or email notification to the house owner to confirm that the process of detection has been completed successfully. In this system, the host can track their visitor through the Email or through an application that depends on face recognition, which is discussed above.

REFERENCES

- [1] Lenovo Face Recognition, <http://lenovoblogs.com/insidethebox/?p=132>
- [2] Nguyen Minh Duc and Bui, Minh," Your face is Not your password.", Ha Noi University of Technology- Viet Nam, security.bkis.vn.
- [3] EMGU CV, http://www.emgu.com/wiki/index.php/Main_Page.
- [4] Implementation of Classroom Attendance System Based on Face Recognition in Class.", International Journal of Advances in Engineering & Technology, July, 2014. Vol. 7, Issue 3, pp. 974-979.
- [5] Raspberry Pi http://en.wikipedia.org/wiki/Raspberry_Pi#cite_note-3.
- [6] Sundas Zafar, Aparicio Carranza, " Motion Detecting Camera Security System with Email Notifications and Live Streaming Using Raspberry Pi", <http://aseene.org/proceedings/2014/Student%20Papers/218.pdf>.
- [7] Kartik S, Kumar R and Srimadhan V.S. "Security System With Face Recognition, Sms Alert And Embedded Network Video Monitoring Terminal", International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 2, No 5, October 2013.

AUTHORS PROFILE

Abdullah Ahmad Basuhail, received the Ph.D. degree in computer engineering from Florida Institute of Technology, Melbourne, FL, USA in 1419H/1998G. His research interests include: digital image processing, computer vision, the use of computer technologies, applications, information technology in e-teaching, e-learning, e-training and e-management supportive systems. Dr. Basuhail was an ex-member of the Saudi Computer Society, the IEEE, and the IEEE Computer Society.



Ahmed AbdulQadir Al-bakeri, received the BSc degree from taibah University, Madinah, Saudi Arabia, in 2013, and then he work as a programmer in (Cooperative Office for Call & Guidance) at Al-Madinah AL munawwarah, currently he working to toward the MSc degree in the department of computer sciences at the university of king abdulaziz. His current research interests are speech recognition (ASR), and human computer interaction.



AndorEstimator: Android based Software Cost Estimation Application

Muhammad Zubair Asghar

Institute of Computing and Information Technology
Gomal University, D.I.Khan, Pakistan

Ammara Habib

Institute of Computing and Information Technology
Gomal University, D.I.Khan, Pakistan

Anam Habib

Institute of Computing and Information Technology
Gomal University, D.I.Khan, Pakistan

Syeda Rabail Zahra

Institute of Computing and Information Technology
Gomal University, D.I.Khan, Pakistan

Sadia Ismail

Institute of Computing and Information Technology
Gomal University, D.I.Khan, Pakistan

Abstract—: The main aim of the proposed system is to assist the software development team to estimate the cost, effort and maintenance of the project under development. Android-based platform, namely MIT App Inventor is used for the development of application, which contains visual block programming language. The current study has following uniqueness of (1)Accuracy of results,(2)user friendly environment(3)no such application is available on android platform to the best of our knowledge. Questionnaire regarding CoCoMo model is developed and circulated by using objective qualitative method. **Findings:** The estimation module of our application is quite important with respect to facilitating the students of software engineering for performing CoCoMo-based cost estimation easily, and enabling the software developers for performing software cost estimation easily. The cost estimator based on CoCoMo model is developed on android platform however, to the best of our knowledge no such application is available. This system can be used by business and educational stakeholders, such as students, software developers, and business organizations

Keywords—CoCoMo model; App Inventor; Cost estimation; Android

I. INTRODUCTION

Development of android-based Conversion and Estimation application can assist the stakeholders related to business and educational sector through the use of smart phones and tablets. The students and software engineers can estimate their project cost, effort, and person per month in the early development of software life cycle.

For the software project management, the software cost assessment is mandatory to reduce the risks and to better

analyze the software development process. The accuracy in estimation of cost also help in decision making. So for this purpose CoCoMo model was developed by using genetic model and ant colony optimization approach to develop the software product by optimizing the current coefficients. In order to find the exact and accurate estimation genetic algorithm is widely used [1]. However in the current era of android based there is a need to develop an android based software cost estimation.

In most of the software effort estimation methodologies that include CoCoMo model were unsuccessful to provide a reliable reference for project manager due to its lack of accuracy. So the Fuzzy expert – CoCoMo model was developed that provide following facilities such as vital information about the estimated effort and also has the ability to not only amalgamate the effort assessment and risk assessment activities into the initial planning phase [2].

To estimate the size, cost and schedule of software projects many refined methods and models are existing. Although for agile software projects the capability to flawlessly predict the software cost of web based software is still doubtful. So Agile MOW approach is presented here in this paper to evaluate effort and cost of software development using agile methodology that is developed for web based projects [3].

In the project planning, software effort estimation is one of the pre-eminent step to be carried out. In order to develop efficient and effective software's accurate estimates are required. For some decades many cost estimation methods have been provided by the software's researchers. As the COCOMO II model is the simplest model so it is commonly used model

among different other models. Also there is no clear benchmark to design neural network model and the fuzzy approach is hard to use. So genetic algorithm has the ability to be a justifiable additional tool for software effort estimation. For optimizing the current coefficients of COCOMO II model this works aim to propose a genetic algorithm in order to achieve more accuracy in estimation [4].

In software development process accurate cost estimation of software project is one of the necessary accomplishment. So it help both the customer and the project manager to make reasonable decisions during project execution. On the other hand there is not much difference between Real Time Software System (RTSS) cost estimation and maintenance cost estimation but for RTSS some critical factors are considered like response time of software for input and processing time to give correct output [5].

For the competitiveness of the software companies the precision and reliability of the estimation of the estimation of the software product is very important. In the management of the software products, good estimates plays a very important rule. So a machine learning method is introduced in this paper which focus to compare machine learning techniques for software effort estimation and to show that robust confidence intervals for the effort estimation can be successfully built [6]. There is an offline application developed to perform CoCoMo based software cost estimation user makes input required for the CoCoMo I calculation and results are obtained [7]. Now a days the use of android is increasing rapidly so android based application for CoCoMo based software cost estimation is required.

The CoCoMo II based calculator is developed to perform cost estimation on the basis of inputs given by the user [8]. As this is an online calculator which require continuous internet connection so this deficiency can be overcome through Android application.

The application, available at [9] is used to perform the basic CoCoMo calculations in all modes: organic, semidetached, embedded.

Another web based system is developed for performing CoCoMo II calculations. The system is available at [10]. As the android application can easily be use for performing CoCoMo II calculations without a need to be online.

The existing literature [11-18] of different studies in text mining are conducted for the development of estimation applications The expansion of android-based application have changed the entire life style of individuals with maximum dependency on the hand-held devices both for entertainment as well as learning. Therefore development of android-based application for software cost estimation is required to facilitate users.

II. METHODOLOGY

The proposed scheme consists of a main module of Software Estimation using CoCoMo model. It is further divided into sub

components particularly: (1) CoCoMo I with basic model, (2) CoCoMo I with intermediate model, (3) CoCoMo I with detailed model, (4) CoCoMo II with early design model, (5) CoCoMo II with Post architecture model.

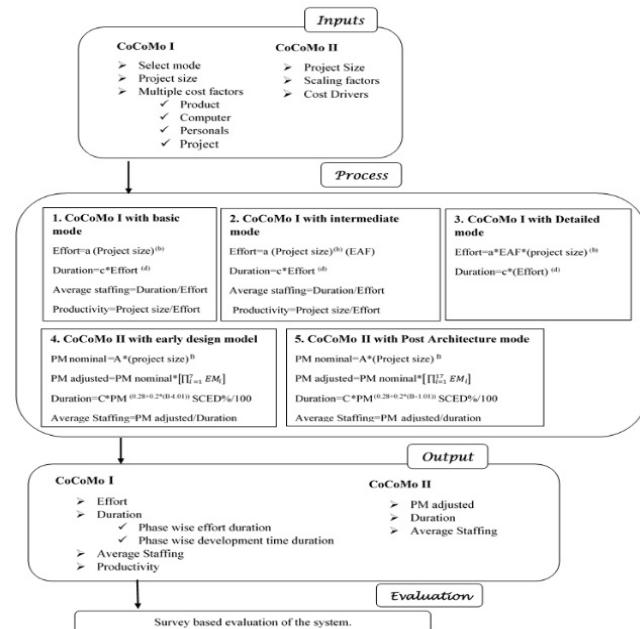


Fig. 1. The proposed system

Fig. 1 presents the execution of proposed system. In the first section inputs are given that are required by the users. The second section is the main section of proposed system in which computation is done where different formulas are used for processing. In the effort and duration equation of CoCoMo I model with basic model, intermediate model and detailed model the term a, b, c and d are constants whose values are given below:

TABLE I. BASIC MODEL

Software Projects	Constant values			
	a	b	c	d
Organic	2.4	1.05	2.5	0.38
Semidetached	3.0	1.12	2.5	0.35
Embedded	3.6	1.20	2.5	0.32

TABLE II. INTERMEDIATE MODEL

Software Projects	Constant values			
	a	b	c	d
Organic	3.2	1.05	2.5	0.38
Semidetached	3.0	1.12	2.5	0.35
Embedded	2.8	1.20	2.5	0.32

TABLE III. DETAILED MODEL

Software Projects	Constant values			
	a	b	c	d
Organic	3.2	1.05	2.5	3.8
Semidetached	3.0	1.12	2.5	3.5
Embedded	2.8	1.20	2.5	3.2

Since in Fig. 1 EAF is the *Effort Adjustment Factor* obtained from the cost drivers. Similarly in CoCoMo II model the term A and C are also constants the values of whom are A=2.94 and C=3.67 where B is a scaling factor and its values is

$$B=0.91+0.1\sum_{i=1}^7 SF_i \quad (1)$$

Where in (1) SF stands for *Scaling Factor*.

$$\prod_{i=1}^7 EM_i \quad (2)$$

Equation (2) shows that there are 7 cost drivers and

$$\prod_{i=1}^{17} EM_i \quad (3)$$

Hence (3) shows that there are 17 cost drivers where EM means *Effort multiplier*. SCED is also a cost driver and it ranges from very low to very high. The third section represents the output of proposed system and survey based evolution is conducted in fourth section.

Now the flow chart of the proposed system is given below:

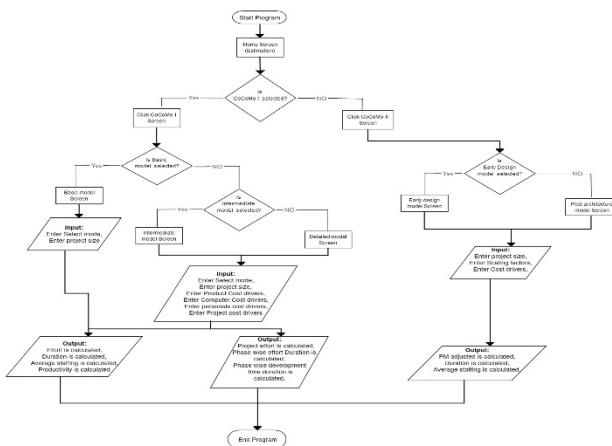


Fig. 2. Flowchart of proposed system

A. CoCoMo I with basic model

The basic CoCoMo I model grants immediate and rough estimates of software cost on time. Users get the needed output of effort, duration, average staffing and productivity by entering the values of select mode and project size.

Algorithm 1. Computation of CoCoMo-I with Basic model

Input: Select mode, Project Size

Output: Effort, Duration, Average Size, Productivity

Begin:

1. If Select mode=Organic then
 2. $Effort \leftarrow 2.4 \times (Project\ Size)^{1.05}$
 3. $Duration \leftarrow 2.5 \times (effort)^{0.38}$
 4. $Average\ Staffing \leftarrow duration / effort$
 5. $Productivity \leftarrow project\ size / effort$
6. If Select mode=Semidetached then
 7. $Effort \leftarrow 3 \times (Project\ Size)^{1.12}$
 8. $Duration \leftarrow 2.5 \times (effort)^{0.35}$

```

9.   Average Staffing  $\leftarrow duration / effort$ 
10.  Productivity  $\leftarrow project\ size / effort$ 
    }
11. If Select mode=Embedded then
    {
12.   Effort  $\leftarrow 3.6 \times (Project\ Size)^{1.20}$ 
13.   Duration  $\leftarrow 2.5 \times (effort)^{0.32}$ 
14.   Average Staffing  $\leftarrow duration / effort$ 
15.   Productivity  $\leftarrow project\ size / effort$ 
    }
End

```

B. CoCoMo I with intermediate model

Intermediate model is an expansion of basic model because it enhances the features of basic model. Firstly, the user choose one of the selection mode (that is organic, semidetached and embedded) then he inputs the value of project size along with various cost drivers specially: (1) Product, (2) Computer, (3) Personals, and (4) Project. These inputs then find out effort, duration, average staffing and productivity which is the required output.

Algorithm 2. Computation of CoCoMo-I with Intermediate model

Input: Select mode, Project Size, Product, Computer, Personals, Project

Output: Effort, Duration, Average Size, Productivity

Begin:

1. If Select mode=Organic then
 2. $Effort \leftarrow 3.2 \times (Project\ Size)^{1.05}$ (EAF)
 3. $Duration \leftarrow 2.5 \times (effort)^{0.38}$
 4. $Average\ Staffing \leftarrow duration / effort$
 5. $Productivity \leftarrow project\ size / effort$
6. If Select mode=Semidetached then
 7. $Effort \leftarrow 3.0 \times (Project\ Size)^{1.12}$
 8. $Duration \leftarrow 2.5 \times (effort)^{0.35}$
 9. $Average\ Staffing \leftarrow duration / effort$
 10. $Productivity \leftarrow project\ size / effort$
11. If Select mode=Embedded then
 12. $Effort \leftarrow 2.8 \times (Project\ Size)^{1.20}$
 13. $Duration \leftarrow 2.5 \times (effort)^{0.32}$
 14. $Average\ Staffing \leftarrow duration / effort$

```

15.    $Productivity \leftarrow project\ size / effort$ 
}
End

```

C. CoCoMo I with detailed model

The detail model covers all the attributes of intermediate model, with an additional feature of calculating phase wise effort duration and phase wise development time duration of the required software. When users make selection from the selection mode (that is, organic, semidetached, and embedded), enters the value of projects size and different cost drivers namely: (1) Product, (2) Computer, (3) Personals, and (4) Project then effort, duration, phase wise effort distribution and phase wise development time duration are determined.

Algorithm 3. Computation of CoCoMo-I with Detailed model

Input: Select mode, Project Size

Output: Effort, Duration, Phase wise effort distribution, Phase wise development time duration.

Begin:

1. If Select mode=Organic then
 2. $Effort \leftarrow 2.4 \times (Project\ Size)^{1.05}$
 3. $Duration \leftarrow 2.5 \times (effort)^{0.38}$
- 4 If Select mode=Semidetached then
 5. $Effort \leftarrow 3 \times (Project\ Size)^{1.12}$
 6. $Duration \leftarrow 2.5 \times (effort)^{0.35}$
7. If Select mode=Embedded then
 8. $Effort \leftarrow 3.6 \times (Project\ Size)^{1.20}$
 9. $Duration \leftarrow 2.5 \times (effort)^{0.32}$
 10. Call mode();
11. Proc mode
 12. If select mode=organic small
 13. Display phase wise effort distribution
 $Plan\ &\ Requirment \leftarrow effort \times 0.06$
 $System\ design \leftarrow effort \times 0.16$
 $Detailed\ design \leftarrow effort \times 0.26$
 $Module\ code\ &\ Test \leftarrow effort \times 0.42$
 $Integration\ &\ Testing \leftarrow effort \times 0.16$
 14. Display phase wise development time duration
 $Plan\ &\ Requirment \leftarrow Duration \times 0.1$
 $System\ design \leftarrow Duration \times 0.19$
 $Detailed\ design \leftarrow Duration \times 0.24$
 $Module\ code\ &\ Test \leftarrow Duration \times 0.39$
 $Integration\ &\ Testing \leftarrow Duration \times 0.18$

```

25. Else
{
26.   Display phase wise effort distribution
     $Plan\ &\ Requirment \leftarrow effort \times 0.06$ 
     $System\ design \leftarrow effort \times 0.16$ 
     $Detailed\ design \leftarrow effort \times 0.24$ 
     $Module\ code\ &\ Test \leftarrow effort \times 0.38$ 
     $Integration\ &\ Testing \leftarrow effort \times 0.22$ 
    Display phase wise development time
     $Plan\ &\ Requirment \leftarrow Duration \times 0.12$ 
     $System\ design \leftarrow Duration \times 0.19$ 
     $Detailed\ design \leftarrow Duration \times 0.21$ 
     $Module\ code\ &\ Test \leftarrow Duration \times 0.34$ 
     $Integration\ &\ Testing \leftarrow Duration \times 0.26$ 
}
47. If select mode=Semidetached medium
{
48.   Display phase wise effort distribution
     $Plan\ &\ Requirment \leftarrow effort \times 0.07$ 
     $System\ design \leftarrow effort \times 0.17$ 
     $Detailed\ design \leftarrow effort \times 0.25$ 
     $Module\ code\ &\ Test \leftarrow effort \times 0.33$ 
     $Integration\ &\ Testing \leftarrow effort \times 0.25$ 
49.   Display phase wise development time duration
     $Plan\ &\ Requirment \leftarrow Duration \times 0.2$ 
     $System\ design \leftarrow Duration \times 0.26$ 
     $Detailed\ design \leftarrow Duration \times 0.21$ 
     $Module\ code\ &\ Test \leftarrow Duration \times 0.27$ 
     $Integration\ &\ Testing \leftarrow Duration \times 0.26$ 
}
60. Else
{
61.   Display phase wise effort distribution
     $Plan\ &\ Requirment \leftarrow effort \times 0.07$ 
     $System\ design \leftarrow effort \times 0.17$ 
     $Detailed\ design \leftarrow effort \times 0.24$ 
     $Module\ code\ &\ Test \leftarrow effort \times 0.31$ 
     $Integration\ &\ Testing \leftarrow effort \times 0.28$ 
62.   Display phase wise development time duration
     $Plan\ &\ Requirment \leftarrow Duration \times 0.22$ 
     $System\ design \leftarrow Duration \times 0.27$ 
     $Detailed\ design \leftarrow Duration \times 0.19$ 
     $Module\ code\ &\ Test \leftarrow Duration \times 0.25$ 
     $Integration\ &\ Testing \leftarrow Duration \times 0.29$ 
}
73. If select mode=Embedded large
{
74.   Display phase wise effort distribution
     $Plan\ &\ Requirment \leftarrow effort \times 0.08$ 
     $System\ design \leftarrow effort \times 0.18$ 
     $Detailed\ design \leftarrow effort \times 0.25$ 
     $Module\ code\ &\ Test \leftarrow effort \times 0.26$ 
     $Integration\ &\ Testing \leftarrow effort \times 0.31$ 
75.   Display phase wise development time duration
     $Plan\ &\ Requirment \leftarrow Duration \times 0.36$ 
}

```

```

82.      System design  $\leftarrow Duration \times 0.36$ 
83.      Detailed design  $\leftarrow Duration \times 0.18$ 
84.      Module code & Test  $\leftarrow Duration \times 0.18$ 
85.      Integration & Testing  $\leftarrow Duration \times 0.28$ 
    }
86. Else
    {
87.     Display phase wise effort distribution
88.     Plan & Requirment  $\leftarrow effort \times 0.08$ 
89.     System design  $\leftarrow effort \times 0.18$ 
90.     Detailed design  $\leftarrow effort \times 0.24$ 
91.     Module code & Test  $\leftarrow effort \times 0.24$ 
92.     Integration & Testing  $\leftarrow effort \times 0.34$ 
93.     Display phase wise development time duration
94.     Plan & Requirment  $\leftarrow Duration \times 0.4$ 
95.     System design  $\leftarrow Duration \times 0.38$ 
96.     Detailed design  $\leftarrow Duration \times 0.16$ 
97.     Module code & Test  $\leftarrow Duration \times 0.16$ 
98.     Integration & Testing  $\leftarrow Duration \times 0.3$ 
}
}
End

```

D. CoCoMo II with early design model

In the primary stages of software project there is slight information about the project size and its nature. So, early design model is used for basic estimates of project's cost and duration. When user inputs the value of (1) project size, (2) scaling factors and (3) multiple cost drivers then he/she gets the desired output of (1) PMnormal, (2) PM adjusted, (3) Duration and (4) Average staffing.

Algorithm 4. Calculation of CoCoMo-II with Early design model

Input: Project Size, Scaling factors, Cost Drivers
Output: PM adjusted, Duration, Average Staffing
Begin:
1. $PM_{nominal} = a \times (Project\ Size)^B$
2. $PM_{adjusted} = PM_{nominal} \times [\pi_{i=1}^7 EM_i]$
3. Duration
$= 3.67 \times PM^{(0.28+0.2 \times (B-1.01))} \frac{SCED\%}{100}$
4. Average Saffing = $PM_{adjusted} / Duration$
}
End

E. CoCoMo II with post architecture model

Post architecture is the most comprehensive model of CoCoMo-II. When the final structure of project is developed then post architecture model is applied and it is also used for maintaining the software product. This model contain the

inputs such as: (1) project size, (2) scaling factors and (3) multiple cost drivers which are then used to get the needed output of (1) PMnormal, (2) PM adjusted, (3) duration and (4) average staffing.

Algorithm 5. Calculation of CoCoMo-II with Post Architecture model

Input: Project Size, Scaling factors, Cost Drivers
Output: PM adjusted, Duration, Average Staffing
Begin:
1. $PM_{nominal} = a \times (Project\ Size)^B$
2. $PM_{adjusted} = PM_{nominal} \times [\pi_{i=1}^7 EM_i]$
3. Duration
$= 3.67 \times PM^{(0.28+0.2 \times (B-1.01))} \frac{SCED\%}{100}$
4. Average Saffing = $PM_{adjusted} / Duration$
}
End

III. EXPERIMENTAL SETUP

The experimental setup section presents details about the implementation and evaluation of the proposed system. As described earlier, we developed the software using MIT App inventor and tested the apps in Blue stack emulator. To evaluate the effectiveness of proposed system, a web-based survey is conducted.

A. Implementation

In Fig. 3, the code block event handler is used in which two procedures are called. In procedure we use if then statement in which we use labels, textboxes and also a spinner code block is used, also some of the blocks are drop from the math Block editor such as Multiply and division.

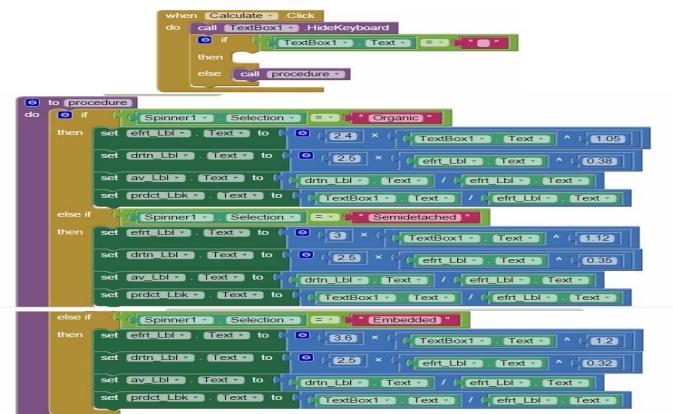


Fig. 3. Code block for CoCoMo I with basic model

Fig. 4 presents the intermediate code blocks which consists of if else statement, procedure, set of labels and also textboxes to execute the instructions.

This screenshot shows a Scratch-style visual programming interface for CoCoMo I. It features a main script starting with 'when Button1 Click' followed by a 'do' loop. Inside the loop, there are several conditional branches ('if' and 'else if') that set various labels (e.g., Eft_Lbl, Dr_Lbl, Efr_Lbl) to different values based on user input from a spinner component named 'Spinner1'. The script also includes calls to procedures like 'call procedure [global EAF v]'. The code uses global variables and text boxes to store intermediate results.

Fig. 4. Code block for CoCoMo I with intermediate model

In the detailed model, Button1 is an event handler which calls two procedures, it also contains labels textboxes and variables. The button contains a spinner component which gives a list of choices from which the user has to make a selection.

This screenshot shows the same visual programming interface as Fig. 4, but with a more detailed model. The main script structure remains the same, but the internal logic for setting labels and variables is more complex, reflecting a deeper level of detail in the model's implementation.

Fig. 5. Code block for CoCoMo I with detailed model

In Fig. 6 the code blocks for early design model that have two procedures, multiple variables and also textboxes are used.

This screenshot shows a Scratch-style visual programming interface for CoCoMo II. It features a main script starting with 'when Call1 Click' followed by a 'do' loop. Inside the loop, there are two main procedures called 'B' and 'C'. Procedure 'B' sets global variables like 'PMad_Lab' and 'Du_Lab' to specific values (e.g., 2.5, 3.67). Procedure 'C' performs calculations involving these variables and other global variables like 'global Sum', 'global Multi', and 'global SCED'. The code uses text boxes to store intermediate results.

Fig. 6. Code block for CoCoMo II with early design model

When calculate button is clicked then a set of instruction inside the event handler are executed. All these instructions are executed in sequence. So it consists of two procedures, set of labels and variables. Fig. 7 shows the following code blocks.

This screenshot shows the same visual programming interface as Fig. 6, but with a post-architectural model. The main script structure remains the same, but the internal logic for setting labels and variables is more complex, reflecting a deeper level of detail in the model's implementation.

Fig. 7. Code block for CoCoMo II with post architectural model

B. Results

We executed our Cost Estimation application using android based platform. Visual block programming language is used for the development of application. Fig. 8 to 12 shows the output screens of main application.



Fig. 8. CoCoMo I with basic model

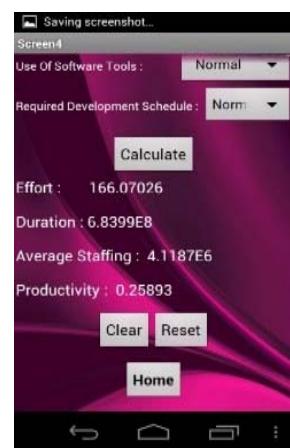


Fig. 9. CoCoMo I with Intermediate model



Fig. 10. CoCoMo I with detailed model

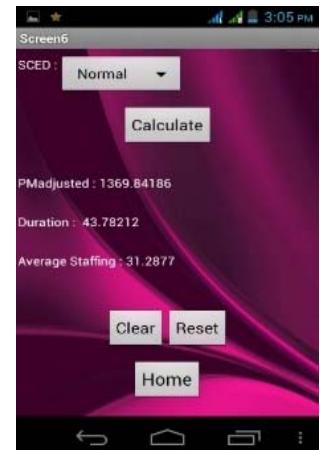


Fig. 11. CoCoMo II with early design model



Fig. 12. CoCoMo II with post architecture model

C. Descriptive Analysis of data

TABLE IV. SHOWING BASIC STATISTICS OF ACCURATE SOFTWARE COST ESTIMATION

Sr.no	Basic Statistics				
	Minimum	Maximum	Median	Mean	Standard deviation
1.	1.00	3.00	2.00	1.90	0.70

The minimum and maximum means the smallest and largest number answer choice that collects not less than one response. It is useful to find the range of answer by subtracting the minimum and maximum. In the Table.IV, minimum and maximum of 1 and 3 presents that there were 6 responses in the uppermost answer (i.e. Strongly agreed) and 4 responses in the lowermost answer (i.e. not agreed).The answer choice that is in the center of all responses shows a median, means there are 50% response before median are smaller and 50% response after median are larger. The median of 2.00 (higher than the 1.90 mean) show that there were more respondents who were agreed than respondents who were strongly agreed. The mean gives the average of entire responses by adding all number answer choices and then divide them by total amount of number. In this case, a mean of 1.90 represents the overall respondents came in somewhere between strongly agreed and the agreed. Finally, the standard deviation shows the growth or alteration of your responses, so here the standard deviation is 0.70.

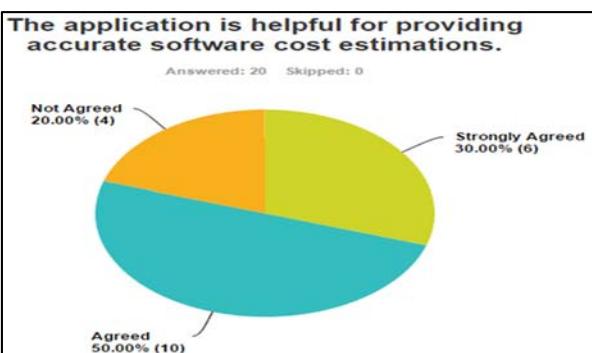


Fig. 13. Pie chart of accurate software cost estimation

Fig. 13 shows that 30% respondents were strongly agreed with the statement, the respondents who were just agreed with the statement were 50% and 20% were not agreed with statement. Prevent from significant loss: The objective of this question was to get information from the respondent that the application is helpful to prevent them know about the significant loss.

TABLE V. SHOWING BASIC STATISTICS OF THE PROJECT EFFORT

Sr.no	Basic Statistics				
	Minimum	Maximum	Median	Mean	Standard deviation
1.	1.00	3.00	2.00	1.80	0.60

In the Table.V, minimum and maximum of 1 and 3 presents that there were 6 responses in the uppermost answer (i.e. Strongly agreed) and 2 responses in the lowermost answer (i.e. not agreed).The median of 2.00 (higher than the 1.80 mean) show that there were more respondents who were agreed than respondents who were strongly agreed. The mean gives the average of all responses. In this case, a mean of 1.80 represents the overall respondents came in somewhere between strongly agreed and the agreed. Finally, the standard deviation shows the growth or alteration of your responses, so here the standard deviation is 0.60.

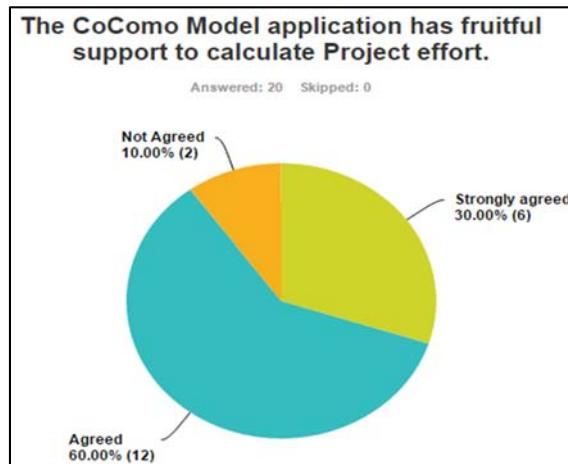


Fig. 14. Pie chart of project effort

The above Fig. 14 shows that the respondents that were strongly agreed with the statement were 30%, whereas 60% respondents were agreed that the application provide support to calculate project effort, while among the 20 respondents feedback 10% respondents were not agreed with the statement.

TABLE VI. SHOWING BAISC STATISTICS OF PREVENT LOSS

Sr.no	Basic Statistics				
	Minimum	Maximum	Median	Mean	Standard deviation
1.	1.00	3.00	2.00	1.80	0.60

In the Table.VI, minimum and maximum of 1 and 3 presents that there were 5 responses in the uppermost answer(i.e.

Strongly agreed) and 4 responses in the lowermost answer(i.e. not agreed).The median of 2.00 (higher than the 1.95 mean) show that there were more respondents who were agreed than respondents who were strongly agreed. In this case, a mean of 1.95 represents the overall respondents came in somewhere between strongly agreed and the agreed. Finally, the standard deviation shows the growth or alteration of your responses, so here the standard deviation is 0.60.

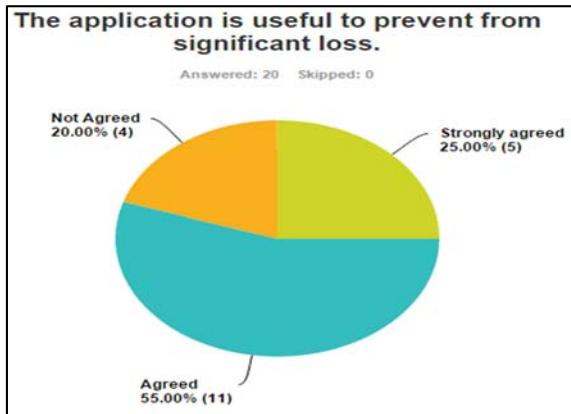


Fig. 15. Pie chart of prevent from significant loss

The above Fig. 15 shows that the respondents that were strongly agreed with the statement were 25%, Agreed respondents were 55% whereas 20 % respondents were not agreed.

TABLE VII. SHOWING BAISC STATISTICS OF THE FINDING APPROXIMATE SLOUTION

Sr.no	Basic Statistics				
	Minimum	Maximum	Median	Mean	Standard deviation
1.	1.00	3.00	2.00	2.00	0.65

In theTable.VII, minimum and maximum of 1 and 3 presents that there were 4 responses in the uppermost answer (i.e. Strongly agreed) and 4 responses in the lowermost answer (i.e. not agreed). The median of 2.00 (equal to the 2.00 mean) show that there were equal number of respondents who were agreed with the statement. In this case, a mean of 2.00 represents the overall respondents came in agreed. Finally, the standard deviation shows the growth or alteration of your responses, so here the standard deviation is 0.65.

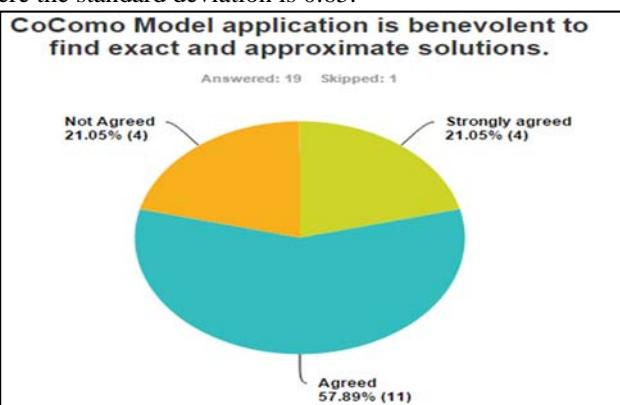


Fig. 16. Pie chart of finding approximate solutions

Fig. 16 shows that the 21.05% respondents were strongly agreed that application is beneficial in terms of finding the exact solutions, 57.89 % respondents were agreed with the statement and 21.05% respondents were not agreed that the application is helpful to find approximate results.

TABLE VIII. SHOWING BASIC STATISTICS OF THE FRIENDLY UER INTEFACE

Sr.no	Basic Statistics				
	Minimum	Maximum	Median	Mean	Standard deviation
1.	1.00	3.00	2.00	1.70	0.56

In theTable.VIII, minimum and maximum of 1 and 3 presents that there were 7 responses in the uppermost answer (i.e. Strongly agreed) and 1 responses in the lowermost answer (i.e. not agreed). The median of 2.00 (higher than the 1.70 mean) show that there were more respondents who were agreed than respondents who were strongly agreed. A mean of 1.70 represents the overall respondents came in somewhere between strongly agreed and the agreed. Finally, the standard deviation shows the growth or alteration of your responses, so here the standard deviation is 0.56.

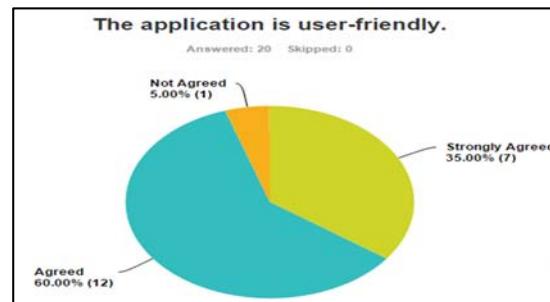


Fig. 17. Pie chart of friendly user interface

Fig. 17 shows that respondents that likes the user interface of the application were 35%, however mostly 60% respondents were found the application is user friendly and only 5% respondents were disagree with the statement.

TABLE IX. SHOWING BASIC STATISTICS OF THE APPROPRIATE EFFORT DURATION

Sr.no	Basic Statistics				
	Minimum	Maximum	Median	Mean	Standard deviation
1.	1.00	3.00	2.00	1.90	0.54

In theTable.IX, minimum and maximum of 1 and 3 presents that there were 4 responses in the uppermost answer(i.e. Strongly agreed) and 2 responses in the lowermost answer(i.e. not agreed). The median of 2.00 (higher than the 1.90 mean) show that there were more respondents who were agreed than respondents who were strongly agreed. A mean of 1.90 represents the overall respondents came in somewhere between strongly agreed and the agreed. Finally, the standard deviation shows the growth or alteration of your responses, so here the standard deviation is 0.54

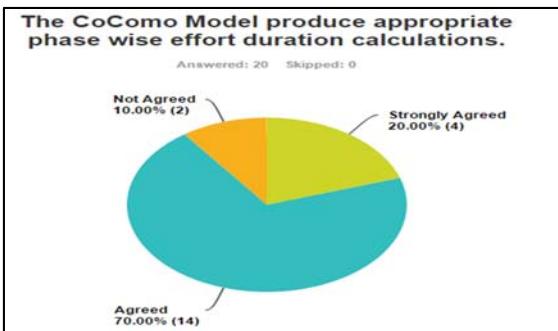


Fig. 18. Pie chart of appropriate effort duration

In the above Fig. 18 shows that 20% respondents were strongly agreed with the statement, the respondents that were agreed with question were 70% and there were just 10% respondents that disagrees with the statement

TABLE X. SHOWING BASIC STATISTICS OF THE UNDERSTANDING OF COCOMO MODEL

Sr.no	Basic Statistics				
	Minimum	Maximum	Median	Mean	Standard deviation
1.	1.00	3.00	2.00	1.95	0.59

In the Table.X, minimum and maximum of 1 and 3 presents that there were 4 responses in the uppermost answer (i.e. Strongly agreed) and 3 responses in the lowermost answer (i.e. not agreed). The median of 2.00 (higher than the 1.95 mean) show that there were more respondents who were agreed than respondents who were strongly agreed. In this case, a mean of 1.95 represents the overall respondents came in somewhere between strongly agreed and the agreed. Finally, the standard deviation shows the growth or alteration of your responses, so here the standard deviation is 0.59

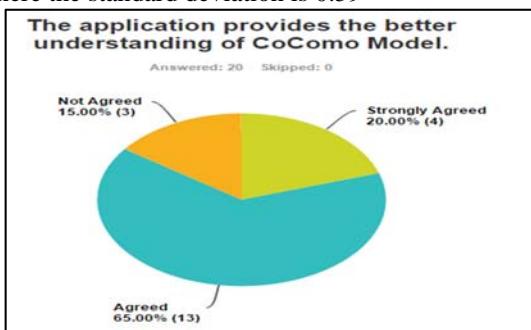


Fig. 19. Pie chart of understanding of CoComo model

Fig. 19 shows that strongly agreed respondent with the statement were 20%, 65% respondents were agreed to the statement, while only 15% respondent do not agree with the statement.

TABLE XI. SHOWING BASIC STATISTICS OF DEVELOPMENT MODE

Sr.no	Basic Statistics				
	Minimum	Maximum	Median	Mean	Standard deviation
1.	1.00	3.00	2.00	1.94	0.64

In the Table. XI, minimum and maximum of 1 and 3 presents that there were 4 responses in the uppermost answer (i.e. strongly agreed) and 3 responses in the lowermost answer (i.e. not agreed). The median of 2.00 (higher than the 1.94 mean) show that there were more respondents who were agreed than respondents who were strongly agreed. In this case, a mean of 1.94 represents the overall respondents came in somewhere between strongly agreed and the agreed. Finally, the standard deviation shows the growth or alteration of your responses, so here the standard deviation is 0.64.

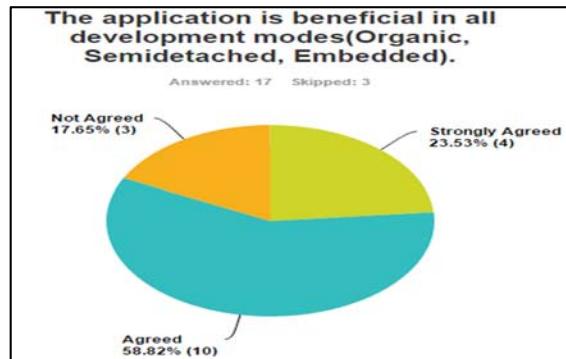


Fig. 20. Pie Chart of development modes

Fig. 20 shows that the respondents that were strongly agreed with the statement were 25.53%, however 58.82% respondents were agreed that the application is benevolent in all development modes and 17.65% respondents were not agreed to the statement

TABLE XII. SHOWING BASIC STATISTICS OF CoCoMo I AND CoCoMo II

Sr.no	Basic Statistics				
	Minimum	Maximum	Median	Mean	Standard deviation
1.	1.00	3.00	1.00	1.60	0.73

In the Table.XII, minimum and maximum of 1 and 3 presents that there were 11 responses in the uppermost answer (i.e. Strongly agreed) and 3 responses in the lowermost answer (i.e. not agreed). The median of 2.00 (higher than the 1.60 mean) show that there were more respondents who were agreed than respondents who were strongly agreed. In this case, a mean of 1.60 represents the overall respondents came in somewhere between strongly agreed and the agreed. Finally, the standard deviation shows the growth or alteration of your responses, so here the standard deviation is 0.73.

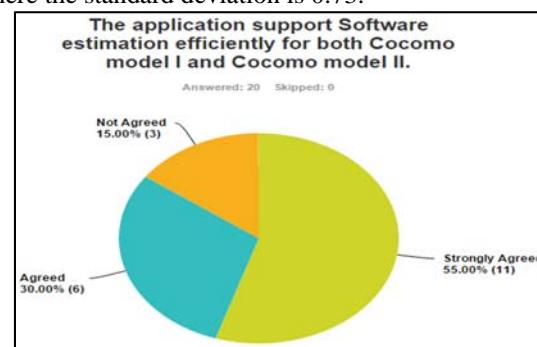


Fig. 21. Pie chart of CoComo I and CoComo II

In Fig. 21 shows that 55% responses were gathered that strongly agreed with the statement, whereas 30% Reponses from the respondents were agreed with the statement, and only 15% respondents disagrees with the statement.

TABLE XIII. SHOWING BASIC STATISTICS OF THE RATE APPLICATION

Sr.no	Basic Statistics				
	Minimum	Maximum	Median	Mean	Standard deviation
1.	1.00	3.00	2.00	2.00	0.65

In the Table.XIII, minimum and maximum of 1 and 3 presents that there were 4 responses in the uppermost answer (i.e. High quality) and 4 responses in the lowermost answer (i.e. Low quality). The median of 2.00 (equal to the 2.00 mean) show that there were equal number of respondents who were agreed with the statement. In this case, a mean of 2.00 shows that overall respondents came in good quality. Finally, the standard deviation shows the growth or alteration of your responses, so Here the standard deviation is 0.65.

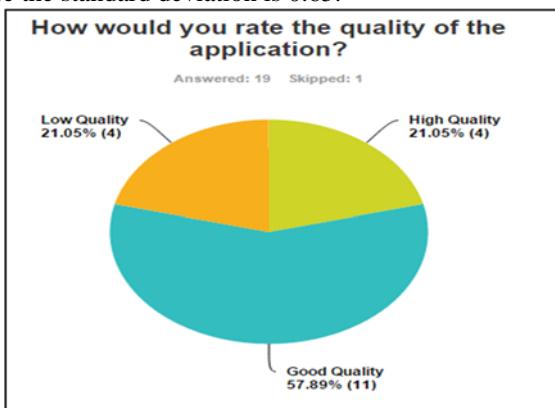


Fig. 22. Pie chart of rate application

Fig. 22 shows respondent that said that the application is of high quality were 21.05%, while 57.89% were said that the application is of high quality and 21.05% respondent found that the application is of low quality.

IV. CONCLUSIONS

This study deals with development of android-based estimation application with focus on developing and integrating the module, name estimation.

The estimation module of our application is quite important with respect to facilitation the students of software engineering for performing CoCoMo-based cost estimation. The application covers both versions of CoCoMo, namely (1) CoCoMo-1, and (2) CoCoMo-II. The distinctive feature of this module is that, to the best of our knowledge, no such application exists in the android-based paradigm. The developed models provide estimation results.

The proposed application is efficient with respect to estimation by using block-oriented programming technique.

Future directions: The application can be enhanced as follows: To implement remaining two models of Cocomo 2, namely (1) application composition model, (2) reuse model.

ACKNOWLEDGMENT

In the name of Allah, the Most Merciful and the Most Gracious, Alhamdulillah, all praises to Allah for the strengths and His Blessings in completing this research paper.

We would like to express our deepest gratitude to our Supervisor Dr. Zubair for his excellent guidance, patience, caring and providing us with an excellent atmosphere for doing our research work

REFERENCES

- [1] www.ijrdo.org/International-Journal.../April-Cse-14
- [2] Manalif, Ekananta. Fuzzy Expert-COCOMO risk assessment and effort contingency model in software project management. Diss. The University of Western Ontario, 2013.
- [3] Litoriya, Ratnesh, and Abhay Kothari. "An efficient approach for agile web based project estimation: AgileMOW." Journal of software engineering and Applications 6.06 (2013): 297.
- [4] Dhiman, Astha, and Chander Diwaker. "Optimization of COCOMO II effort estimation using genetic algorithm." American International Journal of Research in Science, Technology, Engineering & Mathematics 3.2 (2013).
- [5] Chakraverti, Sugandha, et al. Modified Cocomo model for maintenance cost estimation of real time system software. IJCSN, 2012.
- [6] Braga, Petronio L., Adriano LI Oliveira, and Silvio RL Meira. "Software effort estimation using machine learning techniques with robust confidence intervals." Tools with Artificial Intelligence, 2007. ICTAI 2007. 19th IEEE International Conference on. Vol. 1. IEEE, 2007.
- [7] <http://cocomo-calculator.software.informer.com/1.0/>
- [8] <http://cocomo-ii.software.informer.com/1.0/>
- [9] <http://groups.engin.umd.umich.edu/CIS/course.des/cis525/js/f00/kutcher/kutcher.html>
- [10] <http://csse.usc.edu/tools/COCOMOII.php>
- [11] Saqib, Sheikh Muhammad, et al. "Framework for Customized-SOA Projects." International Journal of Computer Science and Information Security 9.5 (2011): 240.
- [12] Ahmad, B., Saqib, S.M., Asghar, M.Z., Jan, M.A. and Ahmad, S., 2011. Concentration on business values for SOA-Services: A Strategy for Service's Business Values and Scope. International Journal of Computer Science and Information Security, 9(5), p.205.
- [13] Ahmad, S., Saqib, S.M., Jan, M.A., Asghar, M.Z. and Ahmad, B., 2011. Reusable Code for CSOA-Services: Handling Data Coupling and Content Coupling. International Journal of Computer Science and Information Security, 9(5), p.196.
- [14] Hussain, Shahid, Muhammad Zubair Asghar, Bashir Ahmad, and Shakeel Ahmad. "A Step towards Software Corrective Maintenance Using RCM model." arXiv preprint arXiv:0909.0732 (2009).
- [15] Jorgensen, M. and Shepperd, M., 2007. A systematic review of software development cost estimation studies. Software Engineering, IEEE Transactions on, 33(1), pp.33-53.
- [16] Asghar, Muhammad Zubair, Maria Qasim, Bashir Ahmad, Shakeel Ahmad, Aurangzeb Khan, and Imran Ali Khan. "HEALTH MINER: OPINION EXTRACTION FROM USER GENERATED HEALTH REVIEWS." International Journal of Academic Research 5, no. 6 (2013).
- [17] Asghar, Muhammad Z., Aurangzeb Khan, Fazal M. Kund, Maria Qasim, Furqan Khan, Rahman Ullah, and Irfan U. Nawaz. "Medical opinion lexicon: an incremental model for mining health

- reviews." International Journal of Academic Research 6, no. 1 (2014): 295-302.
- [18] Asghar, Dr, Muhammad Zubair, and Dr Ahmad. "A Review of Location Technologies for Wireless Mobile Location-Based Services." Journal of American Science 10, no. 7 (2014): 110-118.

Survey of Keystroke Dynamics as a Biometric for Static Authentication.

Mr. Pranit Shinde

Dept. of Computer Engineering
Fr. Conceicao Rodrigues College of
Engineering
Mumbai, India
pspranits10494@gmail.com

Mr. Saideep Shetty

Dept. of Computer Engineering
Fr. Conceicao Rodrigues College of
Engineering
Mumbai, India
ssai.shetty10@gmail.com

Mr .Mahendra Mehra

Dept. of Computer Engineering
Fr. Conceicao Rodrigues College of
Engineering
Mumbai, India
mahendra488@gmail.com

Abstract— Keystroke Dynamics is the study of a user's typing pattern based on the various timing information obtained when a key is pressed and released. It comes under Behavioral Biometrics and has been a topic of interest for authenticating as well as identifying users based on their typing pattern. There have been numerous studies conducted on Keystroke Dynamics as a Biometrics with different data acquisition methods, user base, feature sets, classification techniques and evaluation strategies. We have done a comprehensive study of the existing research and gave our own inference on the topic. In this paper we discuss where the Keystroke Dynamics research currently stands and what scope it has in the future as a biometric application.

Keywords-Keystroke Dynamics, Behavioral Biometrics, User Authentication, Identification, Computer Security.

I. INTRODUCTION

Authentication is the act of verifying a person's claim to be a legitimate user in order to access resources or to gain entry into a system. This is done by comparing a unique secret which is provided by the user during the registration and login process. If the secret matches during both the processes, then the user is said to be a legitimate user. The authentication process is broadly classified into three categories [1].

1. Token: This type of authentication relies on something you have. ATM and Credit Cards employs the use of Token based authentication.
2. Knowledge: This type of authentication relies on something you know. A typical example would be PIN number or username and password. Knowledge based authentication is popular and widely used.
3. Biometrics: This type of authentication relies on something you are and is concerned with various human attributes. Like retina scan, finger print scan, voice recognition etc.

In practice in order to secure a system no single method is foolproof and therefore we need to use a combination of these authentication processes to achieve maximum security. One such process is using ATM card and PIN to withdraw money from an ATM machine. However our primary concern here is with biometric authentication. Many different aspects of human characteristics can be used as a metric for authentication. Fingerprint scanner, Retina scan, Face Recognition, Voice Recognition and Vein Recognition are few of the popular biometric choices used nowadays [1]. Over the past decade or so a new biometric authentication process has been emerging which depends upon the users typing pattern to authenticate and identify a user. Keystroke Dynamics employs the use of a user's timing information recorded during key press and key release also known as keystroke latencies to create a template for each user which would later be compared with the timing information during the login process. If the result fits under a particular threshold then the user is a legitimate user. In this paper we will cover static authentication during login process using keystroke dynamics. The paper is organized in the following way. Section 2 gives a detailed overview of Keystroke Dynamics. Section 3 covers various research conducted on the topic in both statistical as well as neural network. Section 4 shows the problems faced in creating a feasible keystroke dynamics biometric authentication. Section 5 explains the future scope and Section 6 presents our inference on the topic.

II. OVERVIEW OF KEYSTROKE DYNAMICS

A. Behavioral Biometrics

Keystroke dynamics is classified under behavioral biometrics [2]. Behavioral biometrics is based on the psychological attributes of human beings as opposed to the physical traits used in the more traditional biometrics like fingerprint scanner. The assumption here is that each person has a unique typing pattern, and therefore an imposter cannot mimic the typing pattern of a legitimate user [3]. Based on this assumption a static login authentication system can be created

wherein not only the user's password would be verified but also his typing pattern. Thus creating an authentication system which is a combination of knowledge based and behavioral biometrics based system.

B. Static and Dynamic

Keystroke Dynamics can be broadly categorized under two modes of operation. In static mode, the keystrokes of a user are recorded initially during the registration process and later verified for similarity during the login process [5]. In this case the dataset which is provided to the anomaly detector [6] is fixed.

In dynamic mode the task is to ensure that the authorized user is still the same after they have logged in. This can be done by recording the user's keystrokes while the user is interacting with the system. This kind of authentication is also called as continuous authentication [4]. Since the dataset during test phase is arbitrary the anomaly detector also needs to be trained on an arbitrary dataset.

Static authentication can be used in login process for a system, as an access control and to prevent sharing of passwords. Dynamic authentication is mainly used for intrusion detection to ensure the validity of a user throughout the interaction process.

In this paper we focus extensively on static authentication during login process to validate a user. We will deal with various issues concerning with the acquisition of dataset for static process as well as the error caused due to temporal variations in typing pattern of a user.

C. Feature Set

Feature set contains the keystroke metrics used to train, test or retrain the detectors. It is derived from the keystroke timings recorded during the training or test phase. Following are the metrics more popularly used in keystroke dynamics.

Di-Graph latency: Digraph is the timing information obtained from two consecutive keystrokes [7]. It can be categorized into *down-down*: The time delay between a key down press and its consecutive key down press.

$$DD = P_{n+1} - P_n \quad (1)$$

up-down: the time delay between a key release and its consecutive key press.

$$UD = P_{n+1} - R_n \quad (2)$$

hold: the time delay between a key press and its release. This is also known as dwell time.

$$Hold = R_n - P_n \quad (3)$$

Tri-Graph latency: Tri-graph latency is similar to di-graph, however here we use three successive keystrokes to derive the metrics.

N-Graph latency: N-graph can be calculated using more than three keystrokes. It is more popularly known as elapse time between a key and nth-key of a string [8].

$$ET_k = P_n - P_k \quad (4)$$

The above formula is widely used where n-graph is concerned. The total no of vectors created for an n-graph will be (s - n), where s is the sum of all the characters in the string. Since N-graph derives a huge amount of data it is not advisable to use it

where the length of string is huge or unknown as it might generate a large dataset.

D. Data Acquisition.

Data acquisition is the initial stage of keystroke dynamics process. The user is required to type his password during the training phase for a repeated number of times to obtain substantial dataset [6]. The username can also be used as a string along with the password to generate dataset. The length of string may vary, however studies have shown larger inputs give better results. Data can be character-based or numerical or a combination of both. This is to note that for numerical input a standard qwerty keyboard provides two sets of numerical keys 0-9 placed in different positions i.e the num-keys containing numbers as well as the special characters key containing numerals. Therefore the timing data may vary based on which keys have been used by the users. The apparatus required for data acquisition is a keyboard and a keystroke time information recording software. Users might be asked to install the software on their own systems or they may be called to work on the researchers system. The number of data samples required is a major issue in order to create a practical keystroke dynamics application. Since its not feasible to ask the user to repeatedly type the password, the number of repetitions are limited which may result in a smaller dataset.

E. Classification Techniques

Dataset obtained during training and test phase is given to a detector for creating a user template. A detector is a descriptive name given to an anomaly-detector which makes use of classification based techniques to create a user keystroke template [6]. This template is later compared with the results obtained during the test phase to authenticate a user. We will check out in detail two major approaches in classification. Statistical approach is more popularly used pertaining to the fact that it is relatively simple has less overhead and is easy to implement [3][9][10]. Neural network gives more accurate results however the classifier requires both the genuine and imposter dataset [11]. Also the dataset for input needs to be huge which is not feasible for practical implementation.

Statistical techniques

Probabilistic modeling works under the assumption that each keystroke feature vector follows Gaussian distribution [12]. The main concept is to find out what is the probability that a keystroke template belongs to a particular class in this case a user who is registered in the database. Some of the widely used probability modeling techniques is Hidden Markov Model [16], Bayesian Classification [13] [14] [15] and weighted probability [12].

Cluster analysis technique is used to cluster similar characteristic dataset together. The goal is to collect information about keystroke features in order to form a relatively homogeneous cluster. Feature data categorized within a homogeneous cluster are very similar to each other

but highly dissimilar to other clusters. K-means is one of the techniques used for clustering keystroke feature vector [17].

The more popular statistical technique in use is the distance measure. In this technique distance between the training data and test data is calculated and the result is compared with a threshold. If the distance falls within the threshold then the user is a legitimate user. Threshold is calculated using the training dataset and can be adaptive or static. [19] Three most popular distance algorithms are Euclidean distance [18], Manhattan Distance [6] and Mahalanobis distance [6].

We will take a look at each of the distance algorithms in detail.

Euclidean Distance: This is the simplest anomaly-detection algorithm. It considers each password as a single point in an n-dimension space, where n is the number of features in a feature set. In the training phase the dataset obtained can be treated as cloud of points. The squared Euclidean distance of test data from the center of the cloud is calculated. This distance is then compared with threshold to check the legitimacy of the user.

Manhattan Distance: This detector is similar to Euclidean detector; however the distance measure is not Euclidean distance rather it is Manhattan distance. Also known as city block distance or L1 distance it is calculated as,

$$\sum_i^n |x_i - y_i| \quad (5)$$

The Manhattan distance requires simple computation and is robust to the influence of outliers as compared to Euclidean detector or Mahalanobis detector.

Mahalanobis distance: This anomaly-detector takes into account the correlation between the data to correct the heterogeneity and non-isotropy observed in most real data. The squared Mahalanobis distance is calculated as,

$$(x - y)^T S^{-1} (x - y). \quad (6)$$

Where x is the mean of all the training vectors and y is the test vector. S is the covariance matrix of the timing vectors. In the training phase both the covariance matrix and mean vector of training data is calculated. In the test phase the result is calculated as Mahalanobis distance of mean vector and test vector. This result is compared with the threshold for authentication.

Neural Network techniques

A classical neural network structure consists of input layer, output layer and hidden layer. Keystroke data is given as input into the network to produce output based on current state of its initial predetermined weights. These outputs are compared with the actual outputs and error value is calculated. The value is propagated backwards through the network so the weights can be recalculated to reduce error. One major drawback of neural network is that the entire network needs to be retrained if a user is added, removed or updated. Therefore it requires a

large amount of processing. Some of the neural networks used in Keystroke dynamics research are radial basis function network [20], auto-associative, multilayer perceptron [21] and learning vector quantization [22].

F. Performance Measure

The metrics used to access the performance of keystroke dynamics system [23] are,

False Acceptance Rate (FAR): False Acceptance Rate is the probability that the biometric system will incorrectly accept an imposter. It is also known as Type II error.

False Rejection Rate (FRR): False Acceptance Rate is the probability that the biometric system will incorrectly reject a genuine user. It is also known as Type I error.

Equal Error Rate (EER): The rate at which the False Acceptance Rate and False Rejection rate are equal. This is also known as Cross-over error rate. For high accuracy of the biometrics system EER should be lower.

Both FAR and FRR should be as low as possible. If the FAR is high, then unauthorized access would be high which would lead to an unsecure system. Similarly a high FRR will make users annoyed as they cannot log into the system in minimum number of trials.

III. RESEARCH ON KEYSTROKE DYNAMICS

Keystroke dynamics research has been on a rise since the past decade or so. However most of the databases created are proprietary. CMU keystroke dynamics benchmark dataset is publicly available and is one of the important researches conducted in this field [6]. They have compared 14 detectors with a total of 51 subjects. The password used was “tie5Roanl” and was taken 400 times from each subject on different intervals. Joyce and Gupta [9] were the first to use Manhattan distance. They used down-down as the feature set. Their FAR was 0.25 and FRR was 16.36. Bleha et al [14] used Mahalanobis and Euclidean distance with down-down as feature set. The FAR and FRR for Mahalanobis was 2.8 and 8.1. Obaidat & Sadoun [20] got an impressive result of 0 FAR and 0 FRR for neural network based detector. The research was carried out on 15 users. Another neural network based research was conducted by Cho et al [26] by using auto-associative multilayer perceptron algorithm they were able to achieve 0 FAR and 1.0 FRR. Cho et al [24] also used Nearest Neighbor Mahalanobis to achieve a FAR and FRR of 0.0 and 19.5 respectively. Bergadano [25] conducted research on statistical classifier using 154 subjects which gave them a FAR of 0.01 and FRR of 4. The number of subjects was huge and therefore the results reflected improvement for statistical classifier with a low FAR. Thus if substantial user base is present then the statistical classifiers are as good as Neural Network. Because the conditions under which all of these researches have been carried vary hugely, it is impossible to compare them on the same standards. However we have tried to compile most of the important Studies in Keystroke Dynamics in Table I. All of the studies conducted so far have one common goal that is to reduce the FAR and FRR to make keystroke dynamics feasible for practical purposes. However keystroke dynamics being a

behavioral biometrics is constrained by temporal variations which will be discussed in the next section.

Table I. Research conducted on Keystroke Dynamics

Study	Classification	FAR	FRR
Joyce and Gupta [9]	Statistical	0.25	16.36
Bleha et al [14].	Statistical	2.8	8.1
Obaidat & Sadoun [22].	Neural Network	0	0
Cho et al. [26]	Neural Network	0	1
Bergadano et al. [25]	Statistical	0.01	4
Yu & cho [27]	Neural Network	0	3.69
Araujo et al [28]	Statistical	1.89	1.45
Gunnetti & Picardi [29]	Neural Network	0.005	5
Kang et al.[17]	Statistical	3.8	3.8
Pavaday et al.[21]	Neural Networks	1	8
Douhou and Magnus [30]	Statistical	16	1

IV. PROBLEMS IN KEYSTROKE DYNAMICS

Behavioral Biometrics has a major problem of being inconsistent. Typing pattern of a user can become erratic due to many reasons. User may be tired or injured or may be under medication that might affect his typing. Emotions play an important role here since our typing pattern changes when we are flustered or angry. These problems are known as temporal variation and it is one of the reasons why keystroke dynamics fail to give accurate results.

Another problem is that the typing pattern of an individual may change gradually over time. This happens when user gets accustomed to the password, gets adapted to the input device or becomes proficient in typing. This however can be corrected by retraining the detector with new keystrokes each time a user is successful in authentication [17].

V. FUTURE SCOPE

Keystroke Dynamics is the cheapest Biometrics created till now as it only requires a keyboard and keystrokes recording software [6]. It is also a highly transparent process since it doesn't interfere with the user's interaction with the system. In some cases users might not even be aware that they are being secured by an additional biometrics. Users do not have to put in any extra effort in using this biometrics, all they have to do is type the password and the keystroke dynamics system will take care of the authentication. One can say it provides a two-factor authentication with password and the typing pattern. It is very difficult to reproduce the exact keystroke pattern of a user since each person has a unique typing pattern [9]. Even if an attacker gets his hands on the user password he will still be rejected by the biometrics. The only way to bypass Keystroke dynamics is if the attacker somehow gets access to the database storing user's keystroke timing which is impossible. Thus Keystroke Dynamics can be used for websites login process to provide an additional layer of security.

VI. CONCLUSION

Keystroke dynamics has come a long way as a potential biometrics system. Research on Keystroke Dynamics is heading in new direction as focus is given to touch devices. However a lot of work still needs to be done to create a practical biometrics application which will take in account temporal variations and accurately predict if the user is legitimate or not. Being a cheap biometrics gives it an advantage over other traditional biometrics. Furthermore the fact that it works as an added layer of security in combination with Knowledge based authentication like passwords makes it much more effective. In this paper we have tried to summarize Keystroke Dynamics to the best of our knowledge for researchers who are new to this study so they can work on promising research of their own.

REFERENCES

- [1] Lawrence O'Gorman, "Comparing Passwords, Tokens, and Biometrics for User Authentication", Proceedings of the IEEE, Vol. 91, No. 12, Dec, pp. 2019-2040, 2003. J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.
- [2] R.V. Yampolskiy and V. Govindaraju. Behavioral biometrics: a survey and classification. International Journal of Biometrics, 1(1):81–113, 2008.
- [3] R. S. Gaines, W. Lisowski, S. J. Press, and N. Shapiro, "Authentication by keystroke timing: some preliminary results," Tech. Rep. R-2526-NSF, Rand Corporation, Santa Monica, Calif, USA, 1980.
- [4] S. J. Shepherd, "Continuous authentication by analysis of keyboard typing characteristics," in Proceedings of the 1995 European Convention on Security and Detection, pp. 111–114, May 1995.
- [5] John A. Robinson, Vicky M. Liang, J. A. Michael Chambers, and Christine L. MacKenzie, "Computer User verification Using Login String Keystroke Dynamics", IEEE transactions on systems, man, and cybernetics—part a: systems and humans, Vol. 28, No. 2, March 1998.
- [6] K. S. Killourhy and R. A. Maxion, "Comparing anomaly-detection algorithms for keystroke dynamics," in Proceedings of the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN '09), pp. 125–134, July 2009.

- [7] T. Shimshon, R. Moskovich, L. Rokach, and Y. Elovici, "Clustering digraphs for continuously verifying users according to their typing patterns," in Proceedings of the IEEE 26th Convention of Electrical and Electronics Engineers in Israel (IEEEI '10), pp. 445–449, November 2010.
- [8] C.-H. Jiang, S. Shieh, and J.-C. Liu, "Keystroke statistical learning model for web authentication," in Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security (ASIACCS '07), pp. 359–361, Singapore, March 2007.
- [9] R. Joyce and G. Gupta, "Identity authentication based on keystroke latencies," Communications of the ACM, vol. 33, no. 2, pp. 168–176, 1990.
- [10] K. S. Balagani, V. V. Phoha, A. Ray, and S. Phoha, "On the discriminability of keystroke feature vectors used in fixed text keystroke authentication," Pattern Recognition Letters, vol. 32, no. 7, pp. 1070–1080, 2011.
- [11] H. Crawford, "Keystroke dynamics: characteristics and opportunities," in Proceedings of the 8th International Conference on Privacy, Security and Trust (PST '10), pp. 205–212, August 2010.
- [12] F. Monroe and A. Rubin, "Authentication via keystroke dynamics," in Proceedings of the 4th ACM Conference on Computer and Communications Security, pp. 48–56, Zurich, Switzerland, April 1997.
- [13] N. Pavaday and K. M. S. Soyjaudah, "Enhancing performance of Bayes classifier for the hardened password mechanism," in Proceedings of the IEEE Africon 2007 Conference, pp. 1–7, September 20.
- [14] S. Bleha, C. Slivinsky, and B. Hussien, "Computer-access security systems using keystroke dynamics," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 12, no. 12, pp. 1217–1222, 1990.
- [15] R. Giot, M. El-Abed, and C. Rosenberger, "Keystroke dynamics authentication for collaborative systems," in Proceedings of the International Symposium on Collaborative Technologies and Systems (CTS '09), pp. 172–179, May 2009.
- [16] V. V. Phoha, S. Phoha, A. Ray, S. S. Joshi, and S. K. Vuyyuru, "Hidden markov model ("HMM")-based user authentication using keystroke dynamics," U.S. Patent 8136154, March 2012.
- [17] P. Kang, S. S. Hwang, and S. Cho, "Continual retraining of keystroke dynamics based authenticator," in Advances in Biometrics, Proceedings, vol. 4642, pp. 1203–1211, Springer, Berlin, Germany, 2007.
- [18] S. Bhatt and T. Santhanam, Keystroke dynamics for biometric authentication - a survey. In International Conference on Pattern Recognition, Informatics and Mobile Engineering.
- [19] R. O. Duda, P. E. Hart, and D. G. Stork. Pattern Classification. John Wiley & Sons, Inc., second edition, 2001.
- [20] M. S. Obaidat, "Verification methodology for computer systems users," in Proceedings of the 1995 ACM Symposium on Applied Computing, pp. 258–262, February 1995.
- [21] N. Pavaday and K. M. S. Soyjaudah, "Investigating performance of neural networks in authentication using keystroke dynamics," in Proceedings of the IEEE AFRICON 2007 Conference, pp. 1–8, September 2007.
- [22] M. S. Obaidat and B. Sadoun, "Verification of computer users using keystroke dynamics," IEEE Transactions on Systems, Man, and Cybernetics B, vol. 27, no. 2, pp. 261–269, 1997.
- [23] Guven, A. and I. Sogukpinar, "Understanding users' keystroke patterns for computer access security", Computers & Security, 22, 695–706, 2003.
- [24] S. Cho, C. Han, D. H. Han, and H. Kim. Web-based keystroke dynamics identity verification using neural network. Journal of Organizational Computing and Electronic Commerce, 10(4):295–307, 2000.
- [25] Bergando et al, "User Authentication through keystroke Dynamics", ACM transaction on Information System Security" Vol.No. 5, pg 367-397, Nov 2002.
- [26] Cho et al , "Web based keystroke dynamics identity verification using neural network", Journal of organizational computing and electronic commerce, Vol. 10, No. 4, 295-307, 2000.
- [27] E. Yu and S. Cho. GA-SVM wrapper approach for feature subset selection in keystroke dynamics identity verification. In Proceedings of the International Joint Conference on Neural Networks (IJCNN), pages 2253–2257. IEEE Press, 2003.
- [28] L. C. F. Araújo, L. H. R. Sucupira, M. G. Lizarraga, L. L. Ling, and J. B. T. Yabuuti. User authentication through typing biometrics features. In Proceedings of the 1st International Conference on Biometric Authentication (ICBA), volume 3071 of Lecture Notes in Computer Science, pages 694–700. Springer-Verlag, Berlin, 2004.
- [29] Gunetti and Picardi, " Keystroke analysis of free text", ACM Transactions on Information and System Security, volume 8, pages 312–347, 2005.
- [30] S. Douhou and J. R. Magnus, "The reliability of user authentication through keystroke dynamics," Statistica Neerlandica, vol. 63, no. 4, pp. 432–449, 2009.

A Novel Supervised Approach to Detection of Shilling Attack in Collaborative Filtering Based Recommendation System

Krupa Patel
Department of Information Technology,
CSPIT, CHARUSAT,
Anand, India.

Amit Thakkar
Associate Professor,
Department of Information Technology,
CSPIT, CHARUSAT,
Anand, India.

Chandni Shah
Assistant Professor,
Department of Information Technology
CSPIT, CHARUSAT,
Anand, India.

Kamlesh Makvana
Assistant Professor,
Department of Information Technology,
CSPIT, CHARUSAT,
Anand, India.

Abstract— Collaborative filtering is widely used recommendation algorithm to generate variety of recommendation for target users. With increasing popularity of collaborative filtering recommendation, number of users started to insert fake shilling profiles into the system. Due to shilling attack or profile injection attack, accuracy of collaborative filtering recommendation will reduce. This paper attempts to proposed method to detection of shilling attack in collaborative filtering recommendation system using supervised approach. Our proposed method use statistical parameters RDMA, DigSim and LengthVar to identify shilling attack profiles from genuine profile. These parameters are used to train the model for detection of attacker profiles. Then our proposed method will identify genuine profile those are classified as attacker profiles.

Keywords— *Recommendation System, Collaborative Filtering, Shilling Attack, Profile Injection Attack, Supervised Learning, Statistical parameters.*

I. INTRODUCTION

Collaborative filtering provides personalized, variety of recommendation to target users. Having large number of items, it is difficult to find useful items. Hence, collaborative filtering provides or generates recommendation based on ratings of similar users [1][2]. Collaborative filtering algorithm is classified into user-based and item-based collaborative filtering [3][4]. In user-based similarity is calculated between the users to generate recommendation and in item-based similarity is calculated between items to generate recommendation. Collaborative filtering is most widely used algorithm. Collaborative filtering is used by large number of internet e-commerce websites and social media. Example of rating matrix used by collaborative recommendation is shown in Table 1. Set of users is called U and set of item is I. rating given by user $u \in U$ on item $i \in I$ is called r_{ui} . Where, $R = U \times I$. In Table 1. 5 user and 6 items are shown. each cell(u,i) represent rating given by user u on item i .

TABLE 1. U-I Matrix

User (U)	Items (I)					
	I1	I2	I3	I4	I5	I6
U1	5	2		3		
U2	2		4		4	1
U3		1	3		1	
U4	4			1		1
U5	4	3			3	2

With increasing popularity of collaborative filtering based recommendation number of user insert fake rating into rating matrix. Shilling attack or profile injection attack reduce accuracy of collaborative filtering recommendation by inserting fake rating in such a way that system will biased towards intention of attacker. To construct shilling attack profiles attacker use information of rating matrix. To parameters attack size and filler size are used to generate attacker profiles. Attack size is percentage of attack profiles inserted into matrix. And filler size means numbers of items are used as filler items to generate attacker profiles [5][6]. Shilling attacks are classified based on intention (push or nuke) and based on knowledge (random, average, bandwagon, reverse bandwagon, segment etc;) [5]. There are numbers of way to detect shilling profiles are available like statistical measure [7], un-supervised learning, supervised learning etc. Similarity of shilling attack profiles is high with each other then genuine attacker profile so, use of classification to find attacker profile improves detection skills.

Our proposed method takes advantage of this and detects shilling attack profile using classification with statistical attributes. Our proposed method use RDMA, DigSim, LengthVar statistical parameters and perform classification to detect shilling attack profile. Then set of attacker is improved using target item identification by removing those profiles which cannot give rating on target items but classified as attacker profiles.

The rest of the paper is organized as follows. We briefly describe previous related research in Section II. Brief information about shilling attacks is presented in Section III. In the next section IV, we describe our approach in detail.

Finally, we provide our conclusions and future research directions in Section V.

II. RELATED WORK

Number of researchers design various detection scheme based on supervised, un-supervised learning, classification, clustering techniques. In this section we represent existing work in brief and finding and gaps in current research works.

Since, shilling profiles looks like authentic profiles, it is very tough to spot them.[8] Suggest new algorithm known as "Unsupervised Retrieval of Attack Profiles" (UnRAP).They recommend new measure known as Hv-score measure to find shilling profile from genuine profile. They said that Hv-score value of attacker profile is higher than genuine profile. Based on this assumption they identify attacker profile. [9] Extends work of [8] to find group of attacker instead of individual attackers. But both are work well for random and average type of attacks. With help of various detection matrices and analysing rating pattern of attacker [10] Propose unsupervised learning method for detection of fake profile using target item analysis.Algorithm find potential attack profiles using digsim and rdma(Rating Deviation from Mean Agreement) and then refine set of potential profile using target item analysis. Supervised learning is another approach to detect shilling attacks.[11] suggest Ensemble learning concept for shilling attack detection using back propagation neural network classifier, finally output is combined using voting strategy. Use of multiple classifiers to identify fake profiles may reduce efficiency of algorithm. Semi-supervised learning also helpful to detect shilling profiles.[12] Use bisecting k-means algorithm to generate binary decision tree. Intra cluster correlation (ICC) is used to find correlation within cluster between the profiles. This method assumes that attacker profiles in cluster have high ICC between them. And cluster with high value for ICC is considered as attacker cluster. But Performance of this scheme is slightly worse with increasing filler size in segment attack. [13] Detect shilling attacks using clustering social trust information between the users. They propose two algorithms, CluTr and WCluTr, to mix clustering with "trust" among users. According to them user with no incoming trust is considered as attacker profiles. But it may possible that attacker insert fake trust information so this method will not detect that attacker profiles. [14] Use Semi-supervised learning method semi-SAD. Combination of EM- λ and naïve-bayes is used for detection of shilling attacks.

Basic collaborative filtering recommendation algorithms have some problems. These are producing accurate recommendation and Handling many recommendations efficiently. The serious problem like shilling attack reduces accuracy of recommendation system. Supervised learning is more successful then unsupervised learning for detecting shilling attack. Detection of shilling attack is possible but prevention if not possible because when user inserts rating we cannot determine that given user is attacker or not. Most of the research is done to detect random and average shilling attack. But, more shilling attack detection method likes detection of

segment, bandwagon attack need to be developed. Most of the detection scheme work for large attack and filler size. A method that works with different attack size and filler size needed. So we need a method that works with all type of attack with different size.

III. SHILLING ATTACKS

Recommendation schemes are successful in e-commerce sites; they are prone to shilling or profile injection attacks. Shilling attack or profile injection attacks is outlined as,

"Malicious users and/or competitive vendors may attempt to insert fake profiles into the user-item matrix in such a way so they will have an effect on the predicted ratings on behalf of their benefits [7]".

Attack profile for shilling attack is shown in Figure 1.

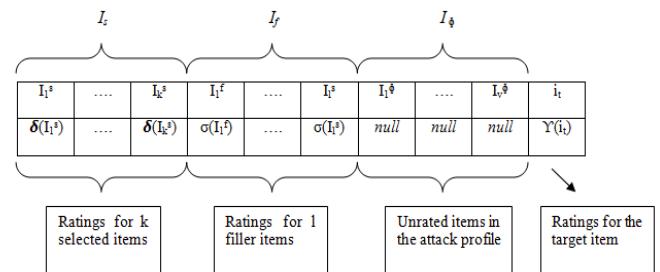


FIGURE 1. ATTACKER PROFILE DESIGN

A. Classification of shilling attacks

Shilling attacks are classified based on intent and based on amount of knowledge required to build shilling attack profiles.

Based on intent shilling attacks are classified as push and nuke attacks. Push attack try to increase popularity of target item by giving high rating to target item. Nuke attack tries to reduce popularity of target item by giving low rating to target item [5].

Based on knowledge required required there are different shilling attack models like average attack, random attack, bandwagon attack, reverse bandwagon, segment attack etc. **Random attacks** operates through attack profiles with ratings for filler items are systems overall mean and r_{max} or r_{min} rating is given to target item for push and nuke attacks, respectively. **Average attack** operates through attack profiles with ratings for filler items are each items mean and r_{max} or r_{min} rating is given to target item for push and nuke attacks, respectively. In random and average attack no selected items are used [7].

Bandwagon or reverse Bandwagon attack An attacker generates profiles with high/low ratings given to popular items and the highest/lowest possible rating to the target item. Filler items are chose randomly and give system mean or item mean as rating. This way injected profile can easily be associated in terms of similarity to other users profile in the system and push/nuke the predictions to the target item [5]. **Segment attack** This is designed to focus on a particular group of users who are likely to buy a specific product. In attack profiles,

attacker inserts high ratings for product the users in the segment probably like and low ratings for others. This way, similarity between users within the segment and injected profiles seems high, and so target item becomes more probably to be suggested [5] [7].

IV. PROPOSED SYSTEM

We proposed system entitled as, "A Novel Supervised Approach to Detection of Shilling Attack in Collaborative Filtering based Recommendation System". This system detects shilling profiles or profile injection attack in collaborative filtering based recommendation by classifies attacker profile using statistical attribute like RDMA, DigSim, LengthVar. And find target item by analyzing rating pattern and improve attacker set. Method works in 3 phases as shown in Figure 2. In pre-processing stage that converts rating data into pre-processed data. Then, learning phase in which classifier model is created and trained and tested. Last is target item analysis phase. This phase improves set of attacker obtain in previous phase.

The objectives of our proposed system are,

- To Identify fake profiles that affect accuracy of collaborative filtering recommendation system.
- To find fake profiles with different attack and filler size.
- To detect different types of shilling attack like random, average, bandwagon, segment attack.
- Improve attacker set by removing genuine attacker using target item identification.
- Reduce false negative value by removing genuine profile from result of classification stage.

A. Description of Proposed System

Consider U-I rating matrix with attacker profiles shown in Table 2 and Diagram is shown in Figure 2.

TABLE 2. U-I MATRIX WITH ATTACKER

	Item1	Item2	Item3	Item4	Item5	Item _n
User1	3		4		2		
User2		1		5			5
User3		1	2			3	
User4	2	4		3			
.....							
Attacker1	3		3		5		
Attacker2		4	3		5		
Attacker3	5		2		5		4
Attacker4	1	3			5		

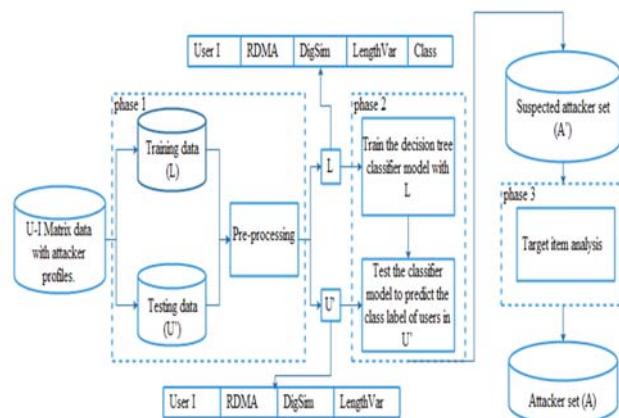


FIGURE 2. FRAME WORK OF PROPOSED SYSTEM

Phase 1: Preprocessing Phase. In this phase input is taken as U-I rating matrix with attacker. after this data is divided into training and testing phase. Training set contain user profile with some attacker profile training set is called as L. and data from testing set contain user profile with no class label known which is called U'. Then for each user profile in L and U' calculate value for statistical variable RDMA, DigSim, LengthVar.

• Rating Deviation from Mean Agreement (RDMA). This measures a user's rating disagreement with other genuine users in the system, weighted by the inverse number of item that user rated. It is defined as,

$$RDMA_u = \frac{\sum_{i=0}^{N_u} |r_{u,i} - Avg_i|}{N_u} \quad (1)$$

Where, N_u is the range of items user u rated, r_{u,i} is the rating given by user u to item i, NR_i is the overall range of ratings in the system given to item i. Avg_i is average rating of item i.

• Degree of similarity (DegSim). Which based on hypothesis that is attacker profiles is highly similar with each other because of theirs characteristics and they are generated with same process [7]. But this profile has low similarity value with genuine profiles. It can be defined as,

$$DigSim_u = \frac{\sum_{v \in \text{neighbors}(u)} W_{u,v}}{k} \quad (2)$$

Where, W_{u,v} similarity (PCC, co-sine) [15] between u and k-nearest neighbours v. and k is number of nearest neighbours of user u.

• Length Variance (LengthVar). This attribute relies on the length of user profile. Most of the attacker enters shilling profile that contains large number of rated items [7]. Thus shilling profile has high value for this attribute. Length Variance (LengthVar) that is a measure of what proportion the length of a given profile varies from the average length within the database. it is defined as,

$$\text{LengthVar}_u = \frac{|n_u - \bar{n}_u|}{\sum_{u \in U} (n_u - \bar{n}_u)^2} \quad (3)$$

Where, n_u is the average length of a profile in the system.

TABLE 3 LABELED DATA (L)

User i	RDMA	DigSim	LengthVar	Class

TABLE 4 UNLABELED DATA (U')

User I	RDMA	Digsim	Lengthvar

Output of this stage is shown in above Table 3, 4. This data is use to generate and train the model in phase 2. In our example shown in table 2 we insert push attack into rating matrix. Phase 1 preprocess the data and represent in form of table 3 and 4.

Phase 2: Model Generation and Testing. This phase classifier model is generated using training data L and tested to predict class label of user profile in U'. For detection of attacker profile we use decision tree classifier model this model use input as attribute values that discussed in phase 1. If value of RDMA and LengthVar for attacker is higher and DigSim value for attacker is lower than genuine profiles. This information is use for train the classifier model then this model is use for prediction of class label of user profiles in U'. And generate suspected attacker set.

Phase 3: Target Item Analysis. Last phase is to improve set of attacker by identifying target item and reduce rate of false positive. By removing user profile that cannot give high rating on target item but still considered as attacker. Target item is considered as item which receives large count for high ratings from most of the attacker profiles than any other item. In our example item 5 is a target item because it receives highest rating from large number of users. After finding target item we remove those profiles from suspected attacker set that cannot give high rating on target item but consider as attacker profile in phase 2.

V. CONCLUSION AND FUTURE WORK

In this paper we propose a novel approach that detects different types of shilling attack in collaborative filtering based recommendation system. The proposal is in the Implementation stage and is completed till the dataset preprocessing. Using the results we are also planning to do a comparative study of the different techniques for detection of shilling attacks in collaborative filtering recommendation. We also evaluate our proposed method with different filler size and attack size variations.

REFERENCES

- [1] D. Almazro, G. Shahatah, L. Albdulkarim, M. Kherees, R. Martinez, and W. Nzoukou, "A Survey Paper on Recommender Systems," 2010.
- [2] G. Adomavicius and A. Tuzhilin, "Toward the next generation of recommender systems: A survey of the state-of-the-art and possible extensions," *IEEE Trans. Knowl. Data Eng.*, vol. 17, no. 6, pp. 734–749, 2005.
- [3] Zheng Wen, "Recommendation System Based on Collaborative Filtering," 2008.
- [4] D. Asanov, "Algorithms and Methods in Recommender Systems," 2011.
- [5] I. Gunes, C. Kaleli, A. Bilge, and H. Polat, "Shilling attacks against recommender systems: a comprehensive survey," *Artif. Intell. Rev.*, pp. 1–33, 2012.
- [6] C. Li and Z. Luo, "Detection of shilling attacks in collaborative filtering recommender systems," *Proc. 2011 Int. Conf. Soft Comput. Pattern Recognition, SoCPaR 2011*, pp. 190–193, 2011.
- [7] R. Burke, B. Mobasher, C. Williams, and R. Bhaumik, "Classification features for attack detection in collaborative recommender systems," *Proc. 12th ACM SIGKDD Int. Conf. Knowl. Discov. data Min. KDD 06*, p. 542, 2006.
- [8] K. Bryan, M. O'Mahony, and P. Cunningham, "Unsupervised Retrieval of Attack Profiles in Collaborative Recommender Systems," *Recsys'08 Proc. 2008 Acm Conf. Recomm. Syst.*, pp. 155–162, 2008.
- [9] G. Lu and S. Engineering, "A GROUP ATTACK DETECTOR FOR COLLABORATIVE FILTERING RECOMMENDATION," *IEEE Internet Comput.*, pp. 2–5, 2014.
- [10] W. Zhou, J. Wen, Y. S. Koh, S. Alam, and G. Dobbie, "Attack Detection in Recommender Systems Based on Target Item Analysis," 2014.
- [11] F. Zhang and Q. Zhou, "Ensemble detection model for profile injection attacks in collaborative recommender systems based on BP neural network," vol. 9, no. October 2013, pp. 24–31, 2015.
- [12] A. Bilge, Z. Ozdemir, and H. Polat, "A novel shilling attack detection method," *Procedia Comput. Sci.*, vol. 31, pp. 165–174, 2014.
- [13] X. L. Zhang, T. M. D. Lee, and G. Pitsilis, "Securing recommender systems against shilling attacks using social-based clustering," *J. Comput. Sci. Technol.*, vol. 28, no. July, pp. 616–624, 2013.
- [14] J. Cao, Z. Wu, B. Mao, and Y. Zhang, "Shilling attack detection utilizing semi-supervised learning method for collaborative recommender system," *World Wide Web*, vol. 16, pp. 729–748, 2013.
- [15] Y. Shi, M. Larson, and A. Hanjalic, "Collaborative Filtering beyond the User-Item Matrix: A Survey of the State of the Art and Future Challenges," *ACM Comput. Surv.*, vol. 47, no. 1, pp. 1–45, 2014.

Privacy Preserving Data Classification using a New Heterogeneous Data Distortion

J. Hyma †, PVGD Prasad Reddy ‡, and A. Damodaram ‡‡

† Department of CSE, GIT, GITAM University, Visakhapatnam, INDIA

‡ Department of CS&SE, AU College of Engineering, Andhra University, Visakhapatnam, INDIA

‡‡ Department of CSE, Sri Venkateswara University, Tirupathy, INDIA

Summary

The new digital technology facilitates us to collect huge amount of data every day. Due to this tremendous growth in size and complexity, two important factors have got the increased attention of all the technology users. One is the complex data analysis that could be done using various data mining methods. The second is privacy concern of the individual towards their data. Privacy Preserving Data Mining (PPDM) is one such process that pays an equal attention towards these two factors. Though there are various techniques in PPDM process, there is no such existing technique that exerts the equal amount of importance on all the roles involved in communication. Our proposed model not only considers the various roles like data owners, data collectors and data users, but also applies the required set of heterogeneous constraints to obtain better privacy protection and better data usability. Heterogeneous constraints used in this work are proposed basing upon the owners willingness to publish the data and existing correlations and privacy analysis carried out by the anonymization framework of the data collector layer.

Key words:

Privacy preserving data mining (PPDM), Heterogeneous constraints, Privacy preserving data classification.

1. Introduction

We all are surrounded by the digital world, which insists us to use smart electronic devices and thus get our desired work done in fraction of seconds. This situation leads to the generation of large volumes of data. The generated data has become a key source for all computational processes. Researchers are continuously trying to use this data efficiently as a powerful input to the desired process and thus extract the useful information. Data mining [1] is one of the powerful technique has been used since several years to extract the useful patterns. This extracted hidden information could be used for several recommendations, predictions and many other personalization purposes [2, 3, 4, 5 and 6]. During this process knowingly or unknowingly some part of personal data is being disclosed. Resolution of HIPAA privacy act, Google privacy violation with street view cars and recently target marketing are well known examples for this sort of privacy

violation. Because of such violations, individuals came to know the drawbacks and its further consequences with their excessive data sharing. It also raised a genuine concern of their data and convinced them not to share data with anybody for any purpose. But what if nobody shares their data? Can we collect wide measurements that are required for so many studies without this data? The answer is obviously no. As a solution PPDM process has been originated [7, 8]. The goal of PPDM is to equally balance the data utility and data privacy by performing data mining efficiently while preserving the privacy. In order to do this, PPDM has provided with various types of approaches [9, 10, and 11]. The categorization is shown in figure [1].

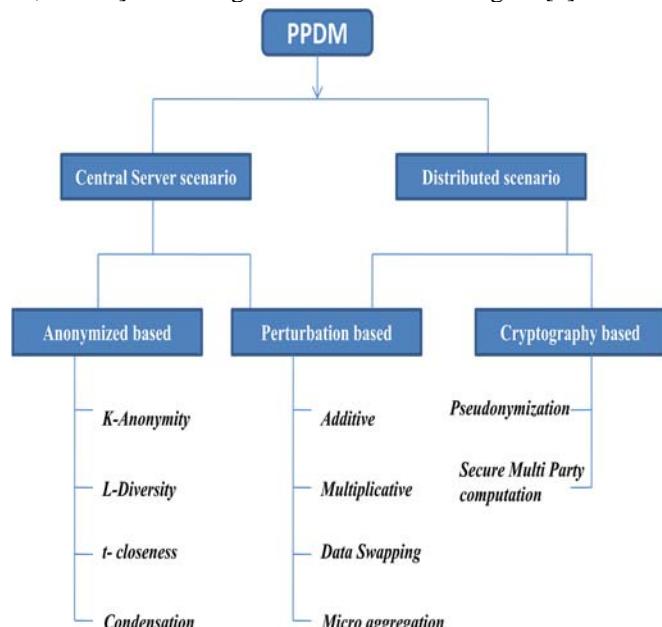


Figure 1 Approaches to Privacy Preserving Data Mining

The existing noise addition methods add the same amount of noise for all the individuals [12, 13]. The personalized privacy and its importance are given in [14]. Such, ‘one privacy level fits all’ approach may not be realistic in practice and it has proved by the survey given in [15]. A two level perturbation and its applicability to privacy preserving data mining are proposed in [16]. The proposed

work also mentioned that reconstruction technique may not work well when applied to many real world data sets. They suggested to skip the reconstruction phase to build data mining models through their experimental results. But with the scattered expansion of the data, new efficient enhancements in data protection are in continuous demand. In this paper we proposed a new working methodology that incorporates constraint mechanism and different type of perturbation with various privacy levels. In our work the perturbation takes place according to the class distribution of the data along with the choice given by the owner, and thus finally it avoids the drawbacks of universal privacy approach and personalized privacy approach. We built the data mining model by skipping the reconstruction phase as mentioned in [16].

The work flow is as follows. Section 2 gives the problem setup and proposed working model is given in section 3, HDD algorithm in section 4. Result analysis is carried out in section 5 followed by a conclusion and future work in section 6.

2. Problem Setup

There are the logical parties in the PPDM communication.

1. Sources, which owns one or more datasets and would like to submit the data to the next level for statistical analysis.
2. Central Data Collector, who takes the responsibility of collecting the data from the sources and make it available for researchers or the data analysts.
3. Data Analysts, who wishes to perform aggregate data analysis over data sets available at central data collector

Trust assumptions: We assume the data owner or the sources, the data collectors are trust worthy, and data analysts need not be trustworthy always. In particular programs supplied by the data analysts may act maliciously and try to leak information. So here we tried to propose a model where the data owners remain anonymous with respect to data analysts and also data collectors by introducing a new anonymization framework.

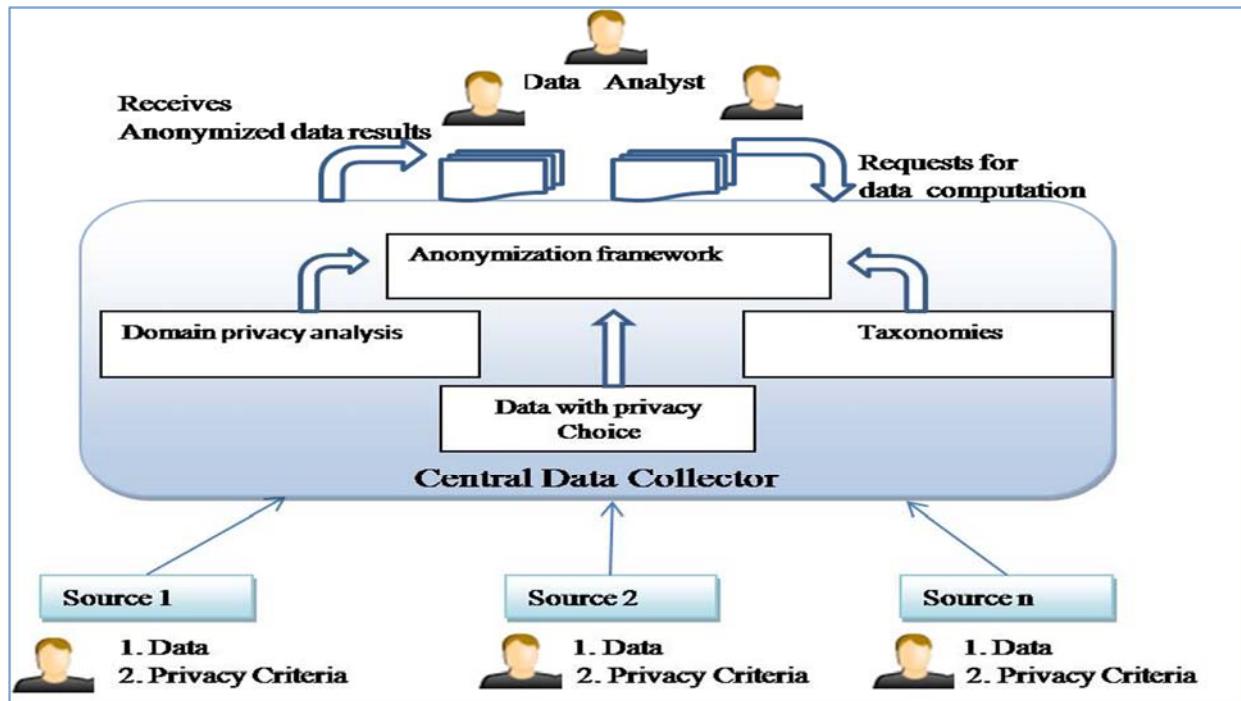


Figure 2 Proposed Model to Privacy Preserving Data Mining

Figure 1 illustrates the high-level system overview of the various entities and their relation in our system model. It also labels the desired framework that determines the data flow among the entities. In the following sections we describe these components more in detail.

3. Proposed Model

A typical data sharing scenario starts with the data submission by the data owner to the data collectors. Then the data collector takes the responsibility of modifying the

data in such a way that it has to meet the requirements of the data user with respect to the expected results and also protects the desired data privacy of its owners. Hence the data collector plays a vital role in PPDM scenario. It has worked well in centralized database environment. Gradually the demand for ‘privacy enhanced technologies by design’ in data sharing is increased with the introduction of distributed environment.

The work proposed in [17] has argued that the data protection should take place at the owner side itself with their individual choice. Because he is solely owner of the data and sharing should happen according to his own choice of disclosure. Research also says that giving complete control to the data owner decreases the data utility.

We proposed our model basing upon the fact that, no individual choice provides the equal balance between data privacy and its utility. The main goal of our model is to carry the equal importance at each and every stage in PPDM communication.

In our previous work [18] we have described the new detailed architecture its working methodology and we also checked with the basic statistical properties that are supposed to be preserved even after its distortion. During the distortion phase we have taken the following three hidden parameters as a primary prerequisite.

- *Privacy choice:* This is the first and foremost parameter collected along with the data from its owner. With its binary value, it says whether the owner wants it to be sensitive or non sensitive.
- *Domain privacy:* This parameter is used by the privacy anonymization layer to analyze the level of sensitivity of each data value in each data object.
- *Correlation:* The third important factor we considered in our model is hidden correlation. In our earlier work [19] we theoretically proved the impact of correlations on the data privacy.

With these three input parameters it generates a privacy mapping vector of each data value and then they will be assigned a privacy class namely High, Medium and Low. This classification is applied in order to avoid the universal privacy preservation process, which completely gets biased either to privacy or utility. Hence in our model we fixed different thresholds for each of these classes. So instead of exerting the same amount of distortion, now it performs distortion according to its class label. After this, the proposed model uses the hybridized perturbation approach where as the existing method uses either noise addition or generalization process. Though the noise addition schemes are simple and effective they are restricted to continuous type of values only. When it comes to discrete data values the perturbation is carried out purely with the process of generalization. It is a process of substituting the actual value with its semantically

meaningful but generalized value from the given taxonomy tree. Here we used a two way approach for data modification. If its attribute type is continuous then it uses noise addition normalization and if it is discrete then taxonomy generalization take place according to its privacy class label. Sample taxonomies are shown in figure [3 and 4].

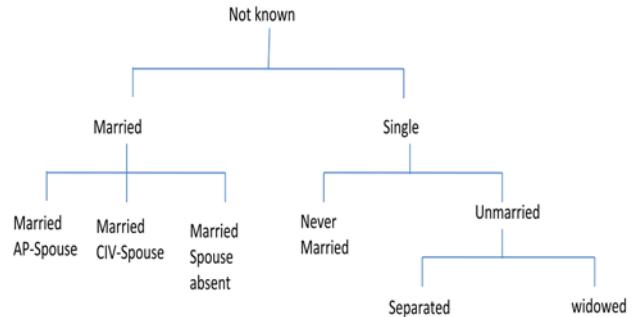


Figure 3 Taxonomy for Marital Status



Figure 4 Taxonomy for Gender

4. HDD Algorithm

Algorithm: HDD Algorithm

Input: Dataset D

Ouput: Distorted data set D'

//generalization of input privacy parameters

Step 1:

for each attribute $A_i \in D$

Generate

Step 1.1: Privacy Choice Vector P_i

Step 1.2: Domain Privacy Vector D_i

Step 1.3: Correlation Vector C_i

//generalization of privacy Mapping Vector

Step 2:

for each data $d_i \in A_i$

if ($D_i C_i P_i == 000 || 001$) then privacy-class(d_i) = Low

elseif ($D_i C_i P_i == 010 || 011$) then privacy-class(d_i) = Medium

else if ($D_i C_i P_i == 100 || 110 || 111$) then

privacy-class(d_i) = High

//data perturbation

Step 3:

for each data $d_i \in A_i$

if ($d_type(d_i) == 'continuous'$) then

$$d'_i = d_i + \frac{d_i - \mu_i}{\sigma_i} + \varepsilon_i$$

else if ($d_type(d_i) == 'discrete'$) then

d'_i = anonymize_t(d_i)

end;

Table 1: List of notations

Notation	Description
D	Original Dataset
D'	Distorted Data set
D_l	Domain Privacy vector; generated with the domain knowledge of the data collector
C_i	Correlation vector; generated with correlation analysis carried out using ‘Pearson Correlation Coefficient’ & ‘Chi-square analysis’
P_i	Privacy choice vector; generated from the choice given by the data owner at the time of data submission.
d_i	Data value
A_i	Attribute in the data set
d_type	Data type of each attribute ; continuous/discrete/nominal/binary
$anonymize_t$	Anonymization or Generalization with taxonomy t.

5. Experimental Consideration

This section gives the detailed result analysis. Our experiment is performed on three different data sets. The data set description is given in table 2.

Table 2: Data Set Description

Dataset	Attributes	Instances	Classes
Adult Data Set	14	32561	2
Liver Data Set	7	345	2
IRIS Data set	4	150	2

Table 3: Comparison of accuracy, error rates of classification techniques

Data Set		Techniques Applied	Accuracy Rate	Error Rate
Adult Data Set	Original	J48	86.4%	13.6%
		NaïveBayes	83.79%	16.21%
	Perturbed	J48	85.68%	14.32%
		NaïveBayes	80.58%	19.42%
Liver Data Set	Original	J48	79%	21%
		NaïveBayes	76.5%	23.5%
	Perturbed	J48	78.5%	21.5%
		NaïveBayes	75%	25%
IRIS Data Set	Original	J48	96.07%	3.93%
		NaïveBayes	94.11%	5.89%
	Perturbed	J48	95.5%	4.5%
		NaïveBayes	93.33%	6.67%

The accuracy of the distorted data is measured with respect to the original data set. We have used WEKA tool to test the accuracy results with various techniques like J48 and Naïve Bayes classification. The results have shown that the model obtained by our proposed distortion method is similarly to the model developed using original data set. We also checked the efficiency with the random split of the data and it has shown very small error deviation.

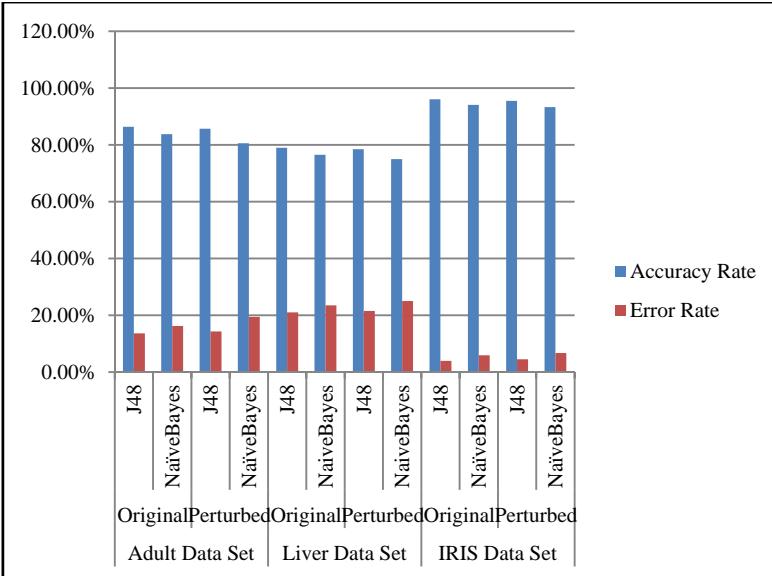


Figure 5 Comparison Plot

Table 4: Comparison of accuracy on original and perturbed data sets (Random split)

Adult Data Set	Data1 (2000)	Data2 (4000)	Data3 (6000)	Data4 (10000)
Test on Original	80.88	84.19	85.33	85.47
Test on Perturbed	79.11	82.22	83.24	84.11
Time	0.08	0.24	0.51	0.64
Liver Data Set	Data1	Data2	Data3	Data4
Test on Original	75.55	76.22	76.86	78.44
Test on Perturbed	74.23	75.11	76.22	77.11
Time	0.05	0.16	0.22	0.45
IRIS Data Set	Data1	Data2	Data3	Data4
Test on Original	97.18	98	98.14	98.22
Test on Perturbed	96	97	97.12	98
Time	0.08	0.06	0.06	0.08

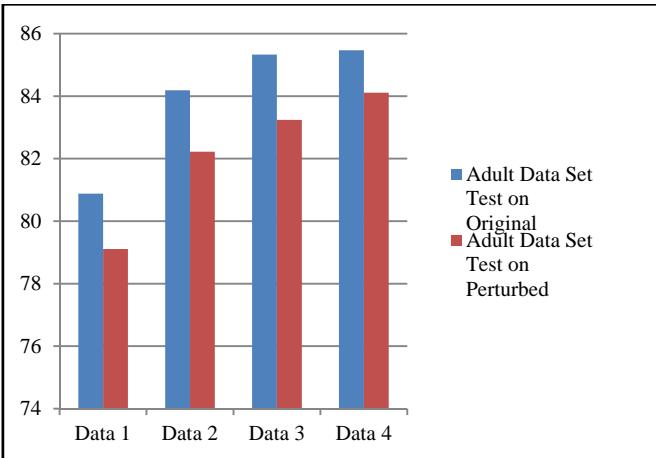


Figure 6 Accuracy with random data split on Adult Data Set

Table 4 shows the results with the J48 algorithm with the random split. When the data is increased the model has shown better classifier results.

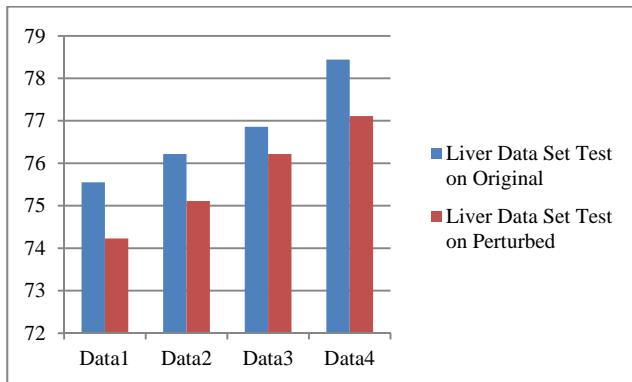


Figure 7 Accuracy with random split on liver dataset

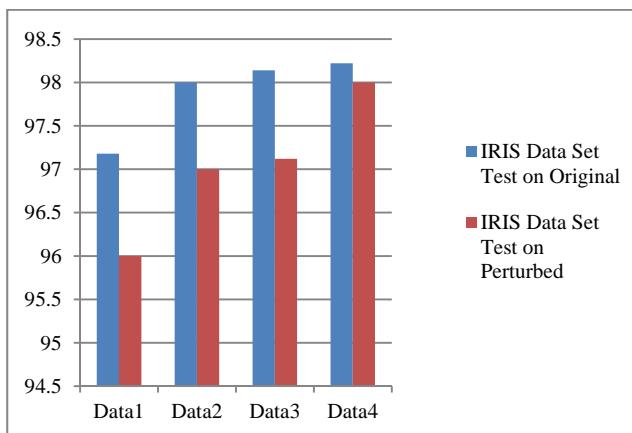


Figure 8 Accuracy with random split on IRIS dataset

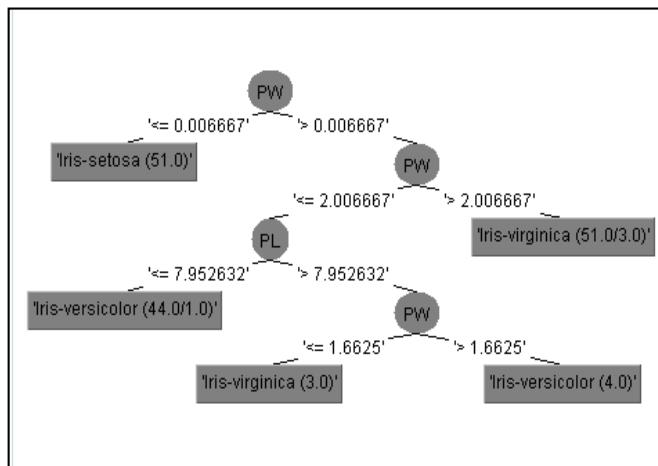


Figure 9 Tree Classifier on IRIS dataset

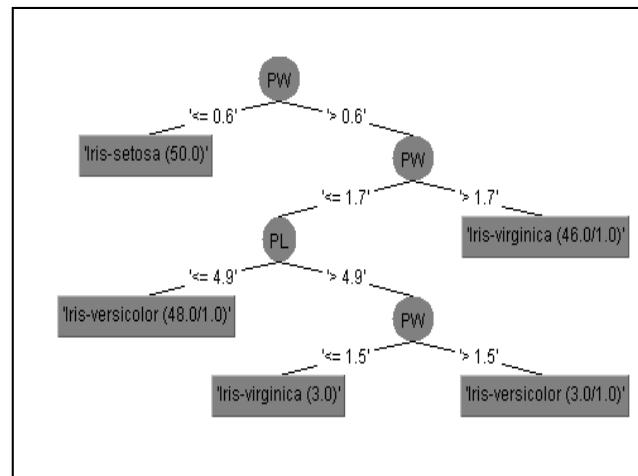


Figure 10 Tree Classifier on Perturbed IRIS dataset

Figure 9 and 10 gives the classification trees generated on original IRIS dataset and perturbed IRIS data set using our heterogeneous distortion method. The perturbed classifier is very slightly deviated from the original classifier.

6. Conclusion

In this paper we proposed heterogeneous data distortion method. It applies hybrid approach of both generalization and noise addition scheme depending upon its attribute type with various levels and also depending upon its class value. This method works better when compared to universal data perturbation and also personalized data perturbation. Results have been shown that proposed heterogeneous data perturbation works well with various classification techniques. As a future work we would like to check the methodology with different techniques in place of generalization and noise normalization.

References

- [1] M Chen, J Han, and P Yu, "Data Mining: An overview from a database Prospective", IEEE Trans on Knowledge and Data Engineering, vol. 8, no 6, pp. 866-883, Dec 1996.
- [2] M. Bertier, D. Frey, R. Guerraoui, A.-M. Kermarrec, and V. Leroy, "The Gossple Anonymous Social Network," in Middleware'10, 2010, pp. 191–211.
- [3] Y. Zeng, N. Zhong, X. Ren, and Y. Wang, "User Interests Driven Web Personalization Based on Multiple Social Networks," in Proc. of the 4th Intl. Workshop on Web Intelligence & Communities. ACM, 2012, pp. 9:1–9:4.
- [4] X. Zhou, Y. Xu, Y. Li, A. Josang, and C. Cox, "The State-of-theArt in Personalized Recommender Systems for Social Networking," Artificial Intelligence Review, vol. 37, no. 2, pp. 119–132, 2012.
- [5] Z. Wen and C.-Y. Lin, "How Accurately Can One's Interests Be Inferred from Friends?" in Proc. of the 19th Intl. Conf. on World Wide Web, ser. WWW'10. ACM, 2010, pp. 1203–1204.
- [6] F. Liu, C. Yu, and W. Meng, "Personalized Web Search for

- Improving Retrieval Effectiveness,” IEEE Transactions on Knowledge and Data Engineering, vol. 16, no. 1, pp. 28 – 40, 2004.
- [7] D Agrawal, R. Srikant, Privacy-preserving data mining, in SIGMOD Conference, 2000, pp 439-450.
- [8] Privacy Preserving Data Mining Yehuda Lindell & Benny Pinkas
- [9] Gagan Aggarwal, Tomas Feder, k-anonymity: Algorithm and Hardness, , Stanford University
- [10] Stanley R. M. Oliveira and Osmar R Zaiane Towards Standardization in Privacy Preserving Data Mining, , University of Alberta, Edmonton, Canada
- [11] Chris Clifton, Murat Kantarcioglu and Jaideep Vaidya, Tools for Privacy Preserving Data Mining, Purdue University.
- [12] D. Agrawal. C.C. Aggrawal, On the design and quantification of privacy preserving data mining algorithms, in: PODS, ACM, 2001.
- [13] H. Kargupta, S.Datta, Q. Wang, K. Sivakumar, On the privacy preserving properties of random data perturbation techniques, in: ICDM, IEEE Computer Society, 2003, pp. 99-106
- [14] E. Toch, Y. Wang, and L. Cranor, “Personalization and Privacy: a Survey of Privacy Risks and Remedies in Personalization-Based Systems,” User Modeling and User-Adapted Interaction, vol. 22, no. 1-2, pp. 203–220, 2012.
- [15] L.F. Cranor, J. Reagle, M.S. ckerman, Beyond concern: Understanding net users attitudes about online privacy, CoRR cs.CY/9904010
- [16] Li Lu, Murat Kantarcioglu, Bhavani Thuraisingham ‘The applicability of the perturbation based privacy preserving data mining for real-world data’, ELSEVIER, 2007.
- [17] Lijie Zhang and Weining Zhang Generalization-Based Privacy-Preserving Data Collection, Springer, 2008, pp 115-124.
- [18]. J.Hyma, PVGD Prasad reddy, A.Damodaram ‘A New Heterogeneous Constraint-based Data Distortion in Privacy Preserving Data Mining’ ,IJAC, 2016, Vol 49.
- [19]. J.Hyma, PVGD Prasad Reddy, A.Damodaram “A Study of Correlation Impact on Privacy Preserving Data Mining” ,IJCA, Vol 129, 2015.

Evaluating the Effects of Network Size and Nodes Mobility Speed on the Performance of TCP over Mobile Ad-Hoc Networks

Aju O. G, Oriola O.

Abstract— The purpose for the design of Transmission Control Protocol (TCP) was to provide reliable end-to-end delivery of data over unsecured networks. Although, it is designed to be deployed in the traditional wired networks but recently, there has been an increase in its deployment over the wireless networks such as Mobile Ad-Hoc Networks (MANETs). This paper investigates the performance of various TCP variants in specified network scenarios in Mobile Ad hoc Networks (MANETs) using Reno, New Reno and SACK as case study under the Dynamics Source Routing (DSR) Protocol by observing the effects of some network designs on the performance of TCP variants in MANETs using throughput, delay and retransmission attempts as performance metrics.

Application traffics were submitted to MANETs while the network size (number of nodes) and the nodes mobility speed were varied to create network models and the resulting throughput, end-to-end delay and retransmission attempts were observed to determine how the network size and the nodes mobility speed affects the performance of the TCP variants.

Index Terms— Mobile Ad hoc Network, Transmission Control Protocol, Selective Acknowledgements, File Transfer Protocol, Hypertext Transfer Protocol, Voice over Internet Protocol.

I. INTRODUCTION

Mobile Ad Hoc Network otherwise known as MANET recently seem to have gained tremendous popularity and considered the most common area of scientific research for both academics and industries that are into mobile computing and communications. The recent increase in the research popularity in this field has been attributed to the current innovations and production of smart, smaller, more convenient, powerful, and affordable mobile gadgets (e.g. smart phones, laptops, handheld digital devices, personal digital assistants, tablets and wearable computers) and applications which tend to encourage and facilitate the consumers' rate of mobile computing usage.

Additionally, the motive of allowing communication facilities to reach every nook and cranny of the world, and provide good and reliable communication

opportunities to the remote areas where fixed communication infrastructure is not viable, particularly during an emergency needs such as natural disaster relief operations, military operations or conferences and seminars has also increased the researches into this area of computing and communication to improve its operations reliability and performance efficiency.

MANET is considered as a form of autonomous complex distributed systems that consist of wireless mobile devices (also known as nodes) which are able to spontaneously interconnect without any pre-existing infrastructure (Siva and Manoj, 2012). It is considered as autonomous because the mobile devices are able to communicate with one another without the use of pre-existing communication infrastructure, and since the network's topology can dynamically change in an unpredictable manner due to the mobility capacity of the nodes which also acts as hosts and routers in the network, the network is then regarded as ad hoc or temporary network

In MANET, nodes acts as both hosts and routers, however, for the nodes to communicate among themselves, data must be routed or transferred from one node to another node using certain transmission protocols. TCP as a form of data transmission protocol was designed to provide a reliable end – to - end delivery of data over unreliable network, though it was initially designed to be used on wired networks, it has also been increasingly deployed on wireless and MANET networks though with less reliability and performance. This is made possible because TCP is designed to be independent protocol which must be independent of the underlying technology and infrastructure on which it runs.

II. MANETS OVERVIEW

A. TCP Mechanisms in MANETs

The Transmission Control Protocol (TCP) is designed to provide a reliable end-to-end congestion control, error control, flow control and numbering system during a transmission of segments using any of the slow start, congestion avoidance, congestion detection, checksum, sequence numbering or acknowledgement mechanism. The protocol is widely used both in wired or wireless communication layers due to its reliability in end-to-end transmission of segments.

The protocol (TCP) establishes, maintains and terminates connections between communicating nodes as part of its

O. G. Aju is with the Department of Computer Science, Faculty of Science, Adekunle Ajasin University, Akungba-Akoko, Ondo State, Nigeria. (e-mail: omojokun.aju@aaua.edu.ng).

O. Oriola is with the Department of Computer Science, Faculty of Science, Adekunle Ajasin University, Akungba-Akoko, Ondo State, Nigeria. (e-mail: oluwafermi.oriola@aaua.edu.ng).

functions, while it also behaves fairly towards other network flows including other TCP agents.

TCP sends data in segments with a specified maximum segment size as negotiated via a three-way handshake between the communicating nodes during an initial connection establishment phase. Each segment of the data has a sequence number assigned to it, when a receiving node receives a segment, it notes the sequence number range of the segment and responds by sending back a cumulative acknowledgement (ACK) to the sending node to confirm that all bytes up to the given sequence number have successfully arrived. The TCP sender also maintains a retransmission timeout (RTO) timer, which on expiration indicates that a segment has been lost and is to be retransmitted. The combination of functions offered by the cumulative ACKs, the retransmission timeout (RTO) timer, segment numbers and the checksum on the segment header offers the transmission's reliability.

Recently, there have been four popular TCP mechanisms (Variants) that have been adopted as reliable transport protocols over MANETs as they have been tested to be easily implementable over small or large scale networks. These four mechanisms are: TCP Reno, TCP New Reno, TCP Selective Acknowledgement (SACK) and TCP Vega. The first three of the four mechanisms will form this research point by reviewing them to determine which mechanism is more effective for certain network scenario through OPNET simulations using different networks scenarios.

1) TCP Reno

TCP Reno is one of the mechanisms of implementing TCP protocols in order to achieve a more effective TCP performance in networks by efficiently controlling the networks' congestions through the adjustment of the networks' window size; the mechanism uses an additive increase and multiplicative decrease congestion control algorithm to constantly regulate the available bandwidth in a network

The mechanism (TCP Reno) increases its window size at every round trip by one, this method is termed additive increase , but reduces its window size to one half of the current window size whenever it experiences any segment delay or loss due to congestion and this method is called multiplicative decrease. These additive increase and multiplicative decrease algorithms method of regulating the bandwidth of a network has shown to result into a fair allocation of bandwidth in a network and consequently reduces the loss of segment caused by network congestion.

However, it has been shown that TCP Reno only perform optimally when only small amount of segments were lost, it performance dramatically diminished when a network losses high and multiple segments in one window (Danielle and Martins, 2006). The major reason for the above deficiency in the operation of this mechanism is that, Reno can only detect a single segment (Packet) loss at one time, therefore if multiples segments were dropped or lost in a network, the first segment loss information will be received when a duplicate acknowledgement is received by the sender, the second information as regards the second or subsequent segments loss will be received after the acknowledgement for

the first re-transmitted segment had been received at the sending node.

2) TCP New Reno

The New Reno mechanism works in a similar way as the TCP Reno discussed above, the mechanism improves upon the congestion recovery mechanism of TCP Reno without requiring any changes to the TCP receivers or the format of the TCP segment (Luc *et al.*, 2008). The mechanism is much more efficient compare with the Reno mechanism in that TCP New Reno can detect multiple segments loss.

Though, TCP New Reno also uses "Fast Re-Transmit" algorithm like TCP Reno when duplicate acknowledgements are received but the TCP New Reno will not exit the fast-recovery state until acknowledgements are received for all the segments (both new and outstanding) in the window when the mechanism entered the fast-recovery state, therefore avoiding the situation in which congestion window have to be reduced severally as in the case of Reno. This situation is made possible because there are provisions during the fast-recovery state that allows the sender to responds to the acknowledgements (ACKs) that covers both the new segment and the outstanding segments at the time the loss was discovered.

However, as efficient as the New Reno seems to be, it has been discovered that it take a whole round trip time (RTT) to detect a segment loss. The mechanism can only vividly ascertain which exact segment was lost after receiving the acknowledgement for the first retransmitted segment.

3) TCP SACK

The Selective Acknowledgements TCP variant otherwise known as SACK is considered as an extension of Reno variant in that its works revolve the correction of most of the problems facing by the Reno and New Reno variants particularly its ability to detect multiple packets loss and the retransmission of more than one packet lost per RTT.

While SACK is regarded as a modified version of the Reno variant, it still retain part of the features found in the Reno variant such as the slow-start and fast-retransmission features that are present in the Reno and New Reno.

SACK works on the principle that, segment should not be acknowledged cumulatively as other variants do but should be selectively acknowledged which bring about its name "Selective Acknowledgements". Therefore, in performing this task, in the process of traffics (segments) transmission from one node to the other node, it therefore provide acknowledgement block that describe which segments are being acknowledged, enabling the sender to know which segments has been acknowledged and which segments are still pending.

Each time a sender enters into a fast recovery phase, the SACK initialize a variable pipe which is an estimate of the number of segments that are still pending in the network while setting the congestion window (CWND) to the half of its current size, each time an acknowledgement is received, the variable pipe is reduce by 1 and every time it retransmit a segment, the variable pipe will be increased by 1.

B. Routing in MANETs

The routing of data in mobile ad hoc networks (MANETs) is quite different from the traditional routing used in wired networks due to the dynamic and unpredictable topologies of MANETs that makes the routing so complex and challenging, the routing algorithm or protocols for MANETs must therefore be operated with little overhead, light weighted but strong enough to meet the mobile nodes constraints and be able to transmit packets efficiently from one node to another. The common routing protocols in MANETs are AODV, DSR and OSLR routing protocols.

1) Ad hoc On-Demand Distance Vector (AODV) routing

Ad hoc On-Demand Distance Vector (AODV) routing protocol is a very common reactive routing protocol that operates on a reactive purpose which otherwise refer to as on-demand routing method, this is because the method procedure of routing is that participant nodes in the data transmission are to maintain routes to only the destinations that are presently in active use (Perkins, 2003). The transmission routes are only established as needed and therefore the proactive way of route discovery does not exist. The advantage of this, is that costs are being saved from the overhead cost that are associated with the frequent routes changes and rediscovery since the topology changes frequently leading to changes in the routes associated with the nodes in the network

Although, this routing protocol only maintains a route entry per destination, it fully fulfils the main two functions of routing protocol which are the route discovery and route maintenance.

2) Dynamics Source Routing (DSR) Protocol

Dynamics Source Routing (DSR) Protocol is also a reactive algorithm routing protocol which shares the same working method with AODV in that it does not maintain routes to all possible destinations but establishes routes when such is needed, thereby saving the overhead cost of maintaining various routes that are not in use.

Dynamics Source Routing (DSR) Protocol is considered a distance vector routing protocol because it makes use of sequence numbers so as to avoid the routing loops that are associated with other reactive routing protocols.

The protocol is very efficient and avoids unnecessary waste of resources, it ensure that every packet is imprinted on its header by the sender the complete route that such a packet has to follow to get to its destination thereby avoiding the need for every intermediate nodes in the network to contain an up-to-date information of packet routes. The protocol will rather makes use of route caching mechanism in which case its table entries may contain multiple routes for the same destination (Tang *et al.*, 2008).

Since routes failure is the major way of data loss in MANETs, DSR protocol is a preferred routing protocol in the frequent dynamics topology network in that it constantly recovers from routing errors by immediately discovering alternate routes from the point of failure

In the process of this experimental simulation, this (DSR) protocol will be used as the default routing protocol.

3) Optimized Link State Routing (OLSR) Protocol

The optimized link state routing protocol is a proactive routing protocol which proactively discovers paths to potential packets destinations by pre-emptively building a view of the network. The protocol is also called table driven protocol because it consistently involves nodes exchanging routing information (Clausen and Jaquet, 2003).

It is well known that not all nodes in an OLSR network forwards traffic, rather the protocol is built upon a concept called multipoint relays (MPRs) which allows each node in the network to select a set of its neighbouring nodes as MPRs, which are then responsible for the forwarding of controlled traffics for the transmission in the network

Since only designated nodes floods the network with traffics, the protocol is able to reduce the cost of network overhead. The MPR nodes provides the possible shortest routes by making available the periodic link status changes to nodes that have selected them in the network

OLSR is mostly applicable in networks where traffics are inconsistent and unpredictable, and communication between set of nodes is not permanent, but rather changes frequently.

III. NETWORK SIMULATION DESIGN

This section described the network design models, the parameters and the necessary evaluation metrics that are needed to analyse and evaluate the performance of the proposed scenarios. Therefore, the software simulation tools platform, the performance evaluation metrics and the network simulation design are all presented.

A. Simulation Tool Platform

The experimental review analysis is conducted using discrete event simulation software called Optimized Network Evaluation Tool (OPNET) modeller version 14.5, a network and application management design and evaluation software suite from OPNET Technologies Inc. It provides dynamic simulation of communication devices, protocols, technologies, and architectural performance in a virtual network environment.

Although, other various software platform tools (Simulators) such as NS-2, GloMoSim, Qualnet, OMNET++, J-Sim among others are being employed in the networks model and application simulation and evaluation, while some of these tools are open source tools others are commercial tools that need to be licensed through purchase, however, the choice of which simulator to be used will be purely driven by the user's (researcher) requirements and the exact research that needs to be covered in the experiment.

B. Performance Metric

For the purpose of this experiment, the following three performances metric will be considered: Throughput, Transmission Delay and Retransmission Attempts. Throughput and Transmission delay are chosen as part of the performance metrics because they measures a transmission policy's effectiveness and are important when dealing with Constant Bit Rate (CBR) applications such as real-time audio as in the case of voice application which is one of the application supported by the network to be simulated.

The network is designed to support and service FTP, HTTP and Voice applications for the traffic analysis where the applications are all considered with heavy traffic loads.

1) Throughput

This is considered as the total number of bits that are sent through the channel per second. It is the ratio of the total amount of segments that gets to a receiving node from a sending node to the time it takes for the receiving node to get the last segment. Therefore, it is defined as the number of packets successfully transmitted by the sender for which an ACK has been received.

Some of the factors that affect throughput in MANETs include the dynamic topology changes, route failure, limited bandwidth and the energy constraints.

2) Transmission Delay

It is the average time that segment (packets) take to travel the network, that is, the time required to get the complete segment from the source to the destination which is expressed in seconds.

Since MANETs are characterized by dynamic node mobility, route failures, energy constraints and packets retranmissions. These factors causes dramatic delay in the network, therefore the expected delay to be used as a performance metric can be said to be how well the TCP variants used in the network were able to adapt to these stated factors.

3) Retransmission Attempts

It is considered as one of the most important performance metric to determine the effectiveness of TCP variants being considered in this experiment. It is majorly used to measure the performance of congestion control mechanism in the network particularly due to route failure. It is defined as the total number of retransmission attempts of segment (packets) that have been lost or damaged due to link failure in the network. It can also said to be the number of packets that had failed in the transmission process which needs to be retransmitted. So, it is assumed that the lower the retransmission attempts the more reliable is the TCP variant under consideration.

C. Network Workload Factors

The system and the workloads parameters are those parameters that affect the performance of the modeled network system during the review process and these parameters include: the number of nodes in a given area (node density), the packets size and the nodes mobility.

1) Node Density

Node density is the number of nodes in the simulation area. It is assumed that as the number of nodes in a fixed area is vary; the performance of TCP will definitely vary.

2) Nodes Mobility

The real life scenario in MANETs is that nodes do not remain static for extended period of time; rather they are frequently motion in a dynamic way. It is therefore considered in this experiment that the networks' nodes are mobile and their mobility effect on the TCP performance will be measured by varying the mobility speed of the nodes in the networks scenarios.

Overall, the two factors or parameters that will be considered in this experimental review will be: the nodes density and the node mobility speed as they affect the performance of TCP variants in a Mobile Ad Hoc Networks (MANETs).

D. Network Area and Modelling

The network models simulations took place over a campus square area with dimensions set to 2000m x 1000m. The mobility model used is the random waypoint model with parameters set to reflect mobility ranging from walking of approximately 2m/s to vehicular speeds of approximately 20m/s.

Since the motive of this experiment is to evaluate the performance of different TCP variants when the full spectrum of their congestion avoidance mechanisms is being over stressed within a period of time, therefore, the reason for the choice of application traffics sources of FTP, HTTP and Voice with very heavy loads. It is therefore an open research question whether TCP variants in MANETs will perform differently under other types of traffic loads, such as Email, Printing, and Database.

The network components that were used during the design of the network models that allows for the attributes definitions and tuning are as follows: A wireless mobile Server; An Application Configuration Node; A Profile Configuration Node; A Mobility Configuration Node and Mobile Workstation Nodes.

Application configuration node is a very important component object in the network; it defines the transmitted data, the file size and the traffic load. Although, it supports common applications, such as Email, HTTP, FTP, Voice, Print among others. FTP, HTTP and Voice applications were purposely chosen because the heavy traffics are required to critically test the performance of the protocol in view and unlike other applications such as printing; FTP, HTTP and Voice would generate heavy traffics that could meet the purpose of the experiment.

The profile configuration node was used to create the user profiles. It describes the activity patterns of a user or group of users in terms of the applications used over a period of time. For these network models, FTP, HTTP and Voice profile were created in a profile configuration component so as to support the FTP, HTTP and Voice traffics that would be generated by the application configuration on component.

The mobility configuration node was used to configure the mobility model of the nodes. In doing so some appropriate parameters such as speed start time, stop time, pause time, mobility area among others are to be spelt out. In order to properly control the movement of the nodes in the network, the nodes has to be restricted or confined to specific mobility area, and in this case, an area of 2000m x 1000m has been chosen as the mobility area in which the nodes can only move, which means that any traffic generated from outside this specific range, would not be considered.

For the purpose of the study, the default random waypoint mobility was used for all simulation purposes. It is a widely used mobility model which is also regarded as the default mobility model in MANETs. The speeds of the nodes were

varied between 2m/s and 20m/s to reflect a real life speed of walking to that of vehicular speed. The reason for this variation of speed on the nodes was to observe the impact of mobility on the TCP performance.

The wireless mobile router is a wireless LAN based server which is used to provide the mobile nodes with the FTP, HTTP and Voice traffics from one point to another and the connection speed was set at 11 Mbps. Finally, all the mobile nodes were configured to generate FTP, HTTP and Voice traffics randomly.

The tables 1-5 demonstrate the individual node parameters that were used in the course of designing the network models and simulation.

Table 1. Network General Parameters

General Parameters	Value
Simulator	OPNET 17.1
Area	2000 x 1000 square meters
Network size	30, 50 and 100 nodes
Data rate	11Mbps
Mobility model	Random way point
Mobility speed	2, 10 and 20 m/s
Traffic type	FTP, HTTP and Voice
File size	Heavy loads
Routing protocol	Dynamic source routing (DSR)
Address mode	IPv6
Simulation time	3,600 seconds

Table 2. Application Configuration Parameters

Application Configuration	Value
Number of Applications	3 (FTP, HTTP and Voice)
Start time offset (seconds)	Constant (5)
Duration (seconds)	End of profile
Application repeatability	Once at start time
Inter-repetition time (seconds)	Constant (300)
Number of repetitions	Constant (0)
Repetition pattern	Serial

Table 3. Profile Configuration Parameters

Profile Configuration	Value
Number of profile	3 (FTP, HTTP and Voice)
Operation mode	Simultaneous
Start time (seconds)	Uniform (100, 110)
Duration (seconds)	End of simulation
Profile repeatability	Once at start time
Inter-repetition time (seconds)	Constant (300)
Number of repetition	Constant (0)
Repetition pattern	Serial

Table 4. TCP Parameters

TCP Parameters	Value
TCP version	Reno, New Reno and SACK
Slow start initial count	1
Fast Retransmit	Enabled
Receive buffer size (bytes)	8,760
Receive Buffer Adjustment	None
Maximum ACK Delay (seconds)	0.02
Maximum ACK segment	2
Duplicate ACK threshold	3
Initial RTO (seconds)	1.0
Minimum RTO (seconds)	0.5
Maximum RTO (seconds)	64
RTT gain	0.125
Deviation gain	0.25
RTT Deviation Coefficient	4.0

Table 5: Wireless LAN Parameters

Wireless LAN Parameters	Value
Wireless LAN MAC Address	Auto assigned
BSS identifier	Auto assigned
Physical characteristics	Direct sequence
Data rate (bps)	11Mbps
Channel setting	Auto assigned
Transmit power (W)	0.005
Rts threshold (bytes)	None
Fragmentation threshold (bytes)	1024
CTS-to-self option	Enabled
Short retry limit	7
Long retry limit	4
AP beacon interval (seconds)	0.02
Max receive lifetime (seconds)	0.5
Buffer size (bits)	256000
Large packet processing	Fragment

The network (Simulation) area of the mobile nodes in the conducted experiment was set to 2000m x 1000m. The nodes size was set to represent small, medium and large sized networks, therefore nodes size of 30, 50, and 100 were used.

The nodes speeds used in the simulation were set to reflect mobility ranging from walking of approximately 2m/s to vehicular speed of approximately 20m/s. Therefore the nodes speeds were set to 2m/s, 10m/s and 20m/s while 2m/s represents a slow walking speed in an office or campus, the 10m/s represents the fast running of a person or slow moving vehicle while 20m/s speed represents normal vehicular movement.

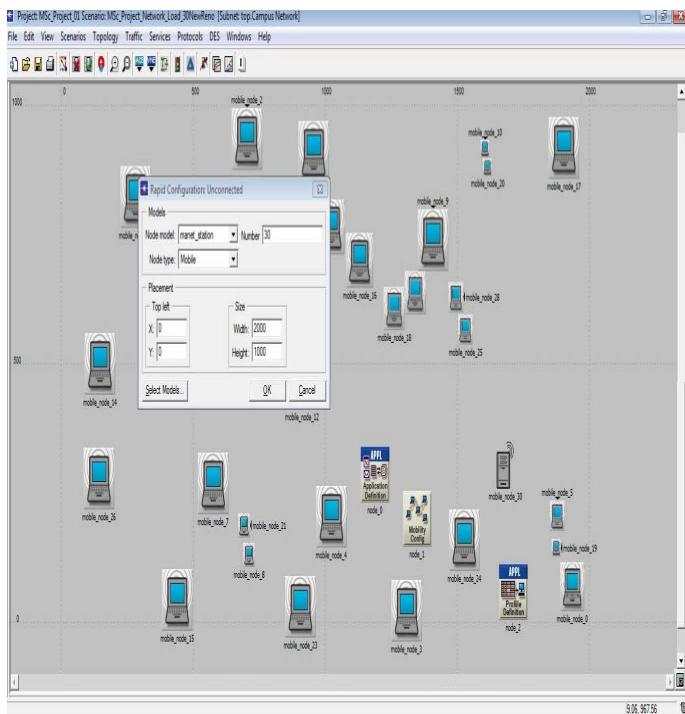


Figure 1. A network with 30 Mobile Nodes

However, since the traffics pattern of the nodes within the network are not to be studied in the experiment, the Random Waypoint (Auto Create) mobility model was used for the configuration of the node speeds instead of the Random Waypoint (Record Trajectory) mobility model. The nodes mobility patterns were therefore defined by the OPNET Modeller automatically.

E. Description of Network Scenarios

The networks simulation scenarios are as follows using network size and nodes mobility speed variation.

1) Network Size Variation

This scenario was made up of nine experiments, which consist of three experiments individually implemented on TCP- Reno, New Reno and SACK variants with the network size of 30, 50 and 100 nodes to determine the TCP performance of small, medium and large network sizes. The nodes speed was set to 10m/s with the generated FTP traffic (packet length) of 500,000 bytes while the HTTP and Voice traffics were set to heavy loads.

Varying the network size was expected to have some effects on the level or degree of network congestion occurrence, a lower network size is likely to reduce the network congestion occurrence while a higher network size is likely to increase the occurrence. Also, lowering the network size will lead to fewer multi-hops connections between nodes, that is, the number of nodes that a segment may likely travel through before getting to its final destination while a network with higher size may increase the multi-hops connections between sender and receiver of a segment.

The performance of the individual experiment under these network conditions will be measured and analysed through the network's throughput, transmission delay and retransmission

counts to determine which of the TCP variant achieves better performance.

2) Nodes Mobility Speed Variation

This scenario was made up of twenty-seven experiments consisting of three experiments implemented on TCP- Reno, New Reno and SACK variants with the network size of 30, 50 and 100 nodes. The nodes speeds were then varied at 2m/s, 10m/s and 20m/s to determine the TCP behaviour with the fixed generated FTP traffics (packets size) of 500,000 bytes and HTTP and Voice traffics set to heavy loads on all the experiment cases.

Varying the nodes mobility speeds was expected to have some impacts on the TCP performance in the networks; therefore, the performance of the individual experiment under these various network conditions will be measured and analysed using the network's throughput, delay and retransmission counts to determine which of the TCP variant can achieve better performance.

IV. SIMULATION INVESTIGATION AND ANALYSIS

This section provides the detailed experimental results of the simulations and the analysis of the TCP behaviours in the specified scenarios in which the networks' node sizes and the nodes mobility speeds were considered as determining factors. The simulation duration was set to 3,600 seconds (60 minutes) over which the performance statistics of throughput, transmission delay and retransmission counts were collected.

A. Varying the Network Size

The table 6 represent the results of simulation for the TCP variants performance on varying the network size (Nodes) between 30, 50, 100 nodes representing small, medium and large enterprise networks using throughput (kbps), transmission delay (sec) and retransmission counts (segment).

Table 6. Network Size Variation Effects on the TCP Variants

Simulation 1: Network Size Variation Effects on the TCP Variants with fixed nodes mobility speed of 10m/s				
Nodes	Metrics	TCP Variants		
		Reno	New Reno	SACK
30	Throughput	3.7	3.8	3.5
	Transmission Delay	0.54	0.52	0.54
	Retransmission counts	5700	5700	5700
50	Throughput	3.5	3.6	3.5
	Transmission Delay	0.75	0.70	0.72
	Retransmission counts	7250	7050	7200
100	Throughput	2.5	2.7	2.5
	Transmission Delay	1.9	1.9	1.9
	Retransmission counts	20000	19200	17600

From the table 6, the derived data shows that the throughput generated in the network decreases as the network size increases from 30 nodes through to 100 nodes across the three TCP variants, the decrease was not much from 30 nodes to 50 nodes (around 0.1 - 0.2kbps) but significantly increased when the network was increased to 100 nodes (difference of 1.0 - 1.1kbps). This could be attributed to the fact that there is high possibility of increase in congestion occurrences as the network size (the number of nodes in the network) increases, hence some segments may be lost or drop during transmission which will definitely results to a decrease in an average throughput of the network. However, the New Reno TCP variant seem to offer better performance as it produce slightly higher throughputs than the Reno and SACK variants.

The table also shows that the transmission delay experienced in the network increases as the network size increases from 30 nodes through to 100 nodes. This could be due to the fact that there was high possibility of increase in congestion occurrences as the network size (the number of nodes in the network) increases since the nodes generate random traffics and the traffics moves within the confined space. However, the New Reno TCP variant offers better performance as it produce slightly lesser delay than the Reno and SACK variants, when the increase in the network size was minimal, however New Reno's better performance seems to fade away as the network nodes moves higher and no tangible difference could be observed between the variants' performance. As the network size increases, the delay experience increases across the Reno, New Reno and SACK variants, and interestingly too, the difference in the delay looks wider as the number of nodes increases further.

The table 6 further shows that the retransmission attempts experienced in the network increases as the network size increases from 30 nodes through to 100 nodes. This means that more segments are being discarded or dropped as the network size increases due to congestion or route failure, and attempts were made to retransmit these segments leading to higher number of retransmission counts.

Also, the difference in retransmission attempts were more recognizable as the number of nodes increases, that shows, the retransmission attempts were directly related or proportional to the increase in the number of the nodes.

While it was observed that there was no meaningful difference recorded as regards the retransmission performance in both Reno and New Reno when the network nodes size was 30 and 50 nodes. There was significant difference as the network size increased to 100 nodes, the SACK variant seem to perform better than the other variants as less segments were retransmitted when the network was very large.

B. Varying the Nodes Mobility

The tables 7 – 9 represent the simulation results for the TCP variants performance by varying the network's nodes mobility speed to 2m/s, 10m/s and 20m/s under various network sizes of 30 (small), 50 (medium) and 100 (large) nodes using throughput (kbps), transmission delay (sec) and retransmission counts (segment) as performance metrics.

Table 7. Nodes Mobility Speed Variation under 30 Nodes

Scenario 2(a): Nodes Mobility Speed Variation Effects on the TCP Variant with 30 Nodes					
Nodes Speed	Metrics	TCP Variants			
		Reno	New Reno	SACK	
2m/s	Throughput	2.8	3.4	2.9	
	Delay	0.72	0.68	0.72	
	Retransmission counts	6250	6100	6300	
10m/s	Throughput	3.7	3.8	3.5	
	Delay	0.54	0.52	0.54	
	Retransmission counts	5700	5700	5700	
20m/s	Throughput	4.1	4.2	4.0	
	Delay	0.48	0.46	0.48	
	Retransmission counts	5300	5280	5300	

Table 8. Nodes Mobility Speed Variation under 50 Nodes

Scenario 2(b): Nodes Mobility Speed Variation Effects on the TCP Variant with 50 Nodes					
Nodes Speed	Metrics	TCP Variants			
		Reno	New Reno	SACK	
2m/s	Throughput	2.5	3.2	2.7	
	Delay	0.84	0.82	0.84	
	Retransmission counts	8700	8550	8600	
10m/s	Throughput	3.5	3.6	3.5	
	Delay	0.75	0.70	0.72	
	Retransmission counts	7250	7050	7200	
20m/s	Throughput	3.8	4.0	3.8	
	Delay	0.52	0.50	0.52	
	Retransmission counts	5500	5400	5500	

Table 9. Nodes Mobility Speed Variation under 100 Nodes

Scenario 2(c): Nodes Mobility Speed Variation Effects on the TCP Variant with 100 Nodes					
Nodes Speed	Metrics	TCP Variants			
		Reno	New Reno	SACK	
2m/s	Throughput	1.8	2.2	2.1	
	Delay	2.2	2.1	2.2	
	Retransmission counts	17200	17500	15600	
10m/s	Throughput	2.5	2.7	2.5	
	Delay	1.9	1.9	1.9	
	Retransmission counts	18000	19200	17250	
20m/s	Throughput	4.2	4.8	4.5	
	Delay	1.5	1.4	1.45	
	Retransmission counts	22000	21400	20600	

1) Throughput

The data shows that the throughput generated in the networks increases as the nodes mobility increases from 2m/s through to 20m/s in a network. This implies that an increase in the nodes mobility causes segments to be delivered more faster which is assumed to lead to reduction in congestion within the networks, this will definitely leads to decrease in the number of segments being discarded and a corresponding increase in the networks throughput.

However, it is observed that the throughput decreases as the number of nodes increases from 30 nodes to 50 nodes and from 50 nodes to 100 nodes from one network to another networks across the TCP variants at a fixed nodes speed of 10m/s, the networks throughput decreases even when nodes increases from 30 to 50, and from 50 to 100. However, different results were obtained when the nodes mobility speeds were varied. In all, in the entire three networks examined New Reno TCP variant offers better performance as it produces slightly higher throughputs than the Reno and SACK variants, although, as the network size increases, the differences in the generated throughputs decreases between the Reno, New Reno and SACK variants

2) Transmission Delay

The data from the tables 7-9 shows that the transmission delay experienced in the networks decreases as the network nodes mobility increases from 2m/s to 20m/s across all the networks. This implies that an increase in the nodes mobility speed causes segments to be delivered more faster which will lead to reduction in waiting time for the incoming segments within the networks resulting to less congestion,

Although, it is evident from the tables that the transmission delay increases as the number of nodes increases from 30 nodes to 50 nodes and from 50 nodes to 100 nodes, notwithstanding the increase in the nodes speed.

In all, in the entire three networks examined New Reno TCP variant offers better performance as it produces slightly lower transmission delay compare to the Reno and SACK variants.

3) Retransmission Counts

The data from the tables 7-9 shows that the retransmission counts (retransmission attempts) experienced in the networks decreases as the network nodes mobility increases from 2m/s to 20m/s for networks with 30 and 50 nodes, however the retransmission counts increases as the nodes mobility increases from 2m/s to 20m/s for the network with 100 nodes.. This implies that an increase in the nodes mobility causes segments to be delivered more faster leading to reduction in waiting time for the incoming segments for the networks with 30 and 50 nodes resulting to less congestion, surprisingly, the same principle did not apply to the network with 100 nodes as the retransmission counts increase as the nodes speed increases, implying that the network started experiencing higher congestion rate as the network becomes large irrespectively of the nodes mobility speed.

In all, in the entire networks examined New Reno TCP variant offers better performance for the small and medium network as it produces lower retransmission counts for the networks with 30 and 50 nodes compare to the Reno and SACK variants. However, the SACK variant

performed better as the network size increased to 100 nodes, this implies that SACK variant performs better when the network is large in the area of congestion control.

V. EXPERIMENTAL OBSERVATION AND PERFORMANCE EVALUATION

From the simulation results, it is observed that factors such as varying the network size (number of nodes) and nodes mobility speed has various effects on different challenges facing mobile ad hoc networks (MANETs) such as networks congestion, routes failure and that the effects of the factors has some influence on the performance of the TCP variants.

A. Network Size Variation Effects on TCP Variants

The effects of network size (number of nodes) variation were boldly reflected from the simulation results as observed from the throughput, delay and retransmission counts. All the TCP variants follow the same pattern in that the throughput of the network as a whole decreases significantly as the network size increases, and the larger the number of nodes in the network, the higher the rate of decrease in the network's throughput.

It then follows that the increase in the number of nodes in the network definitely increase the possibility of congestion in the network leading to higher delay as packets are loss. As the number of nodes in the network increases, more traffic were generated, and since these traffics are to be routed within the specified area (2000m x 1000m), then more congestion and higher delay is expected to occur, and therefore lower throughput.

The performance of the variants on the retransmission attempts when the network size increases is a further manifestation of how each variant could cope with congestion and packet loss. From the simulation results, as the network size increases, the retransmission attempts increase across the three variants, this is because the increase in the nodes in the network increase the number of traffics generated leading to network congestion and delays, and ultimately resulting to segments (packets) loss. As these segments did not get to the final destination and no acknowledgement is received by the source, such segments are meant to be retransmitted. Therefore, the higher the congestion, the higher the packet loss and the retransmission attempts. However, both Reno and SACK variants were observed to have a slightly higher retransmission counts than the New Reno variant.

In general, since throughput of the network is what actually matter to the user, New Reno variant would be the preferred variant under this specific condition when the speed of the nodes are kept constant at a moderate value of 10m/s.

B. Network Nodes Mobility Speed Variation Effects on TCP Variants

The effects of nodes speed variation on the performance of the TCP variants were very significant as shown in the simulation results on tables 7-9 through the throughput, transmission delay and retransmission counts. The throughput

produced by the network as a whole increases as a result of increase in the nodes speed. It follows a pattern of proportionality in that the rate of increase in the nodes speed is directly linked to the increase in the throughput of the network, that is, the higher the nodes speed in the network, the higher the rate of increase in the network's throughput provided the network size remain constant.

However, as the network size increases along an increase in the nodes speed in the networks, the throughput begin to decrease, for example, the throughput of the network when the nodes was thirty (30 nodes) with increase in the nodes mobility speed is higher than the throughput produced when the network size was increase to one hundred (100 nodes) with corresponding increase in the mobility speed.

Interestingly, as the network size is further increase together with an increase in the nodes mobility speed, the above view does not hold as the performance of the TCP variants begin to reduce, which mean more traffics are being generated and the links between nodes are breaking faster and taking more time to re-establish leading to more congestion in the network resulting in the TCP performance reduction.

The delay and retransmission attempts follows the same pattern as that of the throughput, the delay and the retransmission count were seen from the simulation results chart to reduce as the nodes mobility speed increases when the network size is small or moderate as little congestion was experience because the nodes re-establishes the broken links more faster.

Furthermore, the delay and retransmission counts experience increases as the network is more populated by increasing the nodes number to higher level while increasing the nodes mobility speed at the same time, the network fails to cope with such scenario, as more traffics were generated. The result was the high occurrence of congestion and long waiting time for the segments to be transmitted leading to higher segments loss and the subsequent retransmission attempts.

In general, New Reno is observed to have performed better, followed by the SACK while the Reno is the least performed variants among the three TCP variants investigated when the effect of increase in the network's node mobility speed is considered.

VI. CONCLUSION

The goal of this research is to review the performance of various TCP variants in specified network scenarios in the MANETs using Reno, New Reno and SACK as case study under the Dynamics Source Routing (DSR) Protocol. This study has been able to observe the impacts of some network designs and configurations on the performance of TCP variants in MANETs using throughput, transmission delay and retransmission counts as performance metrics.

The FTP, HTTP and Voice traffics were submitted to MANETs while the network size (number of nodes) and nodes mobility speed were varied.

The results show that network size and nodes mobility speed affects the performance of the TCP variants on throughput, delay and retransmission attempts. Overall,

based on this study, it is observed that New Reno performs better than he rest of the variants under a small to medium (30 -50 nodes) network size of an average nodes speed of 2m/s to 10m/s, while the SACK outperforms the other two variants in a large (100 nodes) network size of moderately high nodes speed. However, the performance of these variants under further larger (over 100 nodes) network size and faster nodes speed of over 20m/s may be different from the results obtained in this experiment, that could be considered as a further research work.

REFERENCE

1. R.C. Siva, B. Manoj, "Ad Hoc Wireless Networks: Architectures and Protocols". 1st ed., New Jersey 07458, Prentice Hall, 2012.
2. V. Athanasios, Z. Yan, S. Thrasyvoulos, "Delay Tolerant Networks: Protocols and Applications"- Wireless Networks and Mobile Communications. Boca Raton, FL 33487. CRC Press, 2011.
3. G. Pravin, K. Girish, G. Pradip, "Mobile Ad Hoc Networking: Imperatives and Challenges". IJCA Special Issue on Mobile Ad Hoc Networks (MANETs), 2010.
4. A. Seddik-Ghaleb, Y. Ghamri-Doudane, S.M. Senouci, "TCP Computational Energy Cost Within Wireless Mobile Ad Hoc Network", A Proceeding of IEEE/ACS International Conference on Computer Systems and Applications, Rabat. 2009. pp. 955- 970.
5. P.S. Noreen, "Voice Traffic over Mobile Ad Hoc Networks: A Performance Analysis of the Optimized Link State Routing Protocol". Wright-Patterson, Ohio. Air Force Institute of Technology, 2009.
6. M.I. Saad, Z.A. Zukarnain, "Performance Analysis of Random-Based Mobility Models in MANET Routing Protocol". *European Journal of Scientific Research*. Vol. 32, No. 4, 2009, pp. 444-454.
7. N.I. Sarkar, S. A. Halim, "Simulation of computer networks: simulators, methodologies and recommendations", The Proceeding of 5th International Conference on Information Technology and Application, Cairns, Australia. 2008, pp. 420-425
8. V. Pallapa, L.M. Patnaik, K. Sajal , "Mobile Wireless Networks: Integrated Service Issues". West Sussex, PO19 8SQ. Wiley-Blackwell, 2008.
9. H. Luc, F. B. Pascal, "An Overview of MANETs Simulation". Université du Havre (France). Laboratoire d'Informatique, France, 2008.
10. B. Tang, H. Gupta, S.R. Das, "Benefit-Based Data Caching in Ad Hoc Networks". *IEEE Transactions on Mobile Computing*. Vol 7, No. 3, 2008. pp. 289-304
11. K. Kathiravan, S. Thamarai, A. Selvam, "TCP performance analysis for mobile adhoc network using on-demand routing protocols". *Ubiquitous Computing and Communication Journal*, 2007. pp. 370-376.
12. P. Daniele, H. Martin, "Multipath Fading in Wireless Sensor Networks: Measurements and Interpretation". Network Communication and Information Processing Laboratory, Notre Dame, USA. 2006.
13. B. Azzedine, "Handbook of Algorithms for Wireless

- Networking and Mobile Computing". Boca Raton FL
33487-2742, Chapman & Hall, 2006.
- 14. V. Lenders, W. Jorg, M. Martin, "Analyzing the Impact of Mobility in Ad hoc Networks: From theory to reality". A Proceeding of 2nd International Workshop on Multi-hop Ad hoc Networks. May 2006, pp. 39-46
 - 15. S. Kumar, D. Jing, S. Vineet, "Medium Access Control Protocol for Ad Hoc Wireless networks". A Survey - Marlborough, MA 01752. ATI Technologies Inc., Vol. 4, Issue 3, May 2006. pp. 326-358.
 - 16. H.M El-Sayed. "Performance evaluation of TCP in mobile ad hoc networks". A proceeding of a 2nd International Conference on Innovations in Information Technology, Seoul, South Korea, 2005.

Adaptive Fuzzy Control to Design and Implementation of Traffic Simulation System

Laheeb Mohammed Ibrahim

Software Engineering

Mosul University, Collage of Computer Sc. & Math.
Mosul , Iraq

Mohammed A. Aldabbagh

Software Engineering

Mosul University, Collage of Computer Sc. & Math.
Mosul , Iraq

Abstract—

In this paper a Fuzzy Adaptive Traffic Signal System (FATSS) was designed and implemented to improve optimization and compare fix time traffic light controller. FATSS allows the user to select input parameters and tune rule base to improve optimization and compare fix time traffic light controller.

FATSS reducing the average waiting time for vehicles between 2% to 20%, and that indicate the adaptive traffic light controller based on fuzzy logic outperform is better when is compare with other fixed controller

FATSS was built using C# language in Microsoft Visual studio 2010 development environment. The simulation is implemented by Simulation for Urban Mobility(SUMO).

Keywords-component; formatting; style; styling; insert (key words)

I. INTRODUCTION

Transportation research has the goal to optimize transportation flow of people and goods. As the number of road users constantly increases, and resources provided by current infrastructures are limited, intelligent control of traffic will become a very important issue in the future. However, some limitations to the usage of intelligent traffic control exist. Avoiding traffic jams for example is thought to be beneficial to both environment and economy, but improved traffic-flow may also lead to an increase in demand [12].

Traffic light optimization is a complex problem. Even for a single intersection, there might be no obvious optimal solution. With multiple junctions, the problem becomes even more complex, as the state of one light influences the flow of traffic towards many other lights. Another complication is the fact that flow of traffic constantly changes, depending on the time of day, the day of the week, and the time of year. Roadwork and accidents further influence complexity and performance [38]. In fact, most traffic lights are controlled by fixed-time controllers. A cycle of configurations is defined in which all traffic gets a green light at a fixed point.

The split time determines how long the lights must keep on in each state. Heavy traffic roads can get preference by adjusting the split time. The cycle time is the duration of a complete cycle. In heavy traffic, longer cycles guide to good scenario.

Adaptive control strategies rely mainly on the prediction of the arriving flow [9]. There are two types of prediction. The first is based on the real-time data measured in the field to estimate the movement of vehicles detected. The other is based upon historical data to predict the future arriving flow. For convenience of referencing, we call the former *estimation* and the latter *prediction*. While long-term optimization is ideal for reaching the global optimums, the real-time data based control relies on a number of short-term optimizations to reduce uncertainty in traffic demand and improve accuracy in computation. The short-term optimization, usually in the order of 30 to 60 seconds, makes it possible for all the optimizing processes to be based on estimation rather than prediction. Effectiveness is largely dependent on the accuracy of flow prediction. No matter how the traffic information is obtained, there will always be some difference between the predicted and the field condition. Hence, a desirable adaptive control strategy should reduce reliance on prediction as much as possible.

A reliable estimation model must be developed to provide real-time traffic information for adaptive control. Vehicle arrival information is typically obtained from detectors placed upstream of the intersection, and the objective of estimation is to obtain the vehicle travel time between the upstream detector and the intersection stop line [2, 33]. For system optimization, the ability to estimate traffic conditions for a long duration is desirable, but because of geometric constraints and uncertainties in vehicle arrivals, there is most always a tradeoff between the estimation duration and data accuracy[37].

Similarly, Optimization Policies for Adaptive Control (OPAC) defines travel time as the time for the vehicle to travel between the upstream and the downstream signals [33] and the difficulty in travel time estimation must also be dealt with in congested traffic. This problem exists in the optimization process of every adaptive control system today. However, very limited up to date work is reported in the literature as to how the varying queue length will affect the arrival time estimation[37].

The effectiveness of adaptive control strategies also relies on reasonable estimation of system parameters governing queue formation/dissipation, start-up delay, and vehicle clearance. The start-up delay and the vehicle releasing rate

may be different from time to time due to the influence of construction, incident, and even the weather condition. The differences cannot be accounted for if static parameters are used in the model, and the cumulated error can become large enough to offset any systems advantage over other types of control. However, most of the existing adaptive control strategies do not contain a self-adjusting mechanism.

Fuzzy logic has been used to develop an adaptive traffic signal controller, because it allows qualitative modeling of complex systems, where it is not easy to solve using mathematical models [11, 10, 2, 21] and is good for systems that have inherent uncertainties[18].

The fundamental idea of this paper is to design and implement a general traffic light intersection simulation environment controlled by fuzzy logic with user ability to build its own fuzzy engine, including I/O parameters, membership functions, inference rule based and outputs.

This paper mainly aims to provide hand-outs in two fields, The first is environment for Traffic intersection designrs; and the second is the framework for fuzzy logic . So, there are two primary contributions made by this paper.

- 1- Combination of SUMO with Fuzzy Adaptive traffic controller represents the first simulation environment that can design any traffic intersection(s) controlled by fuzzy logic (The user can implement the fuzzy control to any SUMO traffic light intersection, can choose various parameters provided by SUMO simulation output manually and can tune the fuzzy control parameters on-line. The fuzzy control make new TLS every cycle).
- 2- Fuzzy engine classes used in adaptive control are a general fuzzy engine. So, it can be used in any other field of fuzzy logic applications, and it represents a tool for fuzzy logic systems researchers.

II. LITERATURE REVIEW

The literature review states the Intelligence Methods in Urban Traffic Signal Control. The literature review into Fuzzy logic traffic signal control are:

Pappis and Mamdani, 1977 [2] the first fuzzy logic controller was designed for an isolated two-phase intersection, which had three inputs and one output. Decisions were made every 10 seconds to decide whether to extend green time of current phase or change the way leave to the next phase according to traffic volume of all approaches. Simulations had shown that the above method was effective. This is the earliest example applying fuzzy logic to traffic controls.

Lee et al., 1995 [10] studied the use of fuzzy logic in controlling multiple junctions. Controllers received extra information about vehicles at the previous and next junctions, and were able to promote green waves. The system outperformed a fixed controller, and was at its best in either light or heavy traffic. The controller could easily handle changes in traffic flow, but required different parameter settings for each junction.

Choi et al., 2002 [4] used fuzzy logic controllers, and adapted them to cope with congested traffic flow. Comparisons with fixed fuzzy-logic traffic light controllers

indicated that this enhancement could lead to larger traffic flow under very crowded traffic conditions.

Trabia et al., 1999 [18] presented a two-stage fuzzy logic control method. The controller was designed to be responsive to real-time traffic demands. The fuzzy controller used vehicle loop detectors, placed upstream of the intersection on each approach, to measure approach flows and estimate queues. These data were used to decide, at regular time intervals, whether to extend or terminate the current signal phase. In the first stage, observed approach traffic flows were used to estimate relative traffic intensities in the competing approaches. In the second stage, these traffic intensities were then used to determine whether the current signal phase should be extended or terminated.

Zhiyong et al. 1999 [13] designed a new traffic controller for a single intersection based on the people's strategic decision process to the multi-phase signal traffic control. The inputs of controller were the queue lengths on the contiguous phase lanes and the differences between the current queue lengths and the ones in next phase lanes. The outputs of one were extending green time of the current phases or changing into the successional phases. Fuzzy reasoning rulers were created according to the experiences of traffic police. This controller had been applied practically and worked very well.

Liu et al. 1997 [14] proposed a hierarchical fuzzy control method, and applied it to the arterial coordinated control. Its fundamental principle was to use hierarchical structure and fuzzy theory to solve real time coordinated control problems of traffic trunk road. It regarded all intersections on the trunk as subsystems. According to the cycle length provided by a coordinator, it adjusted the splits of all approaches on line by using fuzzy control methods. Traffic volumes detected at all intersections were sent to the coordinator. The cycle length and splits were determined by using fuzzy control method. The goal of the coordinator and subsystems was to minimize the queue length. Simulation results showed that it could shorten the queue, and reduce total traffic delay.

Aksaç et al. 2011 [1] implemented a real time traffic simulator with an adaptive fuzzy inference algorithm that arranges the foreseen light signal duration. It changes the time duration of lights depending on waiting vehicles behind green and red lights at crossroad. The simulation has also been supported with real time graphical visualization. it creates random traffic flows according to specified parameters.

Zade And Dandekar, 2012 [36] proposed a simulation of fuzzy traffic controller using SIMULINK environment of MATLAB. Results for green light extension time in seconds are obtained with SIMULINK model of fuzzy traffic controller which shows linear increment in the green light extension time for increasing values of traffic density and traffic flow rate. The simulation results showed linearity between inputs applied to the Fuzzy Inference System and output drawn from it.

Most researchers have worked on control an isolated intersection with fuzzy control method [2, 18, 13, 32, 25, 8, 33, 34, 20]. Few of them apply this method to the coordinated control of arterial or area traffic. Area traffic coordinated

control system is a complex large-scale system. There are many interactional factors, and it is difficult to describe the whole system using some qualitative knowledge. It is just the limitations of fuzzy control methods. In a word, it is more appropriate to use fuzzy control methods for traffic signal control of the isolated intersection.

III. FUZZY LOGIC

The problems of uncertainty, imprecision and vagueness have been discussed for many years, particularly by philosophers. The nature of vagueness and the ability of traditional Boolean logic to cope with concepts and perceptions that are imprecise or vague have been discussed at length[72,65].

Fuzzy systems are being used successfully in an increasing number of application areas; they use linguistic rules to describe the systems. These rule-based systems are more suitable for solving the complex system problems mathematically. One of the most important considerations for designing any fuzzy system, the generation of the fuzzy rules as well as the membership functions are applied for each fuzzy set. In most existing applications, the fuzzy rules are generated by expert system in the area, especially for control problems with only a few inputs[16].

Based on the study of Hoogendoorn et al.[6] and others (e.g., Sayers et al.[23,24]), the key benefits of a fuzzy logic (FL) approach are can fuse quantitative and qualitative information, Fuzzy systems can trade off potentially conflicting objectives with the help of expert knowledge, Fuzzy control successfully provides a transparent, flexible and adaptable control structure. The transparency and intuitive nature of the rule base and input variables adopted in FL control system make it relatively easy to develop, test, and modify, FL is well suited to deal with nonlinear input/output relationships, FL can handle the model even when the model parameters are not precisely known or when no prior knowledge about the system is present at all. In fact, FL techniques use measurement data from the process.

To implement fuzzy logic technique to a real application requires the following three steps, see Fig. 1 [35]:

1. Fuzzification – converting classical data or crisp data into fuzzy data or Membership Functions (MFs)
2. Fuzzy Inference Process – combining membership functions with the control rules to derive the fuzzy output
3. Defuzzification – using different methods to calculate each associated output and putting them into a table: the lookup table. Picking up the output from the lookup table based on the current input during an application

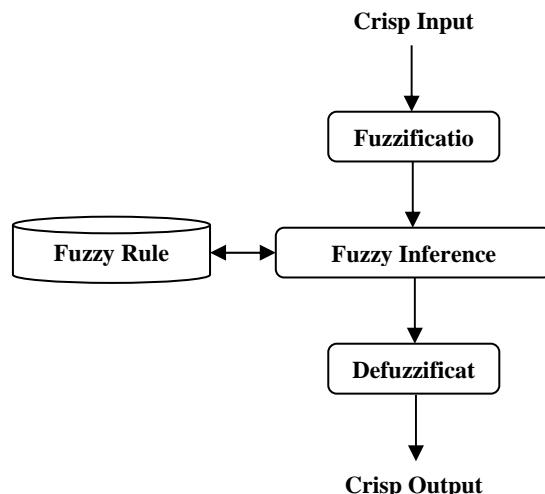


Figure 1. Structure of a Fuzzy Logic Model

IV. SIMULATION

The increasing power of computer technologies, the evolution of software engineering and the advent of the intelligent transport systems have prompted traffic simulation to become one of the most used approaches for traffic analysis in support of the design and evaluation of traffic systems. The ability of traffic simulation to emulate the time variability of traffic phenomena makes it a unique tool for capturing the complexity of traffic systems[28].

Simulation is used for scientific modeling of natural systems or human systems in order to gain insight into their functioning. It can be used to show the eventual real effects of alternative conditions and courses of action. It is also used when the real system cannot be engaged, because it may not be accessible, or it may be dangerous or unacceptable to engage, or it is being designed but not yet built, or it may simply not exist[3].

A computer simulation (or "sim") is an attempt to model a real-life or hypothetical situation on a computer so that it can be studied to see how the system works. By changing variables, predictions may be made about the behavior of the system. A good example of the usefulness of using computers to simulate can be found in the field of network traffic simulation. In such simulations, the model behavior will change each simulation according to the set of initial parameters assumed for the environment[3].

One of the systems that is best studied using a computer simulation is a traffic network. It is more common to experiment with traffic networks in a computer simulated environment because experimenting with traffic in the real environment is not practical[20].

V. TRANSPORTATION SYSTEM

Transportation is an essential element in the economic development of a society. Without good transportation, a nation or region cannot achieve the maximum use of its natural resources or the maximum productivity of its people. Progress in transportation is not without its costs, both in human lives and environmental damage, and it is the responsibility of the transportation engineer working with the public to develop high-quality transportation consistent with the available funds and social policy and to minimize damage. Transportation is a significant element in our national life. It accounts for about 18 percent of household expenditure and employs over 10 percent of the workforce[19].

The traffic or highway engineer must understand not only the basic characteristics of the driver, the vehicle, and the roadway, but how each interacts with the others. Information obtained through traffic engineering studies serves to identify relevant characteristics and define related problems. Traffic flow is of fundamental importance in developing and designing strategies for intersection control[19].

A. Intersection Control

An intersection is an area shared by two or more roads. Its main function is to allow the change of route directions. A simple intersection consists of two intersecting roads; a complex intersection serves several intersecting roads within the same area. The intersection is therefore an area of decision for all drivers; each must select one of the available choices to proceed. This requires an additional effort by the driver that is not necessary in non intersection areas of a highway. The flow of traffic on any street or highway is greatly affected by the flow of traffic through the intersection points on that street or highway because the intersection usually performs at a level below that of any other section of the road[19].

B. Traffic Signals

One of the most effective ways of controlling traffic at an intersection is the use of traffic signals. Traffic signals can be used to eliminate many conflicts because different traffic streams can be assigned the use of the intersection at different times. Since this results in a delay by vehicles in all streams, it is important that traffic signals be used only when necessary. The most important factor that determines the need for traffic signals at a particular intersection is the intersection's approach traffic volume, although other factors such as pedestrian volume and crash experience may also play a significant role. The Manual on Traffic Signal Design gives the fundamental concepts and standard practices used in the design of traffic signals[19]. In addition, the Manual on Uniform Traffic Control Devices (MUTCD) describes eight warrants in detail, at least one of which should be satisfied for an intersection to be signalized. However, these warrants should be considered only as a guide; professional judgment based on experience also should be used to decide whether or not an intersection should be signalized. The factors considered in the warrants are: (Warrant 1- Eight-hour

vehicular volume, Warrant 2- Four-hour vehicular volume, Warrant 3- Peak hour, Warrant 4- Pedestrian volume, • Warrant 5- School crossing, Warrant 6- Coordinated signal system, Warrant 7- Crash experience, • Warrant 8- Roadway network)

The warrants described earlier will help the engineer only in deciding whether a traffic signal should be used at an intersection. [26]. however, there are numbers of terms commonly used in the design of signal times, these are (Controller, Cycle, Phase, Interval, Offset, Change and clearance interval, All-red interval, Peak-hour factor, lane group, Critical lane group, Saturation flow rate) [26].

A traffic signal that is properly designed and timed can be expected to provide benefits for the orderly and efficient movement of people, and effectively maximizes the volume movements served at the intersection. The degree to which these benefits are realized is based partly on the design and partly on the need for a signal. A poorly designed signal timing plan or an unneeded signal may make the intersection less efficient, less safe, or both[28].

C. Traffic controller (Types of Operation)

Despite the many variations in their design, traffic signals can be classified according to operational type as (Pre-Timed (or fixed time), Semi Actuated, Fully Actuated, Adaptive Traffic Signal Controls).

D. Adaptive Traffic Signal Control Overview

Adaptive traffic signal control is a concept where vehicular traffic in a network is detected at an upstream and/or downstream point and an algorithm is used to predict when and where the traffic will be and to make signal adjustments at the downstream intersections based on those predictions. The signal controller utilizes these algorithms to compute optimal signal timings based on detected traffic volume and simultaneously implement the timings in real-time. This real-time optimization allows a signal network to react to volume variations, which results in reduced vehicle delay, shorter queues, and decreased travel times. [28].

All adaptive control systems are driven by a similar conceptual process[42]:

1. Collecting data in real-time from sensor systems to identify traffic conditions.
2. Evaluating alternative signal timing strategies on a model of traffic behavior.
3. Implementing the “best” strategy according to some performance metric.
4. Repeating steps 1,2,3 again and again.

Each adaptive system is distinguished by how it uses different components or approaches to these four key steps in the control of the traffic system[42].

The search methodology itself is not typically important for signal timing, but how the traffic engineer is able to constrain or influence the search of alternative timing strategies is critical to the success of adaptive system deployment. For example[28]:

- The minimum and maximum phase lengths.

- Which phase sequences are allowed or disallowed.
- How rapidly or slowly the system allows timing parameter changes.

Other parameters, specific to individual adaptive systems, are key elements to guide the adaptive system in searching appropriate and effective signal timing strategies[28].

E. Data Collector

With the ever growing traffic demand and rising challenge of controlling it, our networks are equipped with different sensors to measure the actual traffic state. This data is essential for evaluating the performance of transportation systems and for supporting the development of new approaches and technologies that address traffic problems.

F. Detection Technologies

Optimally, consideration of detector technology should involve the following three factors (Cost, Practicality, Accuracy) [41]:

G. Traffic Simulation (SUMO - Simulation of Urban Mobility Traffic Simulation)

One of the systems that is best studied using a computer simulation is a traffic network. It is more common to experiment with traffic networks in a computer simulated environment because experimenting with traffic in the real environment is not practical[5]. The following are well known and widely used traffic simulation packages (SUMO - Simulation of Urban Mobility [3], Quadstone Paramics [22], Treiber's Microsimulation of Road Traffic [30] , Aimsun, [31], Trafficware SimTraffic, [29], CORSIM TRAFVU) [15]

SUMO is an open source software gives users the right to use the software free of charge; a feature that is not very common in commercial software packages. However, open source projects are becoming more and more popular because they give their users the right to use, study and modify the program without any restriction.

Out of the six software packages (Sumo, Treiber's Microsimulation of Road Traffic, Quadstone Paramics Modler, Aimsun, Trafficware SimTraffic, CORSIM TRAFVU) , only the first two are free to use [3, 30], while the other 4 are paid [22, 32,29,15]. While the free packages could be investigated to their full potential, we could only study the demo versions of the four commercial packages. The demo versions had 30 days usage restrictions and/or feature restrictions.

Another feature of the free software packages (SUMO and Treiber's Micro-simulation of road traffic) is that their source codes are freely available for download and use. The difference between the two packages is that SUMO is actually an open source project that is being developed by two different institutions, while Treiber's Microsimulation is a personal software project whose source code has been made available. The source code is not available for study, modification or research for users of the other four commercial software

packages (Paramics Modeller, Aimsun, SimTraffic and CORSIM). One of the most popular features of open source projects is that they can be further modified by other programmers, as already mentioned previously. This feature supports the potential for parallelizing simulaion models and packages to explore high end computer systems.

VI. FUZZY ADAPTIVE TRAFFIC SIGNAL SYSTEM

The mainly preferred feature in a traffic controller at an intersection is that it should be adaptive to any changes in the traffic demand. In case of the traffic controllers that are usually used, the relative durations of the green phases are determined by computer programming based on the traffic pattern at an intersection. But these traffic controllers are not adaptive because the settings can only be altered manually or by computer commands sent by the traffic control center. This problem is solved by using Fuzzy Adaptive Traffic Signal System (FATSS), which is capable of signaling adaptively at an intersection. The objective of this section is to propose a design methodology for modeling fuzzy controllers.

The main role of FATSS is to optimize the green phase duration using the fuzzy engine which uses the traffic demand variables as input variables and membership functions. Then, the fuzzy engine initiates the rule base that depends on input variables and according to outputs generated by fuzzy engine. The simulation program SUMO will change the phase durations to be suitable for new demand state. The general structure of the fuzzy traffic Signal system UML([Unified Modeling Language](#)) Activity diagram will have the structure shown in Fig. 2

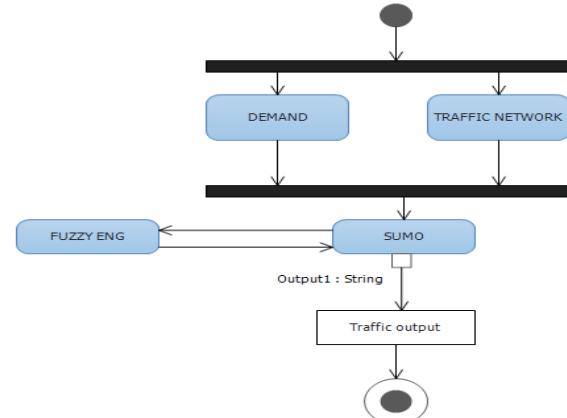


Figure 2. UML Activity Diagram of FATSS

A. FATSS inputs overview

The proposed system is based on multiple inputs which are necessary to run SUMO simulator like traffic network description and demand.

1. Traffic Network

SUMO uses an own road network description. Although being readable (xml) by human beings, at a coarse scale, SUMO road networks are directed graphs. "Nodes" represent intersections/junctions, and "edges" roads/streets. Then is the use of [NETCONVERT](#) [3] tool to build the network file.

- Node Descriptions

Inside the node files, normally having the extension ".nod.xml", every node is described in a single line which looks like this:

```
<node id=<STRING> x=<FLOAT> y=<FLOAT>
[type=<TYPE>]/>
```

The straight brackets ('[' and ']') indicate that the parameter is optional. Each of these attributes has a certain meaning and value range explained in table I.

Table I. Node Attributes Description

Attribute Name	Value Type	Description
id	id (string)	The name of the node
x	Float	The x-position of the node on the plane in meters
y	Float	The y-position of the node on the plane in meters
type	enum ("priority", "traffic_light", "right_before_left", "unregulated")	An optional type for the node

The following types are possible. Any other string is counted as an error and will yield in a program stop:

- **priority:** Vehicles on a low-priority edge have to wait until vehicles on a high-priority edge have passed the junction.
- **traffic_light:** The junction is controlled by a traffic light.
- **right_before_left:** Vehicles will let vehicles coming from their right side pass.
- **unregulated:** The junction is completely unregulated - all vehicles may pass without braking; this may result in additional incidents.

A complete file should look like the xml code 1, which is the node file "fuzzy_node.nod.xml"

XML code 1: node description

```
<nodes>
<node id="5" x="0.0" y="0.0" type="traffic_light" />
<node id="2" x="-500.0" y="0.0" />
<node id="3" x="0.0" y="-500.0" />
<node id="4" x="+500.0" y="0.0" />
<node id="1" x="0.0" y="+500.0" />
</nodes>
```

Only the first node named "5", which is the node in the center of the network, is a traffic light controlled intersection. All other nodes are uncontrolled. You may also notice, that each of both ends of a street needs an according node. This is not really necessary as you may see soon, but it eases the understanding of the concept: every edge (street/road) is a connection between two nodes (junctions).

- Edge Descriptions

The edge is a basic part of a road network, like a normal street which connects two nodes. Within the edges file, each description of a single edge looks like this:

```
<edge id=<STRING> from=<NODE_ID>
to=<NODE_ID> [type=<STRING>]
[numLanes=<INT>] [speed=<FLOAT>]
[priority=<UINT>] [length=<FLOAT>]
[shape=<2D_POINT>[ <2D_POINT>]*]
[spreadType="center"] [allow=<VEHICLE_CLASS>[
<VEHICLE_CLASS>]*"] [disallow=<VEHICLE_CLASS>[
<VEHICLE_CLASS>]*"]]
```

The beginning and the end nodes are defined using their IDs (from="<NODE_ID>" to="<NODE_ID>"). Each edge is unidirectional and begins at the "from" node and ends at the "to" node. If a name of one of the nodes can not be dereferenced, because they have not been defined within the nodes file, an error is generated. For each edge, some further attributes should be supplied, such as the number of lanes the edge has (numLanes), the maximum speed allowed on the edge speed, and the priority may be defined optionally.

The length of this edge will be computed as the distance between the starting and the end point. As an edge may have a more complicated geometry, you may supply the edge's shape within the shape attribute. If the length of the edge is not given otherwise, the distances of the shape elements will be summed.

Table II lists an edge's attributes. The priority plays a role during the computation of the way-giving rules of a node. Normally, the allowed speed on the edge and the edge's number of lanes are used to compute which edge has a greater priority on a junction. Using the priority attribute, you may increase the priority of the edge making more lanes yielding in it or making vehicles coming from this edge into the junction, not waiting.

- Traffic Light Program

Usually, [NETCONVERT](#) produces traffic lights and programs for intersections during the generation process of the networks. But these computed programs differ quite often from those found in real world. To supply the simulation with real traffic light programs, it is possible to load extra programs. In addition, [SUMO/SUMO-GUI](#) allows to load definition which describe when and how a set of traffic lights can switch from one program to another. The user can load new definitions for traffic lights as a part of additional files.

As soon as loaded, the last program will be used. Switching between programs is possible via Weekly Switch Automatism WAUTs and/or TraCI. Also, one can switch between them using the GUI context menu. Table III shows attributes/elements of traffic light signal (TLS). Each phase is defined using the attributes in table IV.

Table II: Edge's Attributes Description

Attribute Name	Value Type	Description
Id	id (string)	The name of the edge
From	referenced node id	The name of a node within the nodes-file the edge shall start at
To	referenced node id	The name of a node within the nodes-file the edge shall end at
Type	referenced type id	The name of a type within the SUMO edge type file
numLanes	int	The number of lanes of the edge; must be an integer value
Speed	Float	The maximum speed allowed on the edge in m/s; must be a floating point number (see also "Using Edges' maximum Speed Definitions in km/h")
Priority	int	The priority of the edge
Length	Float	The length of the edge in meter
Shape		List of positions; the start and end node are omitted from the shape definition; an example: <edge id="e1" from="0" to="1" shape="0,0 0,100"/> (do not separate the numbers with a space!) describes an edge that after starting at node 0, first visits position 0,0 than goes one hundred meters to the right before finally reaching the position of node 1
spreadType	enum ("right", "center")	The description of how to spread the lanes; "center" spreads lanes to both directions of the shape, any other value will be interpreted as "right"
Allow	list of vehicle classes	Explicitly allows the given vehicle classes (not given will be not allowed). Vehicle classes must be separated using ''.
Disallow	list of vehicle classes	Explicitly disallows the given vehicle classes (not given will be allowed). Vehicle classes must be separated using ''.

Table III: TLS attributes/elements.

Attribute Name	Value Type	Description
id@tlLogic	id (string)	The id of the traffic light
type	enum (static, actuated, agentbased)	The type of the traffic light
programID	id (string)	The id of the traffic light program; Please note that "off" is reserved, see below.
offset	int	The initial time offset of the program

Table IV : Tls Attributes Description

Attribute Name	Value Type	Description
duration@phase	time (int)	The duration of the phase
state@phase	list of signal states	The traffic light states for this phase, see below

Each character within a phases' state describes the state of one signal of the traffic light. A single lane may contain several signals - for example one for vehicles turning left, one for vehicles which move straight. This means that a signal does not control lanes, but links - each connecting a lane

which is incoming into a junction and one which is outgoing from this junction. Table V explain signal colors.

Table V: TLS signal colors.

Character	Description
R	'red light' for a signal - vehicles must stop
y	'amber (yellow) light' for a signal - vehicles will start to decelerate if far away from the junction, otherwise they pass
g	'green light' for a signal, no priority - vehicles may pass the junction if no vehicle uses a higher prioritized for stream, otherwise they decelerate for letting it pass
G	'green light' for a signal, priority - vehicles may pass the junction

After having defined a TLS program as above, it can be loaded as an additional file; of course, a single additional file may contain several programs. It is possible to load several programs for a single TLS into the simulation. The program loaded as last will be used (unless not defined differently using a WAUT description). All sub keys of the additional programs must differ if they describe the same TLS. It is also possible to load a program which switches the TLS off by giving the **programID** the value "off", shown in xml code bellow.

```
<tlLogic id="0" type="static" programID="off"/>
```

B. SUMO-GUI Simulation

After completing the input files for SUMO-GUI ,which are described in last sections (Node File, Edges File, Traffic Light Program) ,now the simulation is ready to run. Fig. 3, shows the SUMO-GUI window

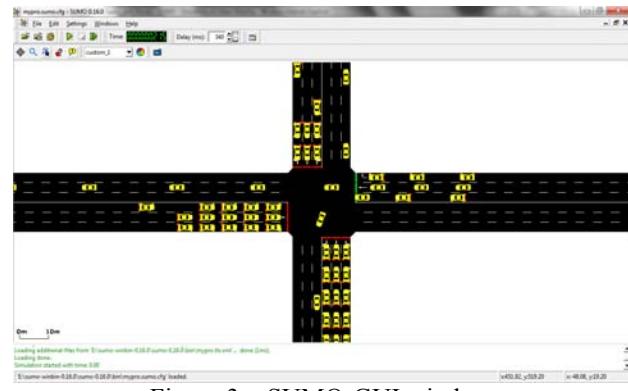


Figure 3. : SUMO-GUI window

C. On-Line Simulation Information Retrieval

Traci is the short term for "Traffic Control Interface", see Fig. 4. It provides the access to a running simulation, and allows to retrieve values of simulated objects and to manipulate their behaviors "on-line". Traci uses a TCP based client/server architecture to provide access to [SUMO](#). Thus, [SUMO](#) acts as a server that is started with additional

command line options(remote-port) then **SUMO** will listen to for incoming connections. When started with the remote-port option, **SUMO** only prepares the simulation and waits for an external application(Traffic Fuzzy Engine), that takes over the control. After starting **SUMO**, a client connects to **SUMO** by setting up a TCP connection to the appointed **SUMO** port.

The client application sends commands to **SUMO** to control the simulation run, to influence single vehicle's behavior or to ask for environmental details. **SUMO** answers with a *Status*-response to each command and additional results that depend on the given command. The client is responsible for shutting down the connection using the **close** command. The system will use TraCI to retrieve input parameters for traffic fuzzy engine. Table VI presents an example for information that can be retrieved using TraCI commands. The information retrieved in table VI will be summarized to derive input parameters for traffic fuzzy engine.

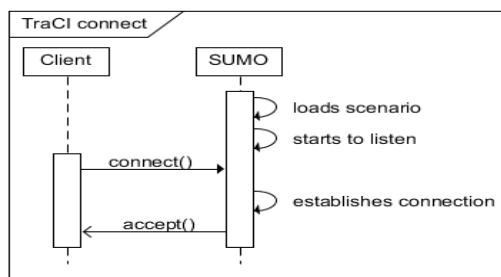


Figure 4. TraCI establishing a connection to SUMO

Table VI: Retrievable Induction Loop Variables

Variable	ValueType	Description
id list (0x00)	stringList	Returns a list of ids of all induction loops within the scenario (the given Induction Loop ID is ignored)
position (0x42)	double	Returns the position of the induction loop at its lane, counted from the lane's begin, in meters.
lane ID (0x51)	string	Returns the ID of the lane the induction loop is placed at.
count (0x01)	int	Returns the number of induction loops within the scenario (the given Induction Loop ID is ignored)
last step vehicle number (0x10)	integer	Returns the number of vehicles that were on the named induction loop within the last simulation step [#];
last step mean speed (0x11)	double	Returns the mean speed of vehicles that were on the named induction loop within the last simulation step [m/s]
last step vehicle ids (0x12)	stringList	Returns the list of ids of vehicles that were on the named induction loop in the last simulation step
last step occupancy (0x13)	double	Returns the percentage of time the detector was occupied by a vehicle [%]

last step mean vehicle length (0x15)	double	The mean length of vehicles which were on the detector in the last step [m]
last step's time since last detection (0x16)	double	The time since last detection [s]
last step's vehicle data (0x17)	complex	A complex structure containing several information about vehicles which passed the detector

D. Input Parameters For Traffic Fuzzy Engine

The previous section describes the method to retrieve information from running simulation (On-line). Fig. 5 shows two parameters (queue length and waiting time) that can be derived from retrieved information to become input parameters for traffic Fuzzy engine.

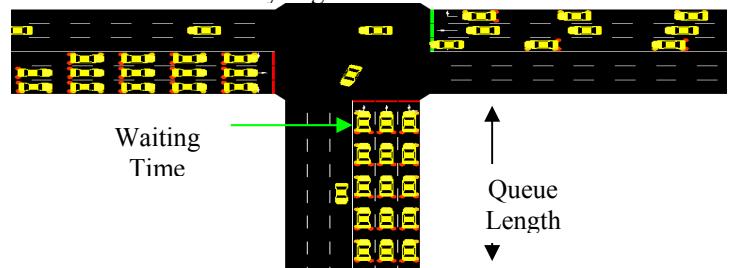


Figure 5. Simulation State Variable

1. Queue Length

The queue length value mean number of vehicles stopped in a lane behind the stop line at a traffic signal waiting for green phase at time t [27]. or the sum of arriving vehicles during the red light time period and the remaining vehicles at the end of previous green light period. During the red interval, the queue of vehicles waiting at the intersection begins to increase. The queue reaches its maximum length at the end of the red interval. When the signal changes to green, the queue begins to clear as vehicles depart from the intersection at the saturation flow rate . For a given time, the difference between the arrival pattern and the service pattern is the queue length.

2. Waiting Time

Waiting time of a single vehicle t_w is basically the time from its arrival to the intersection till the beginning of the green light phase for the vehicle's lane. If an arriving vehicle has green light, then waiting time equals zero [17].The user can summarize the waiting time as total waiting time or average waiting time for one lane or group of lanes for one direction or for all directions.

3. Arrival Flow Rate (Veh/Sec)

The mean of a statistical distribution of vehicles arriving at a point or uniform segment of a lane or roadway.

E. Traffic Fuzzy Engine (TFZENG)

While SUMO simulation is running, the Traffic fuzzy engine can connect as client to SUMO simulation and read the necessary parameters to start the engine which starts to read input parameters like Queue Length (QL) , build membership function and create linguistic variables for it. Fig. 6 explains the UML component diagram for SOMU and Traffic fuzzy engine.

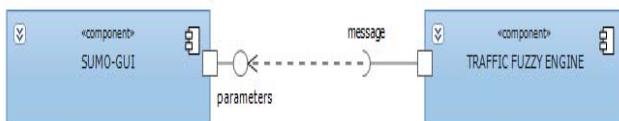


Figure 6. UML Component Diagram for SOMU and TFE.

Because the inputs are real numbers (crisp values) ,so the first step in TFZENG is to represent the input parameter as linguistic variable and build the membership functions according to specific ranges using **Fuzzy Linguistic Variable (FZLV)** class which represents the first class in TFZENG class library. The next section will explain each class in TFZENG and its effort in engine.

1. Traffic Fuzzy Engine (TFZENG) Classes Description

The TFZENG includes 4 classes which corporate to receive input parameters from simulation and process it to give the crisp value as output returned to control the simulation. **Fuzzy Linguistic Variable (FZLV)** is the first class that manipulates the input parameters. This class is responsible for building the linguistic variables for each one of input parameters and it dominates FZMF class. So the Fuzzy Membership Function (FZMF) is a member in FZLV. Each input parameter is defined as an instance of FZLV and because AFC receives real numbers from simulation, it must be converted to a linguistic variable.

The FZLV class is responsible for fuzzification process which converts the numeric value received from simulation to linguistic variables through triangular fuzzifier. At the same time, it will add membership functions with the possibility of changing values during simulation; a feature that provides to the user the possibility of tuning fuzzy engine Online. Each membership function has 4 values for triangular and trapezoidal which represent the values of the function for each input parameter from simulation more than one membership functions.

All membership functions belonging to traffic fuzzy engine belong to a special class FZMF. It is the class which is responsible for creating membership functions where each membership functions is an instance of the class FZMF. After the configuration of input linguistic variables with their membership functions, the user will configure the output linguistic variable and its membership functions which will be used later in the defuzzification process. Defuzzification class responsible for converting the output linguistic variable to

crisp values (green times). The defuzzification process is done using the most widely used centroid method. After the defuzzification process, the traffic fuzzy engine will build TLS (traffic light signal) table relying on new times resulting from Traffic fuzzy engine and sends the table to change simulation signals and repeat previous operations per cycle.

2. Traffic Fuzzy Engine (TFZENG)Classes Implementation

All TFZENG classes are created by C# and the following sections will explain the implementation of each class

• Fuzzy Linguistic Variable (FZLV)

This class is responsible for creating the linguistic variable instances for each input and output parameters. The algorithm 1 describes the working of FZLV class.

Step 4 of algorithm 1 explains that if the current FZLV instance does not have a membership function, the algorithm will jump to another class (FZMF class) which is a member of FZLV class so the new instance of FZMF will be a member of FZLV current instance.

Algorithm 1: FZLV Class Implementation

Algorithm

Input: Name(string),Value.

Output: FZLV instance (Fuzzified Linguistic Variable).

Begin

Step 1: Compare name with all existing instance names.

If found return error "naming instance"

Step 2: Create FZLV instance Name.

Step 3: Set LV value.

Step 4: Does current LV have Membership Function

Yes: Fuzzify the LV value step 5.

No : Create new FZMF instance for current LV.

Step 5: **FOR** each membership function in current LV **Do**

If range1 current LV between range1 and range2

return (value - range1) / (range2 - range1);

else if value between range2 and range3

return 1;

else if value between range3 and range4

return (range4 - Value) / (range4 - range3);

else return 0;

End

• Fuzzy Membership Function (FZMF)

The Fuzzy Membership Function is responsible for creating a membership function set for current FZLV instance.

So all functions of this class are called by current FZLV instance. Algorithm 2 describes the work of FZMF.

Algorithm 2: FZMF Class Implementation Algorithm

```

Input: MF name , Range1, Range2, Range3, Range4.
Output: FZMF instance.
Begin
    Step 1: Compare MF name with all existing instances
    name.
        If found return error "naming instance"
    Step 2:
        A = Range3 – Range2;
        B = Range4 - Range1;
        C = Range2 – Range1;
        S=((2 * A * C) + (A * A) + (C * B) + (A *
        B)
        + (B * B)) / (3 * (A + B)) + Range1
    Step 3:
        M = S – Range1;
        N = Range4 – Range1;
        O=(value * (N + (N - (M * value)))) / 2
        return O;
End

```

In steps 2 and 3 of algorithm 2, the FZMF calculates the centroid value for current membership function ranges and return it to the current FZLV instance.

3. Fuzzy Rules (FZR)

Fuzzy Rules are the class that is responsible for creating and manipulating the fuzzy rule base which is used by fuzzy inference system. The main function in this class is to manipulate IF-THEN strings. So this class will receive fuzzy rules from user and then validates them with current FZLV and FZMF instances. Algorithm 3 describes the main functions of FZR class.

Algorithm 3: FZR Class Implementation Algorithm

```

Input: IF-THEN string.
Output: FZR instance.
Begin
    Step 1: Is the Structure of IF-THEN string
    complete
        No: error " IF-THEN structure error"
    Step 2: for each FZMF instance
        Search antecedent in FZMF name
        Not Found :"error antecedent name"
    Step 3:
        for each FZMF instance
        Search consequent in FZMF name
        Not Found :"error consequent name"
    Step 4: return.
End

```

Algorithm 3 concerns with validation of rule statements. Firstly, it validates statement structure to assure that IF and THEN parts are found. Then step 2, assures that antecedent name (IF condition part) is found in FZMF instances. Finally step 3 assures that consequent name (THEN part) is found in FZMF instances. Fig. 7 shows the GUI for adding, removing and editing the fuzzy rules. Each variable (input/output) represented by ComboBox its value item collections belong to FZMF instances for a specific variable. The AFC reads it automatically from FZMF existing instances. All Fuzzy rules will be activated by AFC program after user rules activation command button "Active". And because a fuzzy rule can have multiple antecedents, so the user can use And/Or ComboBox control to add and/or between antecedent variables. The fuzzy operator (AND or OR) is used to obtain a single number that represents the result of the antecedent evaluation. If the user uses this Fuzzy Rules Builder during simulation running all edited (tuned) rules will be active for the next cycle. So the new rules will affect the phases time of the next cycle (not the current cycle).

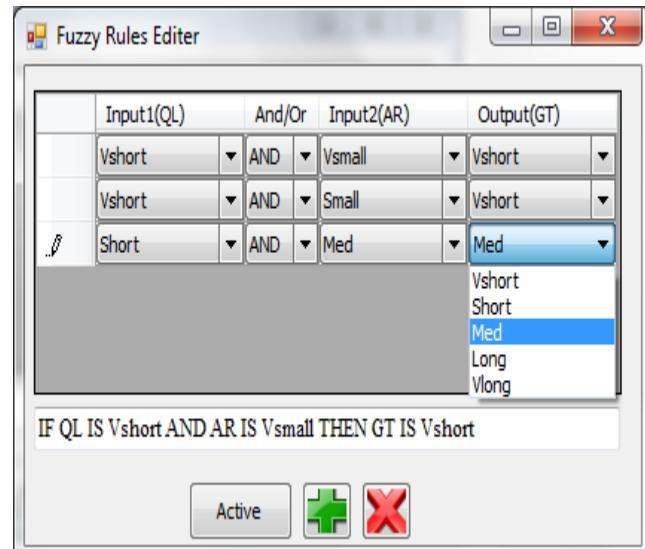


Figure 7. Fuzzy Rules Builder GUI.

- Traffic Fuzzy Engine (TFZENG)**

Traffic Fuzzy Engine class is the main class in the fuzzy engine and it is responsible for the defuzzification process. All other classes in the engine are members in this class. So, TFZENG class can inherit any instance of the classes. Algorithm 4 describes the TFZENG class work. The TFZENG class algorithm 4 explains that the engine depend on Center of Gravity Method (COG) to calculate the output value of fuzzy engine. Algorithm 5 shows the overall operation step to calculate the output value from input value using all fuzzy engine classes.

Algorithm 4: TFZENG Class Implementation Algorithm

```

Input: FZLV instance name.
Output: Defuzzification crisp value.
Begin
    NUM=0;DOM=0
    Step 1: For each FZMF in FZLV instance
            name Do
            Calculate FZMF.value (algorithm 42)
            NUM=NUM+ FZMF.S * FZMF.O
            DOM=DOM+FZMF.O
            Step 2: COG=NUM/DOM
    Step 3: return COG.
End

```

Algorithm 4.5: All Fuzzy Classes Implementation Algorithm

```

Input: input crisp values.
Begin
    Step 1: For each input and output value Do
            Create FZLV instance (algorithm 1).

    Step 2: For each FZLV instance Do
            Create FZMF(algorithm 2).

    Step 3: Create FZR instances( algorithm 3)

    Step 4:Defuzzify (algorithm 4).
End

```

Engine. Also the window form can display a specific simulation output according to Checked Variable (i.e. Queue Length, Arrival Rate and Waiting Time) at the same window. Fig. 10 shows an example of retrieved information from running simulation which represents simulation time until step 250 stopped, checking only Queue length and Waiting Time parameters, and retrieving only Queue length and Waiting Time parameters.

Depending on the current parameter, the user can build the linguistic variable and membership functions by click "Edit" button for each parameter. The membership function will depend on retrieved values. For instance the maximum Queue length retrieved from simulation will be the max range value for membership functions. Figure 11 shows the user interface for Build or Tune the membership function and it provide the following operations:

- Adding new membership function to current input parameter.
- Deleting existed member function from current input parameter.
- Drawing membership functions.
- Saving membership functions with values to XML file.
- Loading membership functions with values from Exist XML file.
- Editing specified membership function values (tuning).

F. AFC implementation

Section (A.1 Traffic network) describes the classes used by AFC program to control the simulation. This section will describe the implementation of AFC program and the way to control the SUMO simulation. The AFC program begins with loading configuration file which determines the traffic network that will be simulated. The configuration file is a SUMO specific XML file that contains a description and information about simulation needed files. The configuration file is responsible for specifying the TraCI remote port to connect to SUMO simulation. After loading the configuration file, the simulation traffic network needs a demand now to start the simulation. The demand can be chosen by AFC by using load demand window (Fig. 8). The user can choose any demand file to start the simulation. Fig. 9 shows the overall diagram of AFC with SUMO.

Now the simulation is ready to run by one click on "start simulation" button . The user also can choose the simulation output file or the simulation will start with default. Indeed, the simulation will load network and demand, then pauses, waiting for user controlling commands which user can manipulate by window form, which shows the number of steps that the user can jump in simulation or specify the input parameters which the user want to send to the Traffic Fuzzy

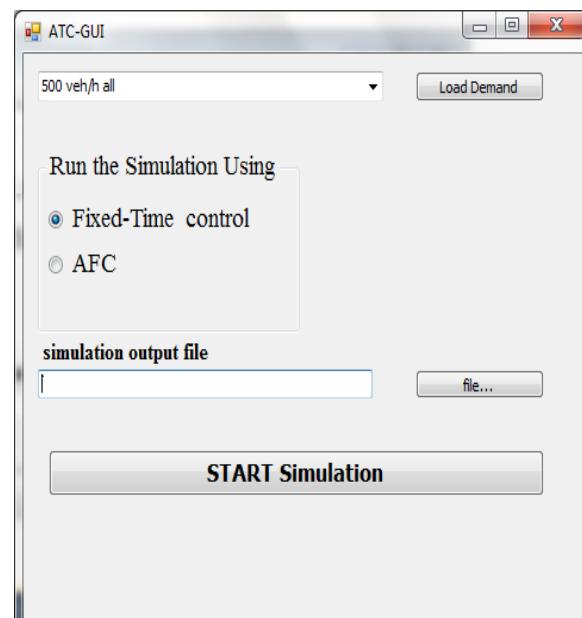


Figure 8. AFC Load Demand Window

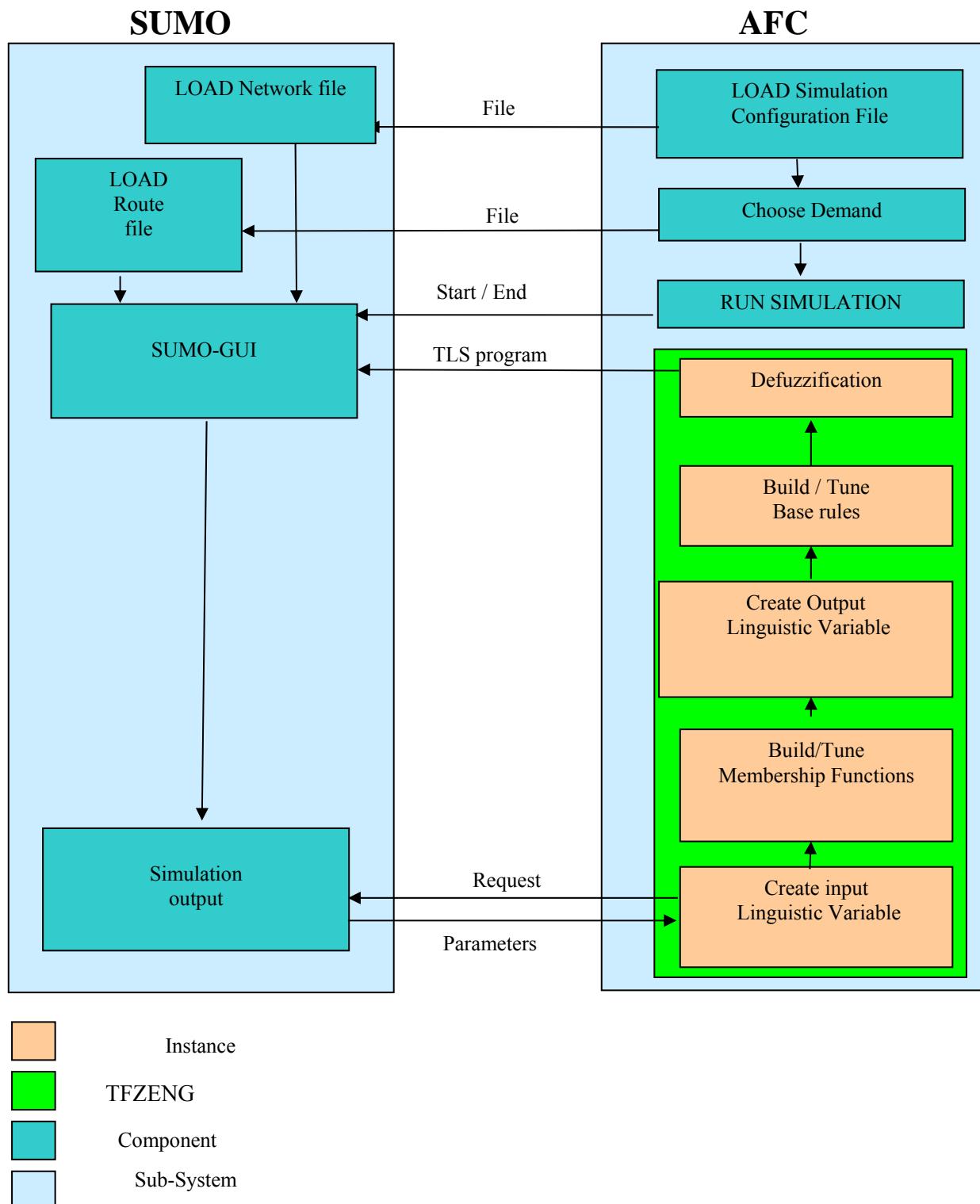


Figure 9 : Overall diagram of AFC with SUMO

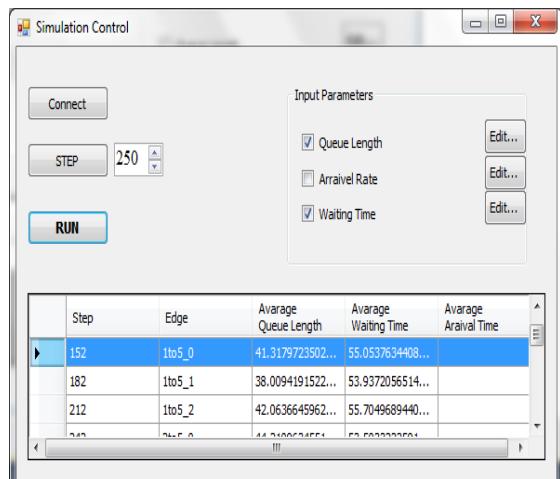


Figure 10 : AFC Simulation Control Window (retrieved information)

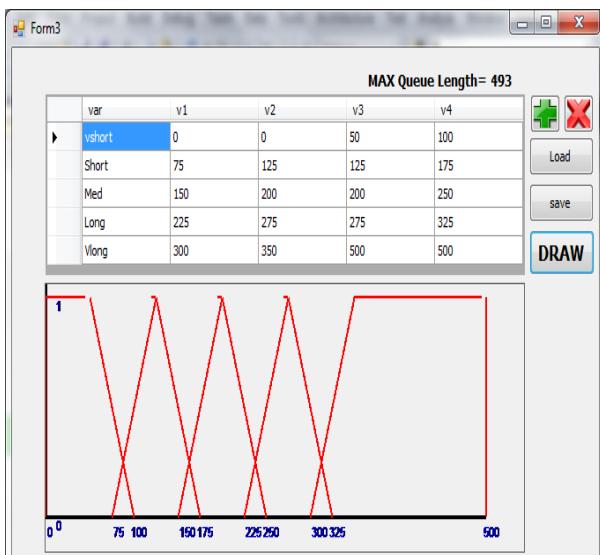


Figure 11 : AFC membership functions edit/Tune

VII. CASE STUDY AND RESULTS

A.

Case Study Description

The first requirement for starting the simulation for study case is the traffic network(intersection). Returning to section 5.1.1, the network will describe the roads and nodes for simulation case. Fig. 12 shows the study case traffic intersection network. The intersection contains four approaches and each approach contains six lanes (Three reaching the intersection and three leaving the intersection). Each lane contains two inductive loop detectors one at the head of lane queue and one at the upstream of lane , which are responsible for reading lane queue status and sending information to AFC program.

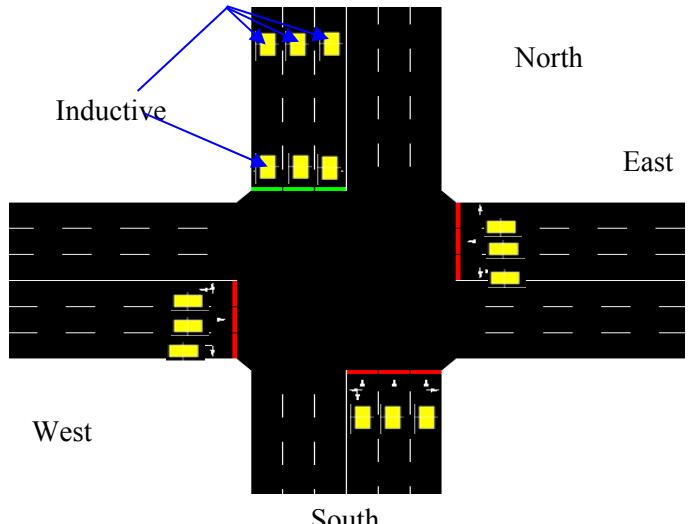


Figure 12. Case Study Traffic Light Intersection

It is usually easy to identify by observing the lengths of queues at the intersection . Sensors should be installed in multiple lanes at locations where the lane 's volume changes with the time of the day, Traffic volumes should be measured on each lane of an intersection approach. Average waiting time per cycle needs to be computed for each lane and sent to AFC as input parameters. A timer starts when a vehicle enters the detection zone of the queue sensor and resets to zero when the vehicle exits the zone of detection. If the system counts a predetermined number of seconds, the queue of vehicles waiting at the red signal lane extends upstream to the queue sensor, a vehicle will be located over the loop longer than the selected delay time. The inductive loop must be long enough to span the distance between standing vehicles. Concomitantly, it must be shorter than the shortest gap in moving traffic so that the breaks between moving vehicles will cause the delay timer to reset. So the distance between the first inductive loop and the second depends on case study traffic properties and behavior.

All data retrieved from SUMO simulation are saved to a database designed for AFC program. The database will ease the work with data to retrieve the specific information and summarize the information to be useful for Fuzzy engine. Because the SUMO is a Microscopic traffic flow simulation, it retrieves information about each car. So, AFC must converts this information to macroscopic parameters(like Volume). Algorithm 6 explains the work of AFC with Database to retrieve the important parameters.

Algorithm 6: AFC DATA MANIPULATION

Input: data record(retrieved by Traci command).

Output: average waiting time.

Begin

Step 1: **For** each vehicle in Red signal lanes **Do**

Vehicle.wait_time= Now -

Vehicle.arrival

Wait=Wait+Vehicle.wait_time.

Step 2: **For** each vehicle in Green signal lanes **Do**

Vehicle.wait_time= Vehicle.departure -

Vehicle.arrival

Wait=Wait+Vehicle.wait_time.

Step 3: Avarage waiting time= wait/vehicle
number

End

B. Demand Generation

The second step to make simulation work is to create a demand. So, the AFC program can create any demand by describing the volume of a given time interval for each intersection direction . All demands will be created before simulation starts and saved to xml routes file. The demand generation program will generate cars and generates routes for those cars.

C. Simulation Running

As soon as the demand file is created, traffic light simulation can start. Firstly TLS program is fixed-time for the first cycle only. The starting phases time is setup by GUI form window in Fig. 13 which enables the user to setup the times for first simulation phase. And then AFC will generate the times for all simulation phases.

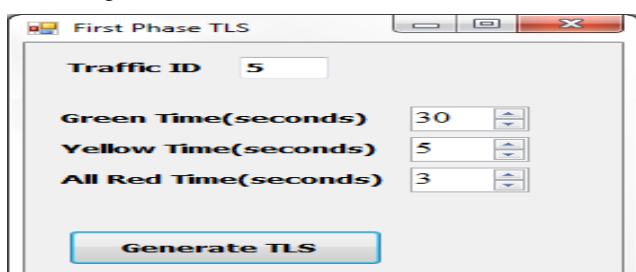


Figure 13. First Phase TLS Times.

D. Reading Variables

Two variables will be used in case study, namely QL and AR, SQL statement will be used to summarize the retrieved information from SUMO for each direction approach. All retrieved information will be stored to DataGridView control, then it can be manipulate as data RecordSet to select the QL and AR variables.

E.

Creating Linguistic Variables and Ranges

Now it is time to specify the ranges of case study linguistic variables. Noticing that QL has five linguistic values (VShort, Short, Medium, Long and VLong. AR variable also has five ranges linguistic values(VSmall, Small, Med, Large and VLarge). Table VII Explains the linguistic variables and their ranges. In practice, all linguistic variables, linguistic values and their ranges are usually chosen by the domain expert.

Table VII: Input Linguistic Variables and Ranges

Linguistic variable	Linguistic value	Ranges	
		From	To
QL	VShort	0	100
	Short	75	175
	Medium	150	250
	Long	225	325
	VLong	300	500
AR	VSmall	0	20
	Small	10	40
	Med	30	60
	Large	50	80
	VLarge	70	100

F.

Determining Fuzzy Sets

Fuzzy sets can have a variety of shapes. However, a triangle or a trapezoid can often provide an adequate representation of the expert knowledge, and at the same time significantly simplifies the process of computation. Fig.14 and 15 show the fuzzy sets for QL and AR variables used in the case study respectively. As noticed, one of the key points here is to maintain sufficient overlap in adjacent fuzzy sets for the fuzzy system to respond smoothly.

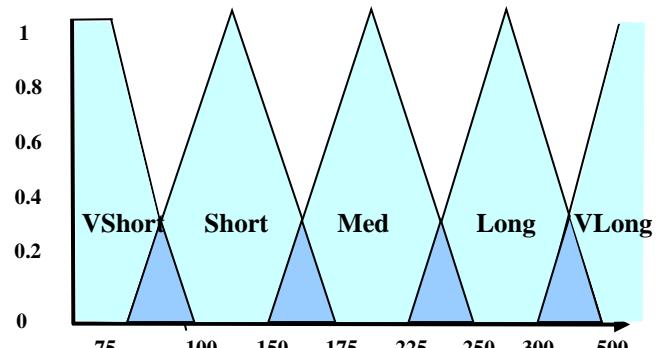


Figure 14. QL Fuzzy Sets

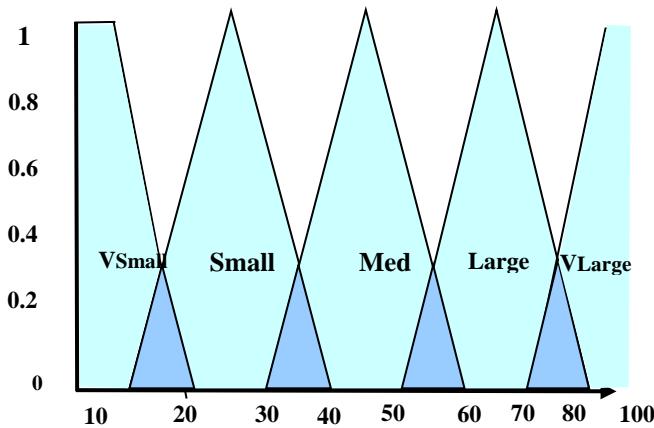


Figure 15 : AR Fuzzy Sets

G. Constructing Fuzzy Rules

The next step in the case study is to obtain fuzzy rules. To accomplish this task, the user might ask the expert to describe how the problem can be solved using the fuzzy linguistic variables defined previously. Required knowledge also can be collected from other sources such as Manuals and books. The two input variable fuzzy sets may enable us to derive 25 rules that represent complex relationships between two variables used in AFC. Table VIII contains these rules.

Table XIII: Fuzzy Rules Matrix

QL AR \ QL	VShort	Short	Medium	Long	VLong
VSmall	VSHORT	VSHORT	SHORT	MED	LONG
Small	VSHORT	SHORT	MED	LONG	VLONG
Med	SHORT	SHORT	MED	LONG	VLONG
Large	SHORT	SHORT	MED	LONG	VLONG
VLarge	MED	MED	LONG	VLONG	VLONG

There are two inputs and one output variable in the case study. It is often convenient to represent fuzzy rules in a matrix form. A two-by-one system (two inputs and one output) is depicted as an $M \times N$ matrix of input variables. The linguistic values of one input variable form the horizontal axis and the linguistic values of the other input variable form the vertical axis. At the intersection of a row and a column lies the linguistic value of the output variable. From table VIII it is clear that the output linguistic variable has fuzzy sets(VSHORT, SHORT, MED, LONG and VLONG) and fig. 16 shows the GT fuzzy sets. Table IX explains the GT output Linguistic Variable and its Ranges.

Table IX : GT Linguistic Variable and Ranges

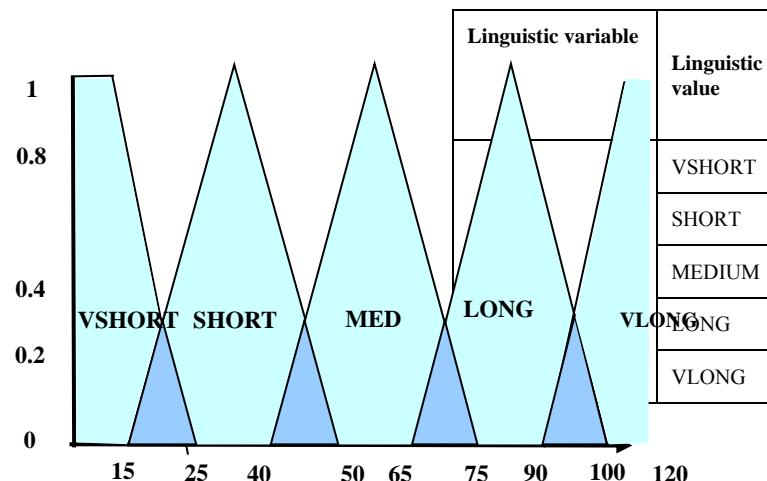


Figure16: GT Fuzzy Sets

H. First Phase Optimization

After all variables are read , linguistic variables are created, fuzzy sets and ranges are setup, simulation will begin with first cycle and before the cycle ends, the AFC will read simulation lane parameters and begin optimization.

The first variable to read is QL. AFC reads variable at simulation step 130 and converts it to linguistic instance. Fig. 17 shows the fuzzification of QL value=154 and its corresponding values in membership functions.

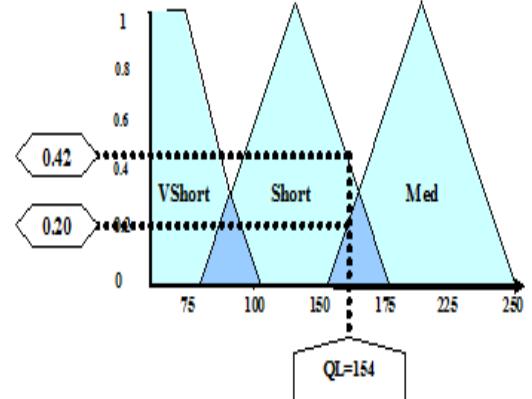


Figure 17 QL Fuzzification.

At the same simulation step 130 ,AR variable will be read and fuzzified by AFC. Fig. 18 shows AR variable value=22 and its corresponding value in membership functions.

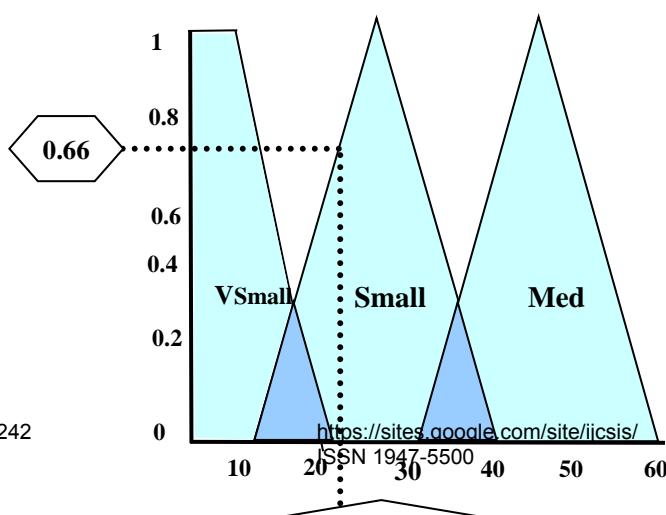


Figure 18: AR Fuzzification

After the fuzzification process for two input variables, rule evaluation process begins by AFC depending on previously built fuzzy rules. Fig. 19 explain that the two input values will belong to two fuzzy rules:

- 1) IF QL IS Short AND AR IS Small THEN GT IS SHORT
 - 2) IF QL IS MED AND AR IS Small THEN GT IS MED
- Each fuzzy rule will be evaluated separately by AFC, Fig. 19 shows the operation of rule evaluation for fuzzy rule1(19.a) and fuzzy rule2(19.b).

After the rules evaluation process done in fig. 19, aggregation process is needed. Aggregation is the process of unification of the outputs of all rules. In other words, membership functions of all rule consequents will be taken and clipped them into a single fuzzy set. Thus, the input of the aggregation process is the list of clipped consequent membership functions, and the output is one fuzzy set for each output variable. Fig.20 shows how the output of each rule is aggregated into a single fuzzy set for the overall fuzzy output.

The last step in the fuzzy inference process is defuzzification. Fuzziness helps us to evaluate the rules, but the final output of a fuzzy system has to be a crisp number. The input for the defuzzification process is the aggregate output fuzzy set and the output is a single number. There are several defuzzification methods, but probably the most popular one is the centroid technique. It finds the point where a vertical line would slice the aggregate set into two equal masses. In a computerized program, the COG is calculated over a continuum of points in the aggregate output membership function and this calculation may be slow for real time adaptive systems, but to speed up the process, a reasonable estimate can be obtained by calculating it over a sample of points. Fig. 21 shows the Defuzzifying of GT variable fuzzy set by a sample of points. For GT variable fuzzy set sample of points in fig. 21. The calculated COG value is

$$\text{COG} = \frac{(25+30+35+40+45) * 0.42 + (50+55+60+65+70)*0.20}{(0.42 * 5 + 0.20 * 5)}$$

$$\text{COG} \approx 43$$

Thus, the result of defuzzification, crisp output GT, is 43. It means the next phase Green Time for current approach will be changed from 30 to 43 seconds. The retrieved crisp variables and defuzzification process crisp values for current phase optimization can be monitored by users using GUI special form shown in Fig. 22. Noticing that GT value =38 retrieved by AFC differs from GT value=43 calculated in

example (fig. 21). That is because COG value retrieved by AFC is calculated for all points in GT output fuzzy sets. So it is more accurate. All the optimization operations explained for first phase will be repeated for all next phases for all approaches until simulation end time

I. Demand Flows

In order to evaluate the effectiveness of the fuzzy logic system, the case study carried out two types of flow, namely

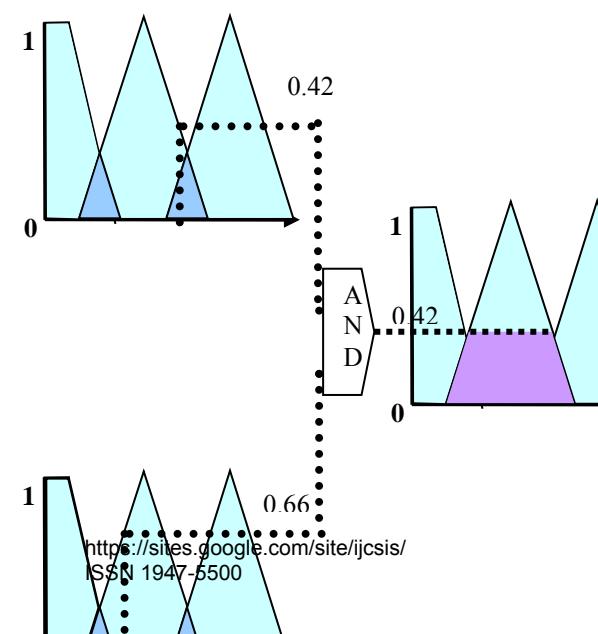
- case 1 (A,B,C,D) traffic flow (vph) is steady for all directions
- case 2 (A,B,C,D) traffic flow (vph) differs for each direction

CASE 1

A simulation run is made for 60 min periods with different traffic flow (vph) for each case (A,B,C,D) to produce the output average delay of vehicles. The results for case 1 show that generally the proposed fuzzy logic system and the fixed time controller produce little difference (best rate Case 1-C =1.7%) in results. See table X that shows the simulation results for case 1.

Table X: Case 1 Results

Case	Average Delay (sec)		IMPROVEMENT (%)
	FIXED TIME SYSTEM	FUZZY LOGIC SYSTEM	
Case 1-A 1500 vehs for each direction (N, E, S, W)	30.8	30.3	1.6
Case 1-B 1200 vehs for each direction (N, E, S, W)	27.3	26.9	1.5
Case 1-C 1000 vehs for each direction (N, E, S, W)	17.8	17.5	1.7
Case 1-D 500 vehs for each direction (N, E, S, W)	12.9	12.7	1.6



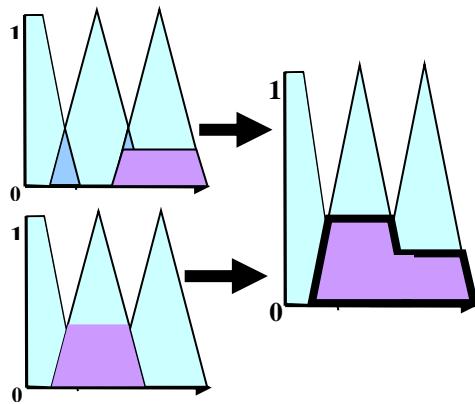


Figure 20: Aggregation of the rule outputs

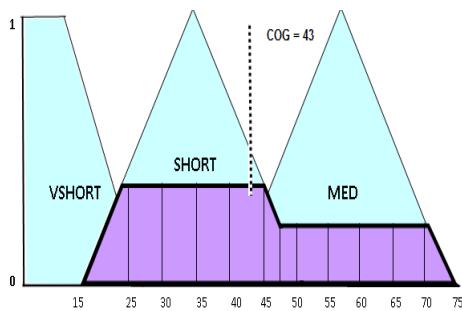


Figure 21: Defuzzifying of GT by a sample of points

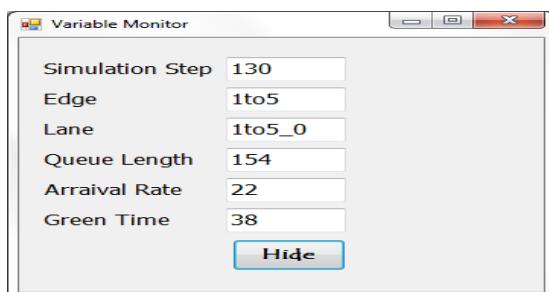


Figure 22: Variables Monitor GUI.

Figure 23 gives a graphical representation of the average waiting time of the cars, proposed fuzzy logic system and the fixed time controller produce little difference results.

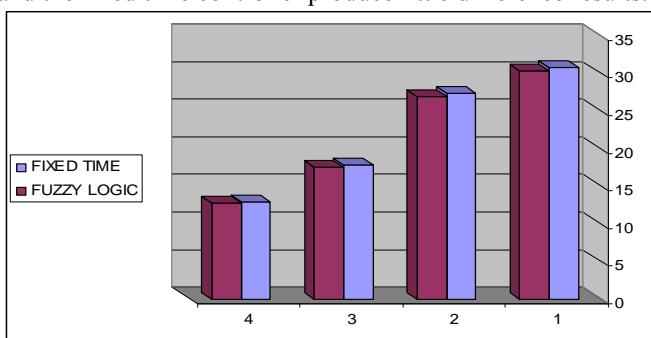


Figure 23: Performance Chart Case 1 (Waiting Time).

CASE 2

A simulation run is made for 60 min periods with different traffic flow (vph) for each case (A,B,C,D) to produce the output average delay of vehicles. This case has unbalanced traffic for each direction. Some times one direction has a heavy traffic and another has a light traffic. The results for case 2 indicate that the proposed fuzzy logic system performs much better (best rate Case 2-A =20.04 %) than the fixed time controller. See table XI which shows the simulation report for case two. Figure 24 gives a graphical representation of the average waiting time of the cars, proposed fuzzy logic system performs much better than the fixed time controller.

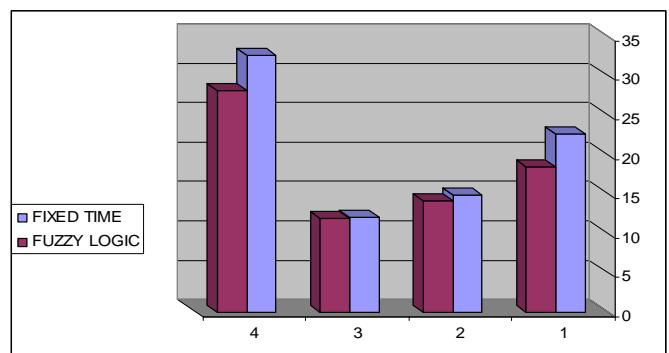


Figure 24: Performance Chart Case 2 (Waiting Time).

For Case 2 , over all time reduction can be calculated by multiplying average waiting time of one vehicle by the number of cars per hour, then it can be supposed that each 1 hour idle car consumes as average 2.5 liter of petrol [7], and each liter of petrol contains 2640 grams of CO₂[7]. Table XII shows the amount of reductions in Time, Fuel and CO₂ .

Table XII: Case 2 time, fuel and CO₂ reduction results.

Case	Average Delay (sec)		Time reduction (seconds)	Fuel amount (liter)	CO ₂ kg
	FIXED TIME SYSTEM	FUZZY LOGIC SYSTEM			
Case 2-A N=1000,E=2000, S=1500,W=1000	22.5	18.4	22550	15.65	42.3
Case 2-B N=500,E=1000, S=750,W=500	14.8	14.1	1925	/	/
Case 2-C N=300,E=500, S=700,W=400	12.0	11.8	380	/	/
Case 2-D N=1500,E=1000, S=1200,W=700	32.5	28.1	19360	13.44	35.5

Case 2-A example:

For case 2-A, the over all reduction in time, fuel and emission reduction can be calculated for one hour:
 $22.5-18.4=4.1$ sec average waiting time reduction
 $4.1 \text{ sec} * 5500 \text{ vehicles}=22550 \text{ sec} \approx 6.26 \text{ hour}$ waiting time reduction for all 5500 car
 $6.26 \text{ h} * 2.5 \text{ liter} = 15.65 \text{ liter}$ fuel reduction
 $15.65 * 2640=41316 \text{ grams} \approx 42.3 \text{ Kg CO}_2$ reduction

For fuel reduction ,supposing there are 4 rush hours every day, so 365 will have 1460 rush hours.

1460 rush Hour * 15.65 liter per hour=22849 liter per year

22849 liter per year * 450 Iraqi Dinar =10282050 I.D. per year, The amount of money approximately 10 million I.D. only for one traffic light.

There are about 150 traffic light intersections in Baghdad only. so in simple calculation it is 1.5 Billion I.D. \approx 1.2 million dollar per year. And these numbers will be increased for big cities like Istanbul which has about 1200 traffic intersections. Finally, the problem does not concern reducing the waiting time for drivers or reducing the cost for fuel. It rather concerns with the environmental factors because reduction of fuel consumption leads to reduction of emissions which affect the environment in a great way. When fuel is burned, it releases CO₂ which is a greenhouse gas into the air and contributes to the greenhouse effect. The greenhouse effect is when these greenhouse gases(such as Co₂) trap energy from the sun ; just like in a greenhouse, and raise the temperature of the earth; thus causing glaciers to melt and ocean currents to change, and eventually resulting in the end of the planet.

7 Conclusions

The intersect between traffic control and fuzzy logic can be rewarding, by understanding the fuzzy logic strengths to improve the design of high performance traffic control systems. The conclusions which have been accessed from AFC are Fuzzy system is suitable for traffic control for two major reasons

- fuzzy logic is well suited for controlling a process or system that is too nonlinear or too poorly understood to use conventional control designs.
- fuzzy logic allows control technicians to implement control tactics used by human operator. Human operators formulate their control tactics based on imprecise information described in linguistic terms.

No processing of quantitative information is involved.

The performance of AFC is affected by the configuration of the membership functions of input/output variables and the rule base., Reducing waiting time between 2% to 20% has the following benefits, as it, increases throughput on the network, reduce dangerous vehicle emissions, which affect human health and environment, and reduce fuel consumption which affects the improving economy.

Open source - cost free – projects (like SUMO) are becoming more and more popular because they give their users the right to use, study and modify the program without any restriction or cost. **At last** Using SUMO reduces the efforts, time and cost that spent by researchers to develop a traffic simulation environment.

The visions about the future works As obviously, this paper are focuses on Fuzzy Logic only, for a future proposal to design a hybrid system that mixes between Fuzzy Logic and other common artificial techniques(like Neuro-fuzzy) to obtain the optimization, or making a comparison between these Fuzzy Logic and other artificial techniques

References

1. Alper Aksaç · Erkam Uzun · Tansel Özyer,A real time traffic simulator utilizing an adaptive fuzzy inference mechanism by tuning fuzzy parameters, Springer Science+Business Media, LLC 2011.
2. C. P. Pappis, and E. H. Mamdani. A Fuzzy Logic Controller for a Traffic Junction. IEEE Transactions on Systems, Man, and Cybernetics, 1977.
3. Centre for Applied Informatics (ZAIK) and the Institute of Transport Research at the German Aerospace Centre: Simulation of urban mobility sumo website. Available at <http://sumo.sourceforge.net/>, 2009.
4. Choi, W., Yoon, H., Kim, K., Chung I., Lee S., A traffic light controlling FLC considering the traffic congestion. In Pal, N. and Sugeno, M., editors, Advances in Soft Computing — AFSS 2002, International Conference on Fuzzy Systems 2002 ,pages 69–75.
5. G. Kotusevski and K.A. Hawick, A Review of Traffic Simulation Software, Computer Science, Institute of Information and Mathematical Sciences, Massey University, Albany, NS 102-904, Auckland, New Zealand 2009.
6. Hoogendoorn S, Hoogendoorn-Lanser S, Schuurman H. Fuzzy perspectives in traffic engineering, Workshop on Intelligent Traffic Management Models, Delft, 1999.
7. Information Guide No.2 "idle reduction" ,United State Environmental Protection Agency (EPA), 2010.
8. KIM Jong-wan. A fuzzy logic control simulator for adaptive traffic management. FUZZ-IEEE Proceedings, 1997(3), pp.1519-1524.
9. Lawrence A Klein, Sensor Technologies and Data Requirements for ITS, ISBN 158053077X, Artech House Publisher, Boston, London, Jan 1, 2001.
10. Lee, J. H., LEE, K. M. AND LEEKWANG, H. , Fuzzy controller for intersection group. Int. IEEE/IAS Conference on Industrial Automation and Control, Taipei, Taiwan 1995. pp. 376-382.
11. Lee, J., Lee, K., Seong, K., Kim, C., and Lee-Kwang, H. , Traffic control of intersection group based on fuzzy logic. In Proceedings of the 6th International Fuzzy Systems Association World Congress 1995 , pages 465–468.

12. Levinson, D. , The value of advanced traveler information systems for route choice. *Transportation Research Part C: Emerging Technologies* 2003.
13. Liu Zhiyong, Zhu Jin, Li Ziupin, Yin Zhengqi; A Multi-phase Fuzzy Control Method Used for Single Intersection. *Information and Control*, 1999,28(6): pp. 453-458.
14. LIU Zhiyong, WU JINPEI, LI XIUPING; Hierarchical Fuzzy Control for Urban Traffic Trunk Roads. *Journal of Highway and Transportation Research and Development*, 1997, 14(3): pp.17-23.
15. McTrans Moving Technology: Thesis: Traffic software integrated system website. Available at <http://mctrans.ce.u.edu/featured/tsis/>, 2009.
16. Md. Shabiul Islam, Bhuyan M. S., Azim M. A., Teng L. K., Othman M. ; Hardware Implementation of Traffic Controller using Fuzzy Expert System, International Symposium on Evolving Fuzzy Systems, September, 2006.
17. Mladen Antunović, Hrvoje Glavaš, FUZZY LOGIC APPROACH FOR TRAFFIC SIGNALS CONTROL OF AN ISOLATED INTERSECTION, Faculty of Electrical Engineering Osijek 2005.
18. Mohamed B. Trabia, et al. A Two-stage Fuzzy Logic Controller for Traffic Signals. *Transportation Research Part C, USA*, 1999(7), pp. 353-367.
19. Nicholas J. Garber,Lester A. Hoel, *Traffic and Highway Engineering FOURTH EDITION* 2009.
20. Niittymäki J., Fuzzy Traffic Signal Control: Principles and Applications, Ph.D thesis, Helsinki University of Technology, Finland, 2002.
21. NIITTYMAKI, J. AND PURSULA, M., Signal control using fuzzy logic. *Fuzzy Sets and System* 2000. 116, pp. 11-22.
22. Quadstone Paramics: Quadstone paramics website. Available at <http://www.paramics-online.com/>, 2009.
23. Sayers T M, Bell M G H, Mieden T, et al. Improving the traffic responsiveness of signal controllers using fuzzy logic. *IEE Colloquium on Urban Congestion Management*, 1995.
24. Sayers T M, Bell M G H, Mieden T, et al. Traffic responsive signal control using fuzzy logic—a practical modular approach.. In: Proceedings of the 4th European Congress on Intelligent Techniques and Soft Computing, 1996, 2159–2163.
25. T. K. Ho. Fuzzy Logic Traffic Control at a Road Junction with Time-Varying Flow Rates. *IEE Electronic Letters*,1996, 17(32): pp. 1625-1626.
26. The Manual on Uniform Traffic Control Devices (MUTCD), U.S. Department of Transportation, Federal Highway Administration, 2000.
27. Traffic Control Systems Handbook, Office of Transportation Management, Federal Highway Administration, 2005.
28. Traffic Signal Timing Manual, U.S. Department of Transportation, Federal Highway Administration, 2008.
29. Trafficware: Trafficware website. Available at <http://www.trafficware.com/>, 2009.
30. Treiber, M.: Microsimulation of road traffic applet. Available at <http://www.traffic-simulation.de/>, 2009.
31. TSS - Traffic Simulation Systems: Aimsun website. Available at <http://www.aimsun.com/site/>, 2009.
32. Xu Dongling, et al. A Fuzzy Controller of Traffic Systems and Its Neural Network Implementation. *Information and Control*, 1992, 21(2): pp. 74-78.
33. Xu Dongling, et al. A Method for Real Time Traffic Fuzzy Control of a Single Intersection. *Information and Control*, 1997, 26(3): pp. 227-233.
34. Xu Jianmin, et al. A New Fuzzy Control Method for Isolated Intersection Traffic Management. *Journal of South China University of Technology (Natural Science)*, 2000.
35. Ying Bai, Hanqi Zhuang and Dali Wang, Advanced fuzzy logic technologies in industrial applications. - (Advances in industrial control), Springer-Verlag London Limited 2006.
36. Zade And Dandekar, Simulation of Adaptive Traffic Signal Controller in MATLAB Simulink Based On Fuzzy Inference System, *International Journal of Computer Applications*, National Conference on Innovative Paradigms in Engineering & Technology NCIPET-2012.
37. Shao Chun,"Adaptive Control Strategy For Isolated Intersection And Traffic Network", University of Akron, May, 2009.
38. Wiering Marco, Jelle van Veen, Jilles Vreeken, Arne Koopman, Intelligent Traffic Light Control, April 2003.
39. Taha M., Ibrahim L., Traffic Simulation System Based on Fuzy Logic, Procedia Computer Science, Complex Adaptive System Pupliciation , Conference Organied by Missouri University of Science and Technology, 2012.
40. Taha M, Traffic Traffic Simulation System Based on Adaptive Fuzzy control, PhD Thesis University of Mosul, College of Computer Sciences and Math. , 2013.
41. Michael S.,Randy M.I, Development of a Phase-by-Phase, Arrival-Based, Delay-Optimized Adaptive Traffic Signal Control Methodology with Metaheuristic Search, University of Texas at Austin,2006.
42. Traffic Signal Timing Manual, U.S. Department of Transportation, Federal Highway Administration, 2008.

A Secure Cooperative Intrusion Detection System for Mobile Ad-Hoc Network

Himanshu Kumar

M.Tech(I.T.)

Department of Information Technology,
SRM University Kattankulathur Chennai

J. Godwin Ponsam

Asst.Professor

Department of Information Technology,
SRM University Kattankulathur Chennai

Abstract: The Mobile Ad-Hoc Network does not have any fixed infrastructure so they rely on their neighbors to relay data packets over a network. Intrusion detection system in mobile ad-hoc network can be carried out in a distribution scenario due to absence of fixed infrastructure. This nature of MANET attracts the malicious users. Intrusion Detection System are the techniques to detect the malicious node. The objective of this project is to propose an Energy efficient system based on a cooperative IDS scheme to deal with intrusions in clustered mobile ad-hoc networks. We are analyzing the Energy Consumption of MANET by using present Protocols in terms of Packet dropping detection ratio, Mobility stability and Transmission Power Control etc.

Keywords: Ad-hoc Network, IDS, Energy Consumption, MANET, Wireless Network;

I. INTRODUCTION

A Mobile ad-hoc network is an important classification of networks which facilitates communication support in critical scenarios including battlefield and tactical missions, search and rescue operation. MANET can be defined as dynamic peer to peer that consist of a collection of mobile nodes. The nodes employ multi-hop information transfer without requiring an efficient infrastructure due to their dynamic and cooperative nature. Intrusion Detection has a long history of research in wired network defense but it is still in the area of mobile ad hoc networks. Security in MANET is a main and important element for the basic functions of a network such as routing, packet forwarding, and network management, network operation can be at risk because of the nature of networks. In mobile ad-hoc network the basic functions are done by every participant node in the network, unlike that use special node to support the basic functions this difference causes many important problems of the security, which are specific to this type of networks. Dynamic configurability adds flexibility to MANET but it makes it vulnerable to attack like DOS attack, Grayhole attack, Wormhole attack, Blackhole attack and IP Spoofing Attacks. Ad-hoc networks are more vulnerable due to nasty neighbor relaying packets.

MANET is basically more popular in sensor application, military operations etc. A Fixed and dedicated link among

the nodes makes a strong and less vulnerable to the network. So an effective Intrusion detection needs a cooperative scheme for severe security to the network.

II. RELATED WORK

In this section we would be discussing some of the research work carried out about IDS in clustered MANETS which are given below.

A.Routing Protocol in MANETS

In previous related research, Routing in mobile ad-hoc networks are broadly classified into two major categories which are as following:

1. Proactive routing Protocol
2. Reactive routing Protocol

Proactive Routing Protocol- Proactive routing table is known as table driven routing protocol. Routing information of each node in the network before it is needed. Nodes can get the knowledge by exchanging nodes information over the network. These are: DSDV and WRP. [10]

Another protocol is Reactive Routing Protocol which is also known as On Demand Routing Protocol in which routing table do not maintain routing table in advance, it collected only when it is required. DSRP and AODV are Reactive routing protocols.

B. Packet Dropping nodes in MANET

Ad-hoc network is vulnerable to various attacks due to its functionality and deployment scenario. It is a network which is decentralized therefore, all the routing activities are handled by nodes. Nodes may misbehave in the network and can drop the packets instead of forwarding them. [4]

Several defending mechanisms have been proposed to detect misbehaving nodes in Ad-Hoc network. On the basis of their functionality these are classified into following: Reputation

based techniques, Acknowledgement based techniques, and Credit based techniques and Intrusion detection systems.

C. Attacks in MANET routing Protocol

Mobile ad-hoc networks are basically vulnerable to two different types of attacks: Active attack and Passive attack. [11] In Active attack, aim of malicious node is to damage other node by causing network outage. It can be internal and external attack. In passive attack, the aim of selfish node is to save their battery life for this own use. These attacks are classified as Modification, Fabrication and lack of cooperation.

D. Cooperative Intrusion detection scheme.

A cooperative scheme uses clustering technique and Back Propagation Network (BPN). The benefits of a clustering architecture are scalability and fault tolerance. Also, it benefits from back-Propagation neural networks in anomaly and intrusion detection. In this system, the response is divided into two types: local response and total partial response. [1] In local response when the intrusion detection system detects a malicious node, it will write the malicious node id in the field in the hello message. When any node receives the hello message, it omits the malicious node from its routing table to isolate it. Then, the hello message updates the route itself. In total response, there is one node that applies intrusions detection system, and when it finds a malicious node, it will tell them. Simulation results clarify the effectiveness of the proposed scheme.

Another scheme proposed by H. Deng, clustered IDS architecture in which only the CHs carry out intrusion detection. It focuses on detecting routing infrastructure of a network and forms clusters using the Distributed efficiency clustering approach protocol. [2]

Yi-an-Huang and Wenke Lee have proposed a cooperative Intrusion Detection Scheme architecture that focuses on run-time resource constraint problem using a clustered based detection scheme where periodically a node is elected as the ID agent of a cluster. [5] In order to address the run-time resource constraint problem, they proposed a clustered based detection scheme. They found in there result that MANET mobility is low, CPU utilization is by up to 29% while maintaining the same level of detection performance.

III. IDS ARCHITECHTURE

The proposed IDS architecture is organized into clustered in which specific nodes act as Cluster Head (CHs) gathering local audit data from its Cluster Member (CMs), analyze them and extracting conclusions about the integrity of the nodes in the cluster. The autonomous clusters-based cooperative formed using the Mobility and Energy Aware Clustering Algorithm (MEACA) algorithm. Another issue is that a malicious node or set of nodes may be elected as CHs hindering or misleading intrusion detection which can be applied in topology of network which changes dynamically. It also considers the mobility and energy of nodes in the cluster formation in order to improve detection accuracy and reduce energy consumption. [8]

Moreover, the distribution of the detection load is based on the remaining energy of each node. In this way, the proposed cooperative IDS balance the energy consumption in a fair and efficient manner.

IV. MEACA Algorithm Implementation

The Mobility and Energy aware Clustering Algorithm works in a distributed manner.. The nodes in the network have several priorities to become cluster head. They exchange their priority values to determine who will become the heads and who will become the members MEACA algorithm satisfies these requirements. [5]

Every node becomes either a cluster head or can be a cluster member. This is true because every node can always locate a node in its neighborhood to be its cluster head. Every node is associated with one and only one cluster. A node chooses its cluster head as follows. First, it sorts the nodes in its neighborhood table from the highest Am to the lowest Am, including itself. Highest Am denoted as max(Am). Second, the node determines a mobility threshold $A^* = \max(A_m)$, where $A \in (0,1)$ Nodes uses mobility threshold eliminate the unstable nodes of which the Am's are lower than Am. Third, in the remaining nodes, the node selects the one with the highest Ae to be its cluster head.

A. Energy Consumption in MANET

Whenever packets are transmitted through intermediate nodes, its energy is consumed everytime. Energy consumption in mobile ad-hoc network can be calculated by mainly in three different ways-

1. Packet Sending
2. Packet Receiving
3. Idle state

We consider energy consumption in Sending mode, Receiving mode, Idle mode, and Sleep mode. We ran our simulation for different number of nodes. To study the Energy consumption and efficiency of mobile ad-hoc network researchers have focused on End to end delay, throughput packet delivery ratio etc. In our proposed work to Evaluate the performance of Energy consumption in mobile ad-hoc network, we apply Cluster based routing protocol (CBRP) to get advantage of clustering, energy efficiency and reduce the overhead of broadcasting. The proposed system takes the input parameters like: Mobility of nodes, Traffic, initial energy of the nodes, and transmission range. It generates the output in terms of the time of simulation. The packets delivered to destination, and the remaining energy of the nodes. In CBRP, during transmitting data from source to destination, if any route error occurred due to some reasons, the next node in the path may abort or move away from the transmission range of the node which is currently forwarding the packets.

B. Mobility Stability

Mobility stability in cluster is defined by the link expiration time (LET).[5]

$$LET_{ij} = [-ab + cd] + \sqrt{(a^2 + c^2)r^2 - (ad - bc)^2} / (a^2 + c^2)$$

- Where, $a = vi \cos \theta - vj \cos \theta$,

- $b = x_i - x_j, c = v_i \sin \theta - v_j \sin \theta$
- $d = y_i - y_j$
- V_i, V_j : speed of nodes.
- I and j are nodes
- θ is moving direction of nodes

C. Mobility of ad-hoc network

Mobility measure (M_v) of a ad-hoc nework = $(1/n) * \sum_{i=0}^{N-1} M_i(t)$.

Where N is the Number of nodes then

$$M_i(t) = (1/(n-1)) * \sum_{j=0}^{N-1} |d/dt(F(dij(t)))|$$

Where i and j are nodes,

$M_i(t)$ is measure of the relative movement of other nodes.

M_v represents the average amount of movement of the node in the network at time t gives measure of mobility.

$$M_v = 1/T \sum_{t=1}^T \sqrt{\{x(t) - x(t-1)\}^2 + \{y(t) - y(t-1)\}^2}$$

Where $x(t)$, $y(t)$ and (x_{t-1}, y_{t-1}) are the coordinates of the node at time t and $(t-1)$.

D. Computation of Energy

Total packet size = size of (preamble + PLCP header + MAC header + IP header + data)

$$\text{Energy Tx} = (\text{Transmitted power} * \text{packet size}) / 2 * 10^6$$

$$\text{Energy Rx} = (\text{Receiving Power} * \text{packet size}) / 2 * 10^6$$

Transmission time for single packet-

$$\text{Transmission time} = (\text{packet size} / \text{bit rate})$$

Total Energy consumption = $(E_a * t_a + E_s * t_s + E_r * t_r + E_i * t_i)$
Where,

- Ea= energy in active mode
- Es= energy in sleep mode
- Ei= energy in idle mode
- Et= energy in transmission mode

V. RESULT AND ANALYSIS

The Simulation is carried out in NS2 2.35 simulator in Ubuntu 14.04 (LINUX). The project setup consists of 20 wireless nodes which creates a mobile ad-hoc network in cluster formation. All the nodes uses AODV as a routing protocol within area of a particular transmission range. I have used a packet size of 1500 bytes and simulation is run for 320 seconds. I have used UDP traffic as underlying transport. During simulation UDP data traffic is sent in bytes/sec by the source node to destination node.

Table 1: Simulation Statistics

Statistics	Values
Channel type	Wireless channel
Protocol	AODV
Simulation time	150 sec.
Packet size	1024 bytes
Traffic rate	128 bytes
MAC layer protocol	802.11
Number of nodes	20
Traffic model	Cbr
Network interface type	Wireless
Transmission range	1000m *1000m
Queue type	Drop trail

Table 2: Energy Parameter

Parameter	Value
Initial energy	20
Idle power	0.05
Receiving power	0.0648
Transmission power	0.744



Figure 1: MANETs Forwarding and Receiving packets within Cluster

NAM is a tool with NS2 2.35 simulator. It gives a graphical representation of network which shows the packet traversing through the network. Figure 1 shows graphical representation of 20 mobile nodes whose packets sizes are 1024 bytes are forwarding and receiving in adjacency range with cooperative scheme. In Cooperative Intrusion detection system architechture, each MANET runs as a detection engine so the energy consumption highly reduce to the lifetime of a mobile node in the network.

Table 3: Energy consuption

Node No.	Idle	Sleep	Transmission	Receiving	Total Energy
9	0.181	0.000	0.376	0.125	38.51747
11	0.111	0.000	0.379	0.215	38.589268
15	0.131	0.000	0.439	0.185	38.489014
17	0.111	0.000	0.427	0.212	38.499288
19	0.111	0.000	0.426	0.213	38.499710

In table 3, Node no. 9,11,15,17 and 19 are those nodes which are active in cluster and sending packets between Source to Destination through cluster Head while packet dropping also occurs. Other nodes in the network also consume their Energy on the basis of their stability of cluster. These Energies are identically minimum then the other ids schemes like stand-alone and hierarchical.



Figure 2: MANETs after releasing Energies

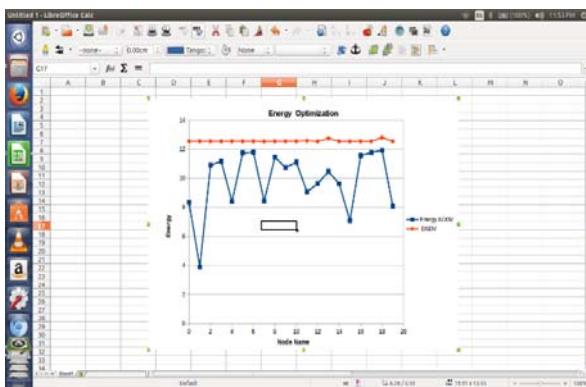


Figure 3: Energy optimization graph between AODV and DSDV

Figure 3 shows the proposed clustering algorithm reduces the Energy in Mobile Ad-Hoc Network to secure a cooperative IDS. This energy optimization graph is plotted between AODV and DSDV Protocols by implementing MEACA algorithm.

VI. CONCLUSIONS

In this paper, we analyzed the energy consumption by evaluating node mobility and Energy information in Mobile Ad-hoc network. Our system maximizes the cluster stability by using MEACA algorithm which specifies the low mobility and high energy nodes to be the cluster head. It also provides the benefits to end to end communication by evaluating packet throughput and packet delay.

In the future enhancement, simulation can be performed for optimizing the energy consumption with some advanced attack by using same cooperative intrusion detection system and others sophisticated algorithm for MANETs.

REFERENCES

- [1] Hajar Al-Hujailan,Mznah Al-Rodhaan,abdullah Al-Dheelaan "A Cooperative Intrusion Detection Scheme for Clustered Mobile Ad Hoc Networks," International Conference on Information Assurance and Security(IAS).
- [2] sara CHADLI, Mohamed EMHARRAF, Mohammed SABER, Abdelhak ZIYYAT "Combination of hierarchical and cooperative models of an IDS for MANETs" InternationalConference on Signal-Image Technology & Internet Based Systems.
- [3] Christoforos Panos,Christos Xenakis and Ioannis Stavrakakis "A Novel Intrusion Detection System for MANETS" Security and Cryptography(SECRIPT), 2010 Proceedings of the 2010 International Conference,IEEE
- [4] Tharinda Nishantha VIDANAGAMA Hidenori NAKAZATO "Mobility in description based Clustered ad-hoc Network" IEEE Globecom 2010 workshop on heterogeneous, Multi-hop wireless and mobile-networks
- [5] Yi Xu and Wenye Wang "MEACA: Mobility and Energy Aware Clustering Algorithm for Constructing Stable MANETs" Military Communications Conference, 2006, MILCOM2006.IEEE
- [6] Aksai agrwal, Savita Gandhi, Nirbhay Chaubey, Naren Tada, Shrushti Trivedi "NDTAODV: Neighbor Defense Technique Ad-hoc On Demand Distance Vector to mitigate Flood attack in MANETs" International Journal of Computer Networks & Communications (IJNC) VOL6, No.1, January 2014
- [7] Said EL KAFHALI, Abdelkrim HAQIQ "Effect of Mobility and Traffic Models on the Energy Consumption in MANET Routing Protocols" International journal of soft computing and Engineering (IJSCE) ISSN 2231-2307,Volume 3, Issue-1, March 2013
- [8] Shaileendra Gupta, C.K.Nagpal and Charu Singla "Impact of Selfish node Concentration in MANETs."International Journal of Wireless &Mobile Networks (IJWMN) Vol.3, No.2 April 2011.
- [9] Zougagh Hicham,Toumanari Ahmed, Latif Rachid, and Idiouker Noureddin "Evaluating and Comparison of Intrusion in Mobile Ad-hoc Networks" International Journal of distributed and parallel system (IJDPS) Vol.3,No .2, March 2012
- [10] Sevil Sen, John A. Clark "Intrusion Detection in Mobile Ad-hoc Networks".First International Conference ADHOCNET 2009.

Ensuring Interoperability Among Heterogeneous Devices through IoT Middleware

Muhammad Ahsan, M. Ramzan Talib, M. Umer Sarwar, M. Irfan Khan, M. Bilal Sarwar

Department of Computer Science, Government College University Faisalabad, Pakistan

Abstract—Internet of Things provides truly ubiquitous and smart environment. The multilayer distributed architecture with a variety of different components together with end devices, applications and the association with its framework poses challenge. Internet of Things middleware actions as a joining link between the heterogeneous areas that communicate across heterogeneous edges. In this work, we study the interoperability issue between heterogeneous devices. We presented guidelines to handle the interoperability issue in Internet of Things. Furthermore, we have proposed architectural framework for Home Area Network.

Keywords-Interoperability, Internet of things, Middleware, Heterogeneous devices

I. INTRODUCTION

The phrase "Internet of Things" means all the things are connected to internet. Sensors can transmit data through internet. In up Internet, interoperable information and communication, based on (physical and virtual) by interconnecting things enable advanced services to the global infrastructure of the information society, the physical world object (physical goods) or identification and communication networks which are capable of being included in the information world (virtual goods). Current information technology, networking and services in real-world data integration technology and solutions that enable most things (IOT) of the Internet under the umbrella term has been defined. Such wide and embedded devices, and RFID technology as sensor data collection technology development, and continuously connected to the network with which the data are transferred lead to a number of smart devices. The number of Internet-connected devices such as data collection and processing, mining and processing of the data leads to extraordinary challenges since 2008, the number of humans on the planet is estimated that prevails [1].

Each item can be identified through a computing device embedded in a unique, work together in the existing Internet infrastructure. Experts, many have been estimated to be comprised of nearly 50 million of the building in 2020. Communication Technology) industry to deal with problems common IOT archieved that the interoperability information. In this paper we illustrate the application domain of the reference IOT and cloud computing, compatibility review of the latest trends and challenges and future Internet design information on how semantic technology can support interoperability, open service infrastructure, and information model. The Internet of Things (IoT) is a novel paradigm that is

rapidly gaining ground in the scenario of modern wireless telecommunications. The basic idea of this concept is the pervasive presence around us of a variety of things— such as Radio-Frequency Identification (RFID) tags, sensors, actuators, mobile phones, etc. which, through unique addressing schemes, are able to interact with each other and cooperate with their neighbors to reach common goals [2].

In accordance with Pike Study a smart location could be the integration regarding technological innovation right strategic method of durability, citizen well-being, and also monetary progress. For that reason, practical clever location designs has to be multi-dimensional, encompassing different factors regarding smartness and also stressing the importance regarding integration and also interaction around multiple names. Remedies are urgently needed, and also easily progressing technologies may just be the response. In fact, computer science alternatives and also technologies possess the prospective, to impact most areas of location ecosystems, coming from atmosphere (waste operations, travelling, governance regarding organic assets and also generation regarding energy) to interpersonal (safety, city planning, housing) integration [3].

MIT Auto-ID Lab IOT (RFID) and networks of wireless sensor using a dedicated IOT Massachusetts Institute of Technology (MIT), 1999 came from the Auto-ID Center. Person-object and object-to-object communication IOT thus the connection of sensors, actuators and other smart technologies basis. A new dimension of information and communication technologies (ICT) have been added to the world no one can access information anywhere, ubiquitously and pervasively, at any time on any device. IOT to multiply and form a network to connect to a whole new dynamic network, will be made [4]. By simply allowing availability regarding, along with interaction using, a diverse number of physical devices or things like, kitchen appliances, surveillance cameras, supervising detectors, actuators, demonstrates, motor vehicles, machines and so forth, the IoT will certainly create the progress regarding applications in lots of various areas, like property automation, commercial automation, healthcare supports, mobile health, aged assistance, wise electricity managing along with clever grids, motor vehicle, traffic managing, and several some others [5].

Most of these applications will certainly use the possibly substantial volume along with number of data produced

by simply this kind of objects to produce brand-new products and services to help people, organizations, along with open administrations [6] and [7]. Extensible Internet Things (IOT) refers to something ("object"), and a discussion of the virtual representation of the object. IOT things on the Internet and among other things that they "talk" to connect the power and features of their "services" to expose to determine how to communicate with other devices. Electronic devices connected to the Internet using the Internet of Things are not related; this is a "smart" web-enabled in order to exchange information. IOT In other words, using the Internet as a medium of communication and exchange of information in the physical world into the virtual world of work.

WSNs, RFID, M2M sales and marketing communications, as well as SCADA tend to be this a number of necessary components (Figure 2) involving IoT. A completely functional IoT middleware should assimilate these kinds of systems to aid this imagined varied application areas [8], [9]. IoT devices heterogeneous and new types of communication devices that challenges together, exchange information on a number of different types of tools designed to support research efforts that could cover the framework middleware expect is from the approach of middleware pose a huge challenge to find in the future interoperability. Improve the living environment of mutual benefit. Information and communication technologies (ICT) perspective, the main idea is the idea of smart home networking devices and services to integrate the use of technology in the home in an effort to control and monitor the living room. The dome of the state dwelling on ubiquitous computing, effectually ability to discover, integrate, and coordinate a wide variety of different devices to establish communication protocols and functionality of the party.

II. RELATED WORK

Exploration in to the IoT continues to be with its first phase, along with a typical classification of the IoT just isn't but obtainable. IoT can be seen coming from several perspectives: Internet-oriented, things-oriented along with semantic oriented (knowledge) [10]. Dissertation, Internet (IOT) deployments throughout the study sustainability issues. Adjust the classic analysis of the way devices and networks to discuss and contribute to addressing issues related to the applications tab. We will discuss their experience with the two projects: "Safe to extend the awareness and dissemination of smart devices for the residents of the house in a safe, inexpensive sensors to detect earthquakes and a large network of Commdevicesy Seismic Network, network, warning us to improve the elastic intermediate device between devices [11]. Internet connected with Things, or perhaps IoT, is really a brand new wave on the Internet, helping appreciable link involving items as well as mankind nevertheless additional strong. This specific area is well known from the massive level of facts which can be generated on the RFID devices from real time. About

managing this facts, the particular IoT middleware presents time constrains relating to both equally opening programs as well as selection as well as holding facts measures. As a result, middleware scalability is really a crucial requirement for helping the actual expansion connected with IoT [12]. "The Internet allows people to things and things connected anytime and anywhere, the place with anything or anyone, actually in use in any / any network" [13]. Figure 1 Source: Cisco IBSG, April 2011

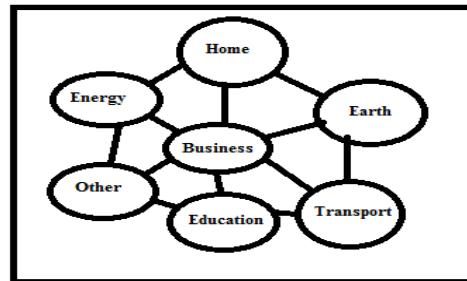


Figure1: Internet of things (IoT)

Ubiquitous research surroundings, sensor, middleware as well as service are extremely significant portion. The actual middleware must mindful sensor's data, and have absolutely to supply brilliant service to help user. Within ubiquitous research surroundings, the particular middleware receives sensor files through a variety of detectors, as well as digesting these kind of files [14]. Initial applications of the device as a theme. The major problem with hardware the same certificates or passwords stored in the device. Hardware devices are exposed to attack. (As discussed above) and a lot of damage in one or all will not be affected. To avoid this, the device can be pre-programmed with a unique identification and capacity. At the time, the development is in the process of registration. In both The complexity and cost, and may affect the ease of use. We must support the use of dynamic customers. The key to any device Cable / ID card registration in the home [15]. G-Sense is a peer-to-peer method pertaining to worldwide realizing and also checking. These methods, while better made and also scalable, never have been recently mostly acquired yet with the commdevicesy. Additionally, sensor discovery remains to be a tough issue. Additional devices focus on unique sorts of stuck devices [16]. The places forward a general middleware framework on the Internet connected with Things (IOT). This specific framework possesses dispersed, loosely bundled, scalable capabilities. To fix the problems connected with device processing connected with communications connected with IOT, the concept of ontology is actually released [17]. RFID and also Wi-Fi sensor commdevicesies were being used collectively in a very sensible home to name a caregiver exactly who penetrates your house. Some sort of ubiquitous research structured sensible home safety management pertaining to digital living seemed to be intended inside Research [18]. UPnP is a well-known technological innovation pertaining to home network and also manage. However, making UPnP-based home commdevicesies seriously isn't effortless. Tips on how to

be connected different devices on the home multilevel is a significant issue due to the fact the majority of existing devices don't have an UPnP software [19]. Which development of the lot depending on SOs lifts numerous issues concerning hw/sw device structures as well as app development device? Several solutions (e. Gary, Fed Net, UbiComp, as well as Sensible Devices) are actually thus far proposed to compliment the particular perspective of your SO-based lot structure [20].

Middleware within IoT is a quite effective research spot. Many alternatives have been suggested in addition to put in place, particularly within the past few years. These alternatives are generally very various within their design strategies (e. h., event-based, database), degree connected with development abstractions (e. h., regional or node degree, worldwide or system level), in addition to setup areas (e. h., WSNs, RFID, M2M, in addition to SCADA). On this review, the existing middleware alternatives are generally gathered for conversation according to their own design and style solutions. As Event-based, Virtual Machine-based, Database-oriented, Tuple-spaces and Service Oriented. A number of middleware work with a mix of diverse style solutions. The UBIROAD middleware [21], ubiSOAP [22] and P2P (SMEPP) [23] is an IoT middleware explicitly built to end up being secured, especially handling troubles within the peer-to-peer product.

III. METHODOLOGY

3.1 Comparison of Different Middleware's

Every one of the stated middleware's help device development and also operations. Context conscious Operation is reinforced by means of HYDRA, UBIWARE, UBIROAD and also SMEPP. Conversely, SOCRADES, SMEPP, GSN, UBIROAD and also HYDRA are generally some situations regarding middleware implementing protection and also individual privacy within their structure. Determined by device portability, syntactic image resolution, HYDRA, SMEPP and also ASPIRE are generally OSGi compliant, UBIROAD works by using CAFFEINE and also XML, UBISOAP works by using J2SE and also J2ME, GSN works by using XML and also SQL, SIRENA and also SOCRADES make use of DPWS even though SOCRADES also works by using SAP NetWeaver device and also ISMB works by using just about any CAFFEINE compliant device. Wherever by is produced making use of J2EE structure and it is integrated together with Oracle Software.

Middleware's Features	Internet of Things Middleware's				
	ASPIRE	GSN	HYDRA	SIRENA	SMEPP
Platform Portability	Yes	Yes	Yes	Yes	Yes
Interoperation	No	No	Yes	Yes	No
Security and Privacy	No	Yes	Yes	Yes	Yes
Context Awareness	No	No	Yes	No	Yes

Table1: Comparison of Different IoT Middleware

Middleware's Features	Internet of Things Middleware's				
	WHEREX	ISMB	UBISOAP	SOCRADES	UBIWARE
Platform Portability	Yes	Yes	Yes	Yes	Yes
Interoperation	Yes	No	Yes	Yes	No
Security and Privacy	No	No	No	Yes	No
Context Awareness	No	No	No	No	Yes

Table 2: Comparison of Different IoT middleware

3.2 Interface protocols of IoT middleware

IoT Middleware's have several short comings or open issues. They are available for respective domains separately.

Interface Protocols for IoT Middleware	Internet of Things Middleware's				
	ASPIRE	GSN	HYDRA	SIRENA	SMEPP
WIFI	No	Yes	Yes	No	Yes
RFID	Yes	Yes	Yes	Yes	No
SENSOR	No	Yes	Yes	Yes	Yes
BLUETOOTH	No	No	Yes	Yes	Yes
ZIGBEE	No	No	Yes	No	No

Table 3: Interface Protocols for IoT Middleware

Interface Protocols for IoT Middleware	Internet of Things Middleware's				
	WHEREX	ISMB	UBISOAP	SOCRADES	UBIWARE
WIFI	Yes	No	Yes	No	Yes
RFID	Yes	Yes	Yes	Yes	Yes
SENSOR	Yes	Yes	Yes	Yes	Yes
BLUETOOTH	Yes	No	No	No	No
ZIGBEE	Yes	No	No	No	No

Table 4: Interface Protocols for IoT Middleware

ISMB for example. Address your RFID domain. GSN handles your sensor commdevicesies on the whole. UBIWARE handles intelligent vehicular methods. There exists zero general middleware and this can be applicable over almost all probable intelligent environments-including intelligent household, intelligent auto, and intelligent city for example. Such as RFID domain, and can become tailored according to your domain specific demands. It's been witnessed with this analyze that will to end scalability troubles IPv6 can be proposed although not however fixed absolutely. Support pertaining to circumstance prognosis along with processing have not also been attained thoroughly. Support connected with semantic modelling along with controlling connected with information amounts in addition slide in the open troubles, especially controlling your crowd sourcing connected with varied domain. There exists a scope

pertaining to research perform to make some sort of general IoT-middleware program, that's applicable over almost all domains.

IV. PROPOSED MIDDLEWARE & IT's REQUIREMENTS

Smart home environment associated with the use of different systems have different systems and applications to perform a number to the next. The need to cooperate in the management of heterogeneous systems, middleware and Internet technologies Bormann, taking into account, to change from independent suppliers and open systems. Lightweight items from EB proposed a ConstrainedApplicationProtocol(COAP). This paper proposes an architecture that is based on the smart home environment, interoperability is the general trend. Figure 2 shows the structure of the proposed system.

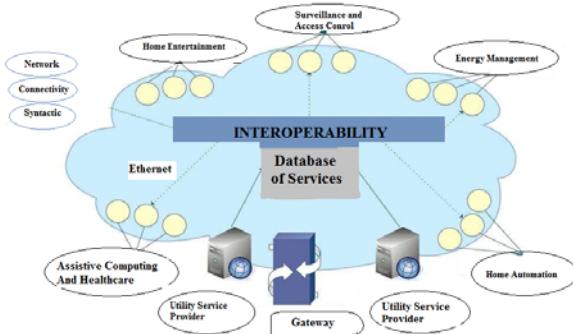


Fig 2: System Structural design

Demand system and decide on the appropriate IO consists of several layers. The middle layer between the system and the service provides a connection service is a service-based Web services. A layer represents the systems, Internet of things, building the gate and Web Service components. The main function of the gate to access the external network. Smart homes are new DI systems or limitations of the service. These restrictions specific modules known as APIs devices and device. I introduced a new dependency system. Both modules consist of pre-defined SQL statements in accordance with the structure of communication in aggressively. In adding, modules and software developers a set of application programming interfaces included in the system software on the affected IOP connected devices to connect. The modules are lots of rules to SQL. For building applications, developers only need to call your favorite statements architectural details. Smart House belonging IO heterogeneous database query messages as structure includes offensive. Request aggressive is illustrated in Figure 3. The structure of the system:

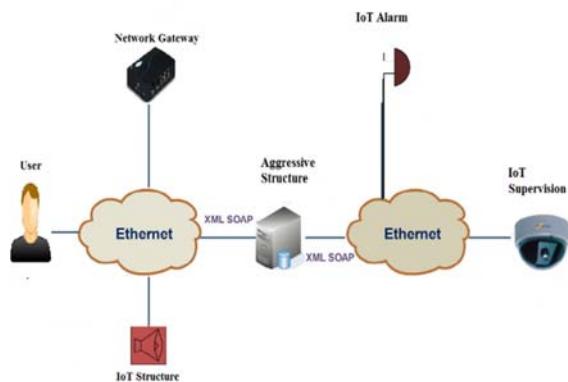


Fig 3: Structure Execution

All three systems to assess the implementation of a common understanding of IOT aggressive things (IOT monitoring equipment, audio equipment and warning devices to the Internet of Things Internet of Things), based on the structure of the Internet. Architecture allows stores intelligent building, new functions, types, and corresponding information service IOT to determine the rules that were set. Internet of Things based surveillance provided as presented in Figure 4:

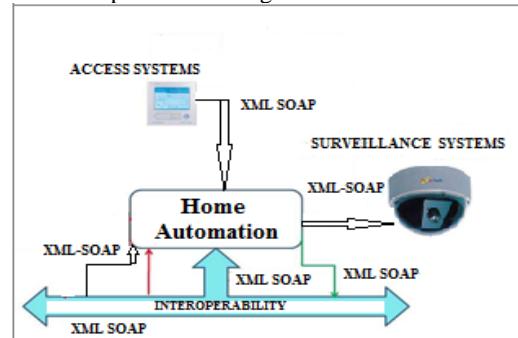


Fig 4: Interoperability of heterogeneous Devices
(Home Automation)

According to many systems and system management features, API added value ECA layers. Sorry for the installation of different systems in the service of other platforms may prove useful API that allows the easy addition of new devices. Now In this situation, Systems surveillance cameras are configured by the IO access for the installation of the door. When you set the level of proactive service completely. Architecture determines the appropriate directions established on ECA technique for interoperation to occur. The supervision structure will conjointly perform responsibilities based on the structure prominence of all devices arranged in Home automation. And you gain full access to the system and the security of the legal system in order to activate the system. Terms of text XML, to certify interoperability among smart home devices. It truly is really worth emphasizing that will virtually every techniques along with devices have the

ability to carry out with cross-event circumstances with the exception of fire alarm. Fire Alarm Systems are classified as universal connections and components in the IOT is automatically activated based on home automation systems.

V. CONCLUSION

Middleware's have numerous brief comings or maybe open problems. They can be used for specific as a separate domain. UBI-ROAD addresses workable road techniques. We have noticed, the assortment of middleware types can be found in diverse scenarios. A selection of them may be varied to attain the necessary requests. We can observe, that each categories of middleware's have a very constrained service for Platform Portability and Interoperation. Hydra, Sirena, SMEPP and wherex tackle your RFID site. Eventually, the option of the middleware is dependent upon the duty to achieve. We are investigating the plan further IOT-based middleware layer in any environment Smart. This paper covers the debate on this subject on behalf of the IOT and When defining the scope of research in the future IOT middleware. This research paper interoperability pain need to develop a home environment. In this research paper, ECA rules must be based on a design proposal for the smart home IoT interoperability. The Aggressive System offers adding of dependences each interval an Internet of things system is organized without interference. Architecture allows interoperability between its integration service systems by permitting innovative dependences to each a novel structure is added.

REFERENCE

- [1] Charu, C., Aggarwal, Naveen, A., & Amit, S. (2013). *The Internet of Things: A Survey from the Data-Centric Perspective*. Springer US, pp 383-428.
- [2] D. Giusto, A. Iera, G. Morabito, L. Atzori (Eds.) (2010), the Internet of Things, Springer, ISBN: 978-1-4419-1673.
- [3] "Smart cities. Intelligent information and communications technology infrastructure in the government, buildings, transport, and utility domains."(2011) Pike Research, Tech. Rep.,[Online].Available:<http://www.navigantresearch.com/research/smart-cities>
- [4] Michahelles, F., Uckelmann, D., & Harrison, M. (2011). *an Architectural Approach towards the Future Internet of Things*, Springer-Verlag Berlin Hidelberg.
- [5] P. Bellavista, G. Cardone, A. Corradi, and L. Foschini,(2013) "Convergence of manet and wsn in iot urban scenarios," Sensors Journal, IEEE, vol. 13, no. 10, pp. 3558–3567, Oct.
- [6] K. Paridel, E. Bainomugisha, Y. Vanrompay, Y. Berbers, and W. D. Meuter (2010), "Middleware for the internet of things, design goals and challenges," Electronic Communications of the EASST, vol. 28,
- [7] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, (2013) "Internet of Things: A vision, architectural elements, and future directions," Future Generation Computer Systems, vol. 29, no. 7, pp. 1645 – 1660,
- [8] H. Zhou, (2012) the Internet of Things in the Cloud: A Middleware Perspective, 1st ed. CRC Press, Inc.,
- [9] C. Perera, A. B. Zaslavsky, P. Christen, and D. Georgakopoulos, (2013) "Context aware computing for the internet of things: A survey," CoRR, vol. abs/1305.0982,
- [10] L. Atzori, A. Iera, and G. Morabito, (2010) "The internet of things: A survey," Computer networks, vol. 54, no. 15, pp. 2787–2805,
- [11] Kyle, Benson. (2015). *Enabling Resilience in the Internet of Things*, Seventh Annual PhD Forum on Pervasive Computing and Communications.
- [12] Gomes, M., da Costa, C.A. (2014).*Internet of things scalability: Analyzing the bottlenecks and proposing alternatives*, Ultra-Modern Telecommunications and Control Devices and Workshops (ICUMT), 2014 6th International Congress IEEE on6-8 ,Oct, 269 – 276.
- [13] P. F. Harald Sundmaeker, Patrick Guillemin and S. Woelffl'e, Vision and Challenges for Realising the Internet of Things. Publications Office of the European Union, 2010. [Online]. Available: <http://www.internet-of-things-research.eu/pdf/IoTClusterbook March 2010.pdf>
- [14] Ji Eun, K., Boulos, G., Yackovich, J., Barth, T., Beckel, C. and Mosse, D., (2012). *Seamless integration of heterogeneous devices and access control in Smart Homes*, 8th International Conference on Intelligent Environments, pp. 206–213.
- [15] FREMANTLE, P., KOPECKY, J., AND AZIZ, B. (2015) Web api management meets the internet of things. In Services and Applications over linked APIs and Data.
- [16] Alfredo J. Perez, Miguel A. Labrador, and Sean J. Barbeau. (2010). G-sense: a scalable architecture for global sensing and monitoring. IEEE Network, 24(4):57–64
- [17] Zhou, M., Fan, H., Ma, Y. (2013).*Semantic annotation method of IOT middleware* Intelligent Control and Information Processing (ICICIP), Fourth International Conference on9-11 June,IEEE 495 – 498.
- [18] Hussain, S., Schaffner, S. and Moseychuck, D.: (2009), *Applications of Wireless Sensor Networks and RFID in a Smart Home Environment*, Seventh Annual communication Networks and Services Research Conference, pp. 153–157.
- [19] Lu, Y., Fang, F., Liu, W.: (2009).*Home Networking and Control Based on UPnP*: An Implementation. In: Second Inter. Workshop on Computer Science and Engineering, WCSE. vol. 2, pp. 385–389
- [20] Giancarlo Fortino, Antonio Guerrieri, Wilma Russo., (2012). *Agent-oriented Smart Objects Development Proceedings*, IEEE 16th International Conference on Computer Supported Cooperative Work in Design.
- [21] TERIYAN, V., KAYKOVA, O., AND ZHOVTOBRYUKH, D. Ubiroad: Semantic middleware for context-aware smart road environments. In Internet and Web Applications and Services (ICIW), 2010 Fifth International Conference on (2010), IEEE, pp. 295–302.
- [22] CAPORUSCIO, M., RAVERDY, P.-G., AND ISSARNY, V. ubisoap: A service-oriented middleware for ubiquitous networking. Services Computing, IEEE Transactions on 5, 1 (2012), 86–98.
- [23] Benito, R. J. C., M'aRquez, D. G., Tron, P. P., Castro, R. R., Mart'in, N. S., and Mart'in, J. L. S. Smepp: A secure middleware for embedded p2p. Proceedings of ICT-Mobile Summit 9 (2009).

SQL Injection Attack Detection & Prevention over Cloud Services

Niharika Singh Ajay Jangra Upasana Lakhina Rajat Sharma

*Department of Computer Science and Engineering, University Institute of Engineering and Technology
Kurukshetra University, Kurukshetra, INDIA*

Abstract — Web servers which provide customer services are usually connected to highly sensitive information contained backend databases. The incrementing bar of deploying such web applications initiated in ranging the corresponding bar of number of attacks that target such applications. SQL Injection Attacks come about when data provided by external user are directly included in SQL query but is not properly validated. The paper proposes a novel detection & a prevention mechanism of SQL Injection Attacks using three-tier system. As the methodology is concerned over static, dynamic & runtime detection and prevention mechanism which also filters out the malicious queries and inspires the system to be well prepared for the secure working environment, regardless of being concerned over the database server only. The cloud proposes the services like SaaS, IaaS, PaaS, DaaS, EaaS. As previous solutions are achieved for the database queries for DaaS service only, but this paper enhances the scope of other services as well. It adapts to maintain security of the whole system even when it is for any of the cloud platforms. The solution includes detection & filtration that reduces attacks to 80% in comparison to other algorithms.

Keywords—Cloud computing; Cloud Security; Architecture, design; Cloud services; Deployment models; SQL Injections;

I. INTRODUCTION

Cloud computing is an on demand, resource pooling, self-service, multilevel virtualization that is independent and is ubiquitous network access which visualize the next generation computing. It is actually inspired by the grid, parallel and distributed computing over the internet deploying highly optimized data setters to provide the resources like hardware, software, data, and platform as required by any application. The concept evolved in 1950 by IBM known as RJE (Remote Job Entry process). In recent years, the popularity and swift growth in storage and processing technologies and computing resources have become cheaper.

Involving the third party over the internet proposes many unreliable strings which can be proved as loopholes.[11] [3] The cloud is storing a huge amount of data including personal and confidential details, thus, securing the data in the cloud tends to a major point of concern. The successes of the internet have turned more powerful, efficient, thus are pervasively available than ever before. In 2006 Amazon implemented its first cloud AWS (Amazon Web Service) [1]. It offers a new style of application program that can work as a platform which supports dynamically organized services simultaneously. To understand the concepts of the cloud computing technology a performance based efficient approach will be required for new paradigms to systematize the usually shared information and to deploy & develop the affiliated changes in different user-oriented platform models [2]. Applying the various but suitable methods for providing privacy checks to the escapes is itself a major challenge of the cloud computing. [13] Web servers which provide customer services are usually connected to highly sensitive information contained backend databases. The incrementing bar of deploying such web applications initiated in ranging the corresponding bar of number of attacks that target such applications. According to a study, it was stated that 80% of cyber-attacks are outperformed at the application layer & over the audited websites where 98% of them are clearly targeted. SQL Injection Attacks (SQLIAs) are being identified as one of the foremost security threats to the web applications. [12] It initiates a vulnerable query to destroy the connected server systems and give attackers unauthorized access to underlying databases & rights to delete, modify and retrieve valuable and confidential information stored in databases.

II. CLOUD PLATFORMS

The section describes that there are four platforms which are being designed to meet the needs and expectations of cloud computing technology [8]. Injecting the SQL queries harms the database on the client server, but it might be possible that the attack might happen in any of the following cloud types that are as follows [11].

Public cloud: Computing infrastructure is hosted by a cloud vendor on vendor premises and can be shared by various organizations. E.g. Amazon, Google, Salesforce.com, Microsoft etc.

Private cloud: The computing infrastructure of private cloud is not shared with other organizations, but rather is dedicated to a particular organization. It is more expensive but reliable in comparison to the public cloud. E.g.: HP data centers, IBM sun, Oracle, 3tera etc.

Hybrid cloud: When public & private cloud works together it is called hybrid cloud “Organizations may host critical applications on private clouds, whereas relatively less secure concern on public cloud”.

Community cloud: The cloud is shared by two or more private, public or community cloud. E.g.: Group of schools comes under specific university [8].

III. FORMATION OF CLOUD COMPUTING

This part of the paper describes the organization of the technology. In simple terms “the cloud” can be predicted as a metaphor for the internet that is quite familiar cliché, but when it is integrated to the term “computing” its meaning gets bigger & hazy. Cloud computing offers the opportunity to organizations that could simply connect to the cloud and use the available resources on a PAY PER USE basis, which avoids the company’s capital expenditure on additional of premises infrastructure resources and instantly scale up and scale down according to business requirements [3]. Cloud computing consists of cloud client, services, applications, platform, storage & infrastructure measured services. Cloud computing is the highly automated utility based paradigm shift consists of optimized and efficient framework that includes servers, virtual desktops allocates services for computer network over the internet prescribing software platform and applications for easy and agile deployment of secure data management [5].

Accessing & storing content through cloud initiates many different levels of checkpoints to get authorization. SQLIAs are the way that may harm at any of the checkpoint level including any of the XaaS (X as a service) The technology provides broad network access using resource pooling, on demand self-service with rapid elasticity, resulting in continuous high availability, interoperability and standardized scalability for the hardware and software components providing data secrecy and ease for capital investment [2] [6].

IV. MOTIVATION

Study says about SQLIAs that the queries are injected to attack databases of the client. Whether it is on the internet or if attacker attacks a cloud, the data is possessed to be affected, but if the SQLIAs are attacked to modify the configuration of any server system or to spoof a platform where one is working over a confidential work? It is always considered to get detection & prevention solutions for SQLIAs on the Daass level but one must find solutions for SaaS, PaaS, IaaS, & EaaS level. The solutions that are found are supposed to be much more effective as for the DaaS to get 70-90% of the success.

The fig-1 is depicted the insertion of SQL Injected query in the network that penetrates firewall and breakthrough the other levels of servers at the client end.

V. DEPLOYMENT MODELS & EVALUATION

Cloud computing is the type of internet-based computing, where different services such as servers, data storage modules are delivered to any organization computers and devices through the internet. The internet cloud can communicate through various devices like PC, mini note, notebook, remote desktop, remote server, database, mobile phones, etc. contains three different service layers that are software, platforms and infrastructure[1][2]. This helps the users to get better services, but it is counted as a single phase. On the other hand, attackers are ready to hack, spoof, or harm the systems that might belong to any of the following service categories. [8].

Software as a service (SaaS): It refers to an application that can be accessed from anywhere over the world as long as you have an internet connection. They have certain features like SSL encryption, a cryptographic protocol. Ex: G-mail, yahoo-mail, Google apps, MS office 365.

Platform as a service (PaaS): This service layer delivers a computing platform typically includes an operating system, programming language, etc. It is a platform for developers to write and create their own applications. For ex: AWS elastic beanstalk Google app engine, salesforce.com, windows azure, etc.

Infrastructure as a service (IaaS): It provides hardware and infrastructure to the users to rent and tariff for a limited period of time. It is also known as “Hardware as a Service”. Ex: firewalls Google computes engine, Amazon HP cloud, EC2 etc. The three layers are the basic service layers that were discovered in the early sixties and on analyzing modern research and study projects, some new service layers have been discovered that are listed out as [4].

Data as a service (DaaS): A large amount of data over the internet is stored in an unmanaged way which requires to be maintained by applying sorting algorithms and defining data allocation methods. Thus the model work over the bulk amount of data retrieval initiates the availability, security and data management leads to concurrency & efficiency in data storage maintenance. It benefits in gaining the agility, cost-effectiveness and data quality. Ex: VMware, Citrix etc.

Education as a service (EaaS): This service layer includes the e-learning and smart classes’ concepts that are demonstrated as an education-oriented services. The model establishes distant learning programs that help users accessing the knowledge and services independent of their location. E.g. Educomp, Indiamart, and Microsoft smart class library, etc. To meet the requirements and to efficiently use such services there are many service providers that can be listed out in the following way. See Fig.2. The fig also depicts that at every level it requires some kind of security protocols that must be strong enough to handle any kind of breakthrough possibility & stop the attacker to affect the system.

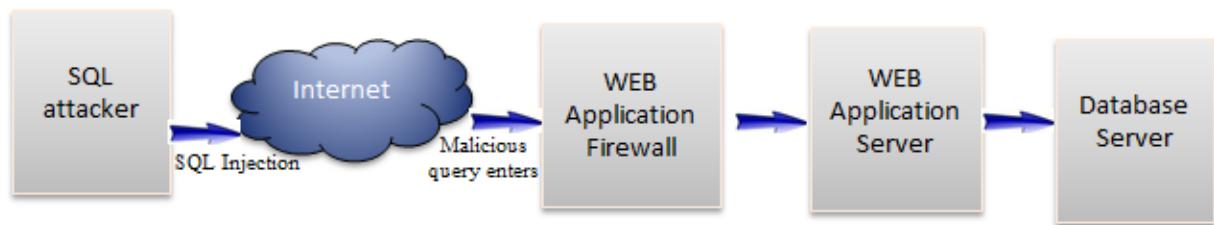


Fig. 1: Representation of the way SQL Injection Attack is initiated.

TYPE OF SERVICE	SUB-SERVICES	SERVICE PROVIDERS
1) Cloud storage:	Database	<ul style="list-style-type: none"> • Google Big Table, • Amazon simple DB
	Network attached storage	<ul style="list-style-type: none"> • Nirvanix Cloud NAS, • Mobile MeDisk
1) Cloud infrastructure:	Grid computing	<ul style="list-style-type: none"> • Sun grid
	Full virtualization	<ul style="list-style-type: none"> • Skytap, • Go Grid
	Compute	<ul style="list-style-type: none"> • Amazon Elastic compute cloud
2) Cloud applications:	Peer-to-peer	<ul style="list-style-type: none"> • BitTorrent, • SETI, • Lain-Lain
	Web applications	<ul style="list-style-type: none"> • Facebook
	SaaS	<ul style="list-style-type: none"> • Google Apps, • Salesforce.com, • Lain-Lain
3) Cloud platform:	Web application framework	<ul style="list-style-type: none"> • Ruby on Rails • Python Django, • .net
	Web Hosting	<ul style="list-style-type: none"> • atlantic.net
	Proprietary	<ul style="list-style-type: none"> • Force.com

Fig. 2: Examples of Different Service Providers

VI. SQLAs SOLUTION FOR DIFFERENT CLOUD SERVICES

When the system is divided over three-tier architecture: The introducing approach is fairly a runtime detection & prevention methodology following three-tier (Client-Logic Access- Data Server) organization to process, access and exchange queries. As it ensures that the Data-Server tier will probably not execute any vulnerable code which affects the system or the hosted operating systems & devices partially or completely. The technique is working over the database server side being associated with a distributed cloud environment to provide a security controlling system for ensuring the secure execution of all requested queries without any database hacking or fabrication.

Procedure

Receive_Query_Unveil_Message (T: Tier level number)

begin

Update row T of access table to increase input count;

end

Procedure

Finish_Query (T: Tier level number)

begin

Update row T of access table to increase consumed count;

End

Procedure Upon_Idle

Begin

Report to server controller non-zero difference for previously unreported rows of access table;

End

The algorithm for tier-architecture detects the completion of the query exchange process at tier level. As the queries $Q = \{q_1, q_2, q_3 \dots q_s\}$ go through a tier architecture representation for $T = \{t_1, t_2, t_3 \dots t_n\}$, that is for the proposed scenario works over up to n=3 levels. A general example to understand the SQL query injection can be studied through fig-3. The architecture is dependent upon the three-tier architecture system which is divided as follows:

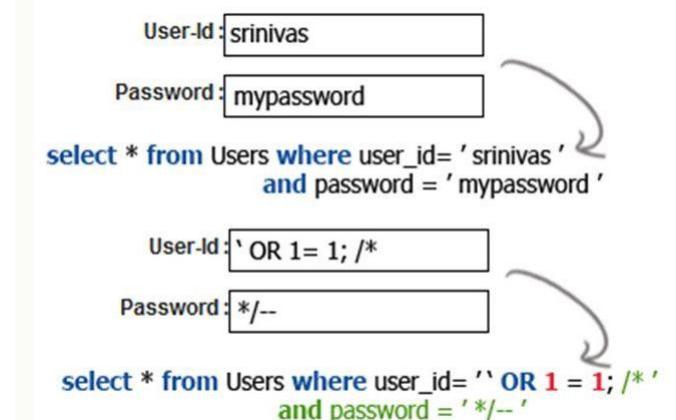


Fig-3 general example of SQL query injection. [7]

First tier (client tier) - The tier consists of applications that access a server which is usually located on a different machine from the server making a distributed environment. As here it is concerned to web browsers, servers or standalone application running on different machines that processes queries to request & response through the servers. If there are

S servers that share a communication through Q queries, the ratio of detecting a breakthrough would be directly proportional to R number of activities run where $R = \{r_1, r_2, r_3 \dots r_t\}$. Where on the whole the query associativity would be:

$$Q_i = \sum_{i=1}^t R$$

$$Q_i = \sum_{i=1}^t (r_1 + r_2 + r_3 \dots r_t)$$

As, each R outperforms s number of queries. Thus,

$$Q_i = (q_1, q_2, q_3 \dots q_s)_1 + (q_1, q_2, q_3 \dots q_s)_2 + \dots + (q_1, q_2, q_3 \dots q_s)_t$$

$$Q_i = t(q_1, q_2, q_3 \dots q_s)$$

$$Q_i = tQ$$

For which, if we have $i = 1$,

$$Q \cong t$$

The queries when are processed through distributed servers it gives the result into HTML form webpages. The webpages are uniquely

identified with their corresponding *url*. To find the associative probability it is further divided by 100 for the overall evaluation.

Second tier (logic access tier) – The layer concerns over the server codes that may include platform or such software applications which processes and set up communication behavior in between far over placed servers and systems, outperforming over C#, JSP, ASP.NET, VB, PHP etc. on the behalf, the layer is responsible for the authentication, authorization, caching, coupling & cohesion, exception management, validation and though is effectively logs & audit the progressive queries, say Q.

Third tier (data server tier) – it represents and considers database services over distinct servers. This layer embraces all the database objects that might be used by applications, such as schemas, views, tables and stored procedures. Definitions of the instance-level objects available for SQL server objects are stored over the databases over the data server tier. The tools of the layer can be listed out as: Application Developer, Database Administrator, Independent Software Vendor, IT Administrator, etc. supporting the operations EXTRACT, DEPLOY, REGISTER, UNREGISTER, UPGRADE which might help in EXPORT-IMPORT of the request –response queries.

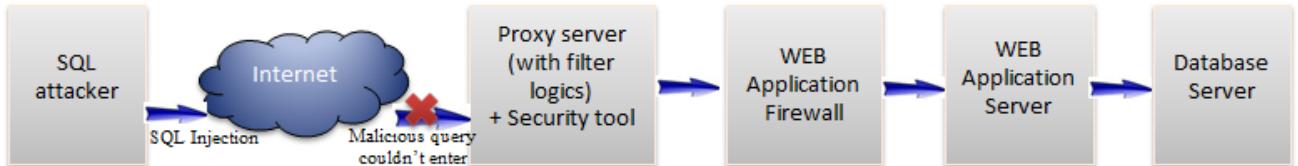


Fig. 4: Representation of the way SQL Injection Attack is detected and filtered & stops malicious query.

The proposed methodology indulges this 3-tier architecture which defines the level-wise security from SQLIA's attacks. By proposing the proxy server over the cloud DSP (Data Service Provide) 40% of the attacks reduces. For excluding the other 60% of the attacks Valid Security tool can be installed over the proxy server that helps queries to get compared from the original one using some metrics already stored over the security tool that filters out the malicious queries. It protects the firewall to get crossed-over, see fig-4.

VII. IMPLEMENTATION & EVALUATION ANALYSIS

The experimental process is under progress that is required to do on a large scale, including SQL, NOSql & NewSQL databases and also the application oriented scenarios. On the basis of the work done till the date it possesses to evaluate at 75-87% success to get success probability associativity using

the proposed formula. It secures the data of all the cloud types and the services provided. The system guidelines can be predicted through table-2.

Initiating over a supercomputer sometimes is a difficult task, but here an archetype is to be designed for execution of queries and transactions for carrying up over inter and intra-cloud. Thus, in concern, Table-1 shows system configuration scenario instigating technical attributes like RAM, OS, Hard-disk etc. required for the implementation of the proposed solution. In fig-4 the smallest average (for 4 different queries for the comparison table-1) over which the lines have contracted is represented which has a very small difference of negotiation. One complete single cycle includes the static & dynamic variability and the process that leads to filtration after the detection of injected SQL queries. In the graph (see fig-5) for the practical evaluation the following queries are picked with 57 vulnerable instructions at the same:

Table-1 details of considered query comparison for evaluation.

Query cycle	Query type
Query-1	it takes 57 Read instructions in a single go
Query-2	it takes 57 Write instructions simultaneously

Query-3	takes 57 Update instructions
Query-4	it takes 57 Retrieve instructions in parallel

Table-2 technical details of implementation environment

Setup phase	Technical attributes	Configuration
System setup	RAM Capacity	8 GB
	Processor	Intel(R) Core(TM) i7 CPU Q 740 @ 1.73GHz 1.73GHz Turbo up to 1.93 GHz
	Operating system	Windows 7 ultimate
	Hard-disk	1 TB
	Graphic card (if required)	NVIDIA GeForce GT 425M-2GB

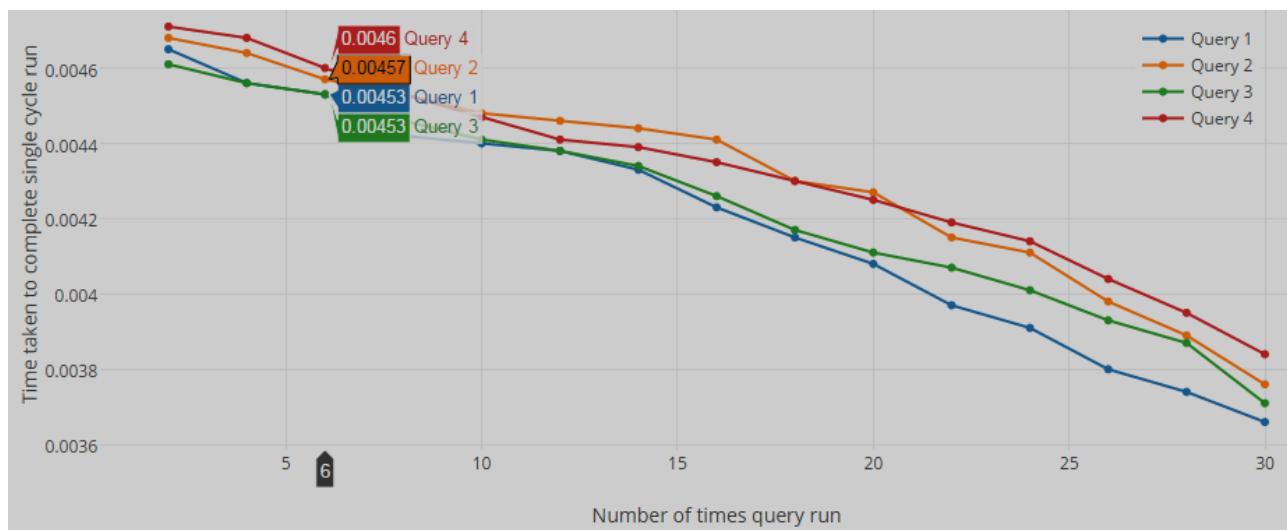


Fig-5 Average negotiation comparison for 4 random queries with 57 transactions included in a single query

SQL Inject Me lets you test the page you're viewing for Cross Site Scripting vulnerabilities.

Each tab represents a form on the page and lists all the fields. Just fill in good values for all the fields and mark which ones are to be tested (they will become yellow) then click either "Test with All Attacks" or "Test with Top Attacks".

Unnamed form 1

These are the fields in this form:

keywords – Change this to the value you want tested

searchType – web

SQL Inject Me lets you test the page you're viewing for SQL Injection vulnerabilities.

Each tab represents a form on the page and lists all the fields. Just fill in good values for all the fields and mark which ones are to be tested (they will become yellow) then click either "Test with All Attacks" or "Test with Top Attacks".

Unnamed form 1

Execute Run all tests

Change this to the value you want tested

locale-only on

lang en-US

from /en-US/firefox/addons/policy/0/7597/52585?src=addondetail

Fig-6(a)-6(b) Query tested through SQL inject me simulation.

To evaluate the work and to deal with the static and dynamic queries the online SQL inject me is used. To validate the work queries are run in bulk followed by different cycles parallel. Fig.6 shows and observes the work flow presented with a flow where 6(a) depicts the process to fire the query through one system and 6(b) representing the random server to be attacked. Studying the facts and the process grows further major trends as well that will be evaluated in future.

VIII. CONCLUSION

The introducing approach is fairly a runtime detection & prevention methodology following three-tier (Client-Logic Access- Data Server) organization to process, access and exchange queries. As it ensures that the Data-Server tier will probably not execute any vulnerable code which affects the system or the hosted operating systems & devices, partially or completely. The technique is working over the database server side being associated with a distributed cloud environment to provide a security controlling system for ensuring the secure execution of all requested queries without any database hacking or fabrication. By proposing the proxy server over the cloud DSP (Data Service Provide) 40% of the attacks reduces. For excluding the other 60% of the attack security tool is installed over the proxy server helping queries to get compared from the original one using some metrics already stored over the security tool that filters out the malicious queries & protects the firewall to get crossed-over.

REFERENCES

- [1] 1. *Towards safer information sharing in the cloud*. **Casassa-Mont, Marco, et al., et al.** Berlin : Springer, August 23 , 2014, International Journal of Information Security, pp. 319-334. 10.1007/s10207-014-0258-5.
- [2] “Next generation of computing through cloud computing technology”, **Muhammad baqer mullah, Kazi reazul islam, Sikder sunbeam Islam**, 2012 25th IEEE Canadian Conference on Electrical and Computer Engineering (CCECE).
- [3] “cloud computing features,Issues and Challenges:A big picture”, **Deepak puthal, B.P.S Sahoo, Sambit Mishra, Satyabrata swain**,2015 International Conference on Computational Intelligence & Networks, pp. 116-123.
- [4] An approach to enable cloud service providers to arrange IaaS, PaaS and SaaS using external virtualization infrastructures”, **Antonio celesti, Francesco tusa, Massimo villari, Antonio puliafito**, “2011 IEEE World congress on services, pp. 607-611
- [5] “SLA-based resource allocation for software as a service provider (SaaS) in cloud computing environments”,**Lillin wu, Saurabh kumar garg, Rajkumar buyya**, 2011 11th IEEE/ACM International symposium on cluster, cloud and grid computing, pp.195-204.
- [6] “Open learning optimization based on cloud technology: case study implementation in personalization E-learning”, **Nungki selviandro, Mira suryani, Zainal A. Hasibuan**, February 16~19, 2014, pp. 541-546.
- [7] “Implement of cloud computing for e-Learning system”, **Manop phankokruad**,2012 International Conference on Computer & Information Science (ICCIS), pp. 7-11
- [8] 2. *Extended results on privacy against coalitions of users in user-private information retrieval protocols*. **Colleen M. Swanson, Douglas R. Stinson**. 4, s.l. : Springer, February 12 , 2015, Cryptography and Communications, Vol. 7, pp. 415-437.
- [9] 3. *Global sensitivity measures from given data*. **Elmar Plischke, Emanuele Borgonovob, Curtis L. Smithc**. 3, s.l. : elsevier, may 1, 2013, European Journal of Operational Research, Vol. 226, pp. 536-550. 10.1016/j.ejor.2012.11.047.
- [10] 4. *Cache Serializability: Reducing Inconsistency in Edge Transactions*. **Eyal, I., Birman, K. and van Renesse, R.** columbus, OH : IEEE, june-july 29-2, 2015, 2015 IEEE 35th International Conference on Distributed Computing Systems (ICDCS), pp. 686-695. 10.1109/ICDCS.2015.75.
- [11] 5. *Combining Static Analysis and Runtime Monitoring to Counter SQL-Injection Attacks*. **W. Halfond, A. Orso**. s.l. : IEEE, Proceeding of the Third International ICSE Workshop on Dynamic Analysis .
- [12] 6. *Detection and Prevention of SQL Injection Attacks*. **Halfond, William G.J. and Orso, Alessandro**. s.l. : Springer, 2007, pp. 85-109.
- [13] 7. *CANDID: Preventing SQL Injection Attacks using Dynamic Candidate Evaluations*. **Bandhakavi, Sruthi, et al., et al.** Alexandria, Virginia, USA : ACM, October-November 29-2, 2007.
- [14] 8. *Privacy-enhanced architecture for smart metering*. **Félix Gómez Marmol, Christoph Sorge, Ronald Petrlík, Osman Ugus, Dirk Westhoff, Gregorio Martínez Pérez**. 2, s.l. : Springer, november 28, 2012, International Journal of Information Security, Vol. 12, pp. 67-82. 10.1007/s10207-012-0181-6.

Survey On Issues In Wireless Sensor Networks: Attacks and Countermeasures

Rangstone Paul Kurbah¹, Bobby Sharma²
Assam Don Bosco University, Guwahati, Assam
rangstonepaul@yahoo.com¹
bobby.sharma@dbuniversity.ac.in²

Abstract—Wireless Sensor Networks have become popular day by day. They find their applications in numerous areas. These networks, however, have some constraints like the physical size (that they must be compact), energy (that minimum energy must suffice them for long hours), memory space (that they should effectively work with just minimum memory space installed on them), and above all that their construction cost must be minimum. Due to these constraints they face some security issues. Securing the data that flows through these networks must be of paramount importance and the security issues that are faced by these networks must be addressed in order to enhance their reliability and usage. This paper focuses on the security aspects of Wireless Sensor Networks. It presents the general characteristics of Wireless Sensor Networks, their constraints, their security goals, the thread models, the different types of attack on WSNs and their defensive measures.

Keywords: Attacks, Defensive Measures, Nodes, Security, Wireless Sensor Network (WSN).

I. INTRODUCTION

A Wireless Sensor Network consists of a number of nodes (with wireless communication capability) called sensor motes (Field Device) [3]. The number of motes in WSNs can be from hundreds to a few thousands of them. The WSNs find application in many areas like for example in medical care, geographical monitoring, forecast systems, home and office applications, transportation, manufacturing, logistics, military operations, environmental monitoring, industrial monitoring and surveillance. The WSNs find applications in such numerous areas owing to their easy-to-apply and flexible installation. However, due to these properties, they are also liable to many security issues and attacks. More so, they are required to provide availability, authorization, authenticity, integrity, confidentiality, data-freshness in very limited resource constraints [5]. Due to the limited resource constraints and their limited computational power, they pose a great deal of challenges in term of security aspects [6].

The content of this paper is organized as follows:

Section 1. Architecture of sensor node

Section 2. Overview of WSN

- Section 3: Characteristic of WSN's.
- Section 4: Some of the constraints in WSN's.
- Section 5: Security goals of WSN's.
- Section 6: Thread models.
- Section 7: Attacks on WSN's.
- Section 8: Defensive measures to attacks on WSN's.

II. ARCHITECTURE OF SENSOR NODES

The basic sensor node has four major components in general namely the sensing unit, the processing unit, the transmission unit and the power unit [16], [17], [18], [19].

A. The Sensing Unit

The sensor unit senses the physical environment and tells the Central Processing Unit (CPU) to process the data it feeds and to store the data. The sensor unit is comprised of the sensor and the Analog to digital converters (ADCs). The sensor performs conversion of the physical phenomenon into electrical signal which is in turn converted into digital signal by the ADC.

B. The Processing Unit

The processing unit which consists of the microcontroller or the microprocessor is the one which performs execution on the data fed by the sensor unit, execution of communication protocols, cryptographic tasks and controlling of the sensors.

C. The Transmission Unit

The Transmission unit consists of the antenna (transceiver) for communication with other sensor nodes in the network including the base station. It transmits data it receives from the CPU to the outside world.

D. The Power Unit

The power unit supplies the required electrical energy to all the other components in the sensor node. The power supply unit is generally the battery/batteries.

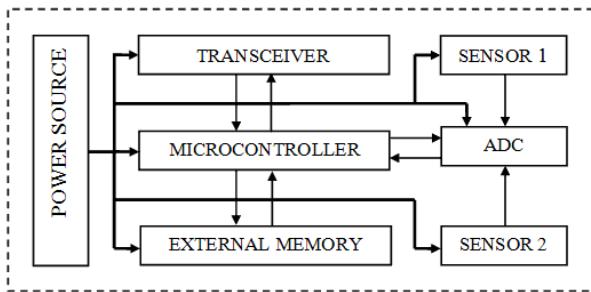


Figure.1: Sensor Node Architecture [18], [19]

III. OVERVIEW OF WIRELESS SENSOR NETWORK

The Base Stations (BS) are the Local Sites Masters [20]. A base-station is a node which may be fixed or mobile responsible for connecting the sensor network to some communications infrastructure or may be to the Internet where a user can access the data reported [21]. The gateway acts as an interface between the application platform and the sensor nodes. All the data or information received from the sensor nodes are gathered by the gateway and transmitted to the application. The Task Manager collects the information from the Base Station (Local Sites Masters) for processing or computation and stores it for future use [20]. The overview of WSN is shown in figure 2.

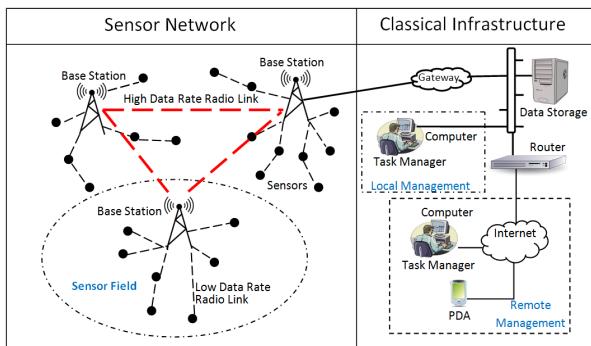


Figure. 2: Overview of WSN [20]

IV. CHARACTERISTICS OF WSN'S

The WSNs exhibit a number of characteristics that make them attractive for a number of applications but at the same time giving rise to a number of security challenges. The following are the general characteristics of WSNs as described in [4], [6], [9].

A. Compact size

Due to their nature of deployment and purposes, the physical size of the WSNs nodes are kept small. Owing to this characteristic, there is a constraint on the size of the main chipboard and the number and size of components on it. Therefore only the crucial parts are installed in the nodes. This limits their computational power to an appreciable extend.

B. Physical Security

The WSNs nodes are deployed in hostile environment and have to interact with the surroundings. Therefore they are liable to all sort of physical attacks.

C. Power

The WSNs nodes are powered by non-renewable energy with the help of batteries. They are deployed in areas where human interaction with them is not much or even not at all. However, the energy will eventually get exhausted with time and with the amount of processing that they have to perform. The sensor nodes with security features like authentication mechanism, encryption-decryption mechanism, and the like, consume more batter power at a much higher rate, thus making the situation worse.

D. Memory Space

Each of the nodes in WSNs has to have some memory for their processing, storage of data and cryptographic keys and other useful information needed for their proper coordination among themselves in the WSN. However, due to the constraints on the size and power, the memory size is compromised. Only the smallest possible size of memory is given to each mote. This in turn leads to the requirement that the codes, the cryptographic keys and other security algorithm to be as small as possible.

E. Bandwidth

In Comparison to any other wireless networks, WSNs use a much lower bandwidth. The amount of data transmitted and received by the nodes is also low. This is important in order to reduce the rate at which power is dissipated so that their lifespan is increased. It is estimated that the transmission of one bit requires as much power as executing eight hundred to one thousand instructions. Hence, the bandwidth is compromised for the sake of power saving.

V. SOME OF THE CONSTRAINTS IN WSN'S

Some of the constraints in WSN's that are discussed in [4], [11], [15] are as follows.

A. Limited resources

The WSNs are required to survive and be functional with just the limited amount of resources available to them. The limited resources are like the low small memory, low computational power, limited bandwidth and low battery power (sometimes no rechargeable ones are used). This constraint poses great challenges to resource - hungry security enhancing mechanisms.

B. Small size message

The messages in WSNs are usually of smaller sizes than those in other wireless networks or in other networks in general. Hence, the concept of message segmentation is not implemented in most WSNs.

C. Nodes Addressing Scheme

Because of the relatively larger number of motes that can be part of a WSN, it becomes impossible to have a global addressing scheme to identify each of the motes in the WSN as the identity maintenance overhead is high.

D. Sensor nodes location and data redundancy

Since the data collected from the sensor nodes are analyzed based on the locations of the nodes, hence it is extremely important to locate each and every node in the WSN. Also because there might be a common phenomenon of data collection, the redundancy of the data can be highly probable.

VI. SECURITY GOALS OF WSN'S

The security goal of WSN is to protect data from any adversaries or attackers to view confidential data, manipulate them or to bring about the Denial of Service (DoS). The authors in [6], [9], [11], [15], present some of the security goals of WSN's as follows:

A. Availability

This ensures that all the services that the WSNs provide should be available even if there is DoS attack on it.

B. Authorization

This ensures that only the authorized nodes are allowed to exchange information between them.

C. Authentication

This ensures that any nodes that participate in the WSN should show their real identity. That is to say that masquerading is averted.

D. Confidentiality

This makes sure that the data are not leaked to any unintended recipients or users. The data is to be understood or makes sense only to the intended recipients.

E. Integrity

This ensures that the messages that are shared amongst authorized nodes are not tampered by any malicious nodes in between. They reach the destination nodes as they were sent from the source.

F. Non-repudiation:

This makes sure that the sender cannot later deny sending a message that it has really sent it.

G. Data Freshness

This ensures that the data received by the destination node is recent and that the adversaries cannot replay old messages again.

H. Robustness

When any node/nodes in the network is/are compromised the entire network is not compromised.

I. Self-organization

The node should be autonomous (self-organizing) and should be self-healing (fault tolerance).

VII. THREAT MODELS

The authors of [1], [4], [8] posit that threads in WSN can be classified into the following categories:

A. Passive and Active attacks

In passive attacks, the intruder only views the content of the data (eavesdropping), thereby breaching the data confidentiality aspect of the security goals. In active attacks, the adversary performs some modification on the data streams and even creates fake data streams thereby breaching the data integrity aspect of the security goal.[6],[9],[15].

B. Outsider and Insider Attacks

The outsider attack is one in which the attack is considered to be from nodes that do not belong to the WSN. The insider attack, on the other hand, is one in which the attacker is actually one of the legitimate (compromised) nodes of the WSN. The insider attack may have some confidential information of the WSN like the cryptographic keys and they also have the trust of the other sensor nodes. The insider attack, due to its very nature, is much more difficult to detect.

C. Laptop-class and Mote-class attack

In mote-class attack, the adversaries perform the attack by employing some nodes that have the same or similar capabilities as the other nodes of the WSN. In laptop-class attack, the adversaries employ more powerful devices like

laptop to cause harm to the network. The harm caused by laptop-class attack is much more worst than the ones caused by any malicious nodes.

VIII. ATTACKS ON WSN'S

The following are the attacks on Wireless Sensor Networks.

A. Denial of Service (DoS) Attack

The denial of service (DoS) attack can be carried out at the physical, data link, network and transport layers. The following are the two types of DoS attacks:

1) Jamming Attack

Nodes in WSN transmit messages to other nodes by utilizing some frequencies. The adversaries can tune the frequencies of its malicious nodes my transmitting the same frequencies as the other legitimate nodes. This causes interference with the frequency of legitimates nodes [12]. This process is called Jamming. The jammed nodes may be temporarily or even permanently suspended from being able to receive or transmit messages to other nodes in the network. The use of a single frequency for communication in WSN makes it more susceptible to jamming attack [4].

However, due to the distributive nature of WSN, the efficacy of this attack is not 100%. Nonetheless, even if only a few nodes in the WSN are jammed, the impact may still be detrimental to its overall performance.

2) Physical Attack

The WSN, as mentioned earlier, are deployed in all sorts of environmental conditions. Sometimes the environment can be extremely harsh and hostile. Therefore, they nodes are under constant pressure from the surroundings. Moreover, the designs of the nodes is such that the cost of construction is minimal and the size is compact which makes it difficult to add any physical strength to them to make them temper-proof. Due to these weaknesses, the adversaries can easily break them down and extract the confidential data in them like the cryptographic parameters and the source code giving them the feasibility to modify the codes to have access to the network [12]. The adversaries may also remove the legitimate nodes and in their places they may put the malicious and illegitimate nodes, thereby putting the entire WSN in danger. [9].

The physical attack is difficult to deal with because of the very nature of WSN, to keep the cost minimal and the size of the nodes compact.

B. Collision Attack

Collision is another form of jamming at the data link layer. Collision is caused by continues transmission of messages. Sunil et al [4] say that collision alters the

messages which then causes the collided messages to be retransmitted due to checksum mismatch at the receiving node. If this happens very often then the energy gets depleted very quickly and also other resources like bandwidth get wasted.

C. Exhaustion Attack

This form of attack aims at draining the energy of the sensor nodes. The attack fakes the collisions making the nodes to retransmit messages even if the messages have reached the destination intact. The malicious node may do so by continuously sending request to the neighboring nodes, making them to respond continuously [6].

D. Neglect and Greed attack

Messages sent by a sender to a destination node may be routed or re-routed through a number of nodes called hops. While on their journey towards the intended destination node, the messages may be routed through some malicious or compromised nodes that divert their route to some other fake nodes. Thus the messages may get dropped along the way. This attack adversely affects the expecting neighboring nodes making them to wait for the dropped packets and also renders them not to be able to transmit messages.

E. Homing Attack

The most important nodes in WSN are the base stations or cluster nodes. The adversaries make efforts to track these nodes by analyzing the traffics. Once they found out these cluster nodes or base station, they will perform all sorts of attacks on these nodes, physically attack them or capture them thereby misusing them for their own interests.

F. Routing Information Alteration (Spoofing)

The authors of [5] say that in this attack the adversaries alter the routing information, creating new routes, shortening or lengthening the existing routes thereby increasing the latency of messages delivery. This can lead to retransmission of messages. He/she can also forge error messages that increase the latency or even deprive the nodes to access to the channel. The routing information can be changed so as to attract or repel the traffics so as to increase the latency of message delivery.

G. Black Holes/Sinkholes Attack

This is another form of routing information alteration attacks. If we use distance-vector based protocols in WSN, the WSN will be more prone to sinkhole attack. The malicious node advertises zero-cost route thereby attracting traffic to itself thus creating a metaphorical sinkhole [6]. The neighboring nodes of the malicious nodes compete for the unlimited bandwidth, which causes contention of resources among the nodes and message disruption.

H. Flooding Attack

This is a resources exhaustion attack. In this attack, the malicious nodes send continuous request to the neighboring nodes. Such an attack makes the neighboring nodes (to whom the requests were made) to allocate resources to each an every request made by the malicious nodes causing starvation to the legitimate nodes [12]. If this attack continues, the memory and energy resources of the nodes will get drained.

I. De-synchronization Attack

Sunil et al [4] explain that in this attack, the malicious nodes transmit some control flags and sequence number of the old frames to the legitimate nodes, making them think as if their synchronization has lost. This causes the legitimate nodes to retransmit the assumed missed frames again. If this transmission of altered messages persists, the nodes will soon run short of resources that they require to continue doing their work. The other side effect of this attack is that the legitimate nodes become incapable of sharing any useful information with other nodes as they are infinitely engaging in the synchronization-recovery processes.

J. Sybil Attack

Newsome et al [2], describes this attack as an attack in which a malicious node exhibits multiple identities. This attack causes the redundancy mechanism in the distributed data storage systems in peer-to-peer network to fail.

Sybil attack adversely affects the fault tolerance scheme in WSN like data aggregation, voting, routing algorithms, multi path routing, topology maintenance and fair resource allocation. Because of its ability to affect the geographical routing protocols, the malicious node can ooze the illusion to the network as if it is located in many geographical regions at a time. Also the malicious node can create additional votes during the voting process owing to its ability to present multiple identities for itself.

K. Selective forwarding Attack

In selective forwarding, a malicious node acts like a black hole that selectively routes some of the messages and dropping some of them [3]. This is done so to avert any suspicion by the other neighboring node. If the malicious node drops all the packets/messages, the neighboring nodes will suspect a malfunctioning of the route, thus try to find new routes for the packets. The malicious node may also drop packets from some particular nodes but faithfully route packets to other nodes.

Selective forwarding gives the impression that all the nodes in the network are reliable. Thus, this type of attack is very difficult to detect.

L. Wormholes Attack

In this type of attack, a malicious node advertises to its neighboring nodes that they are just a few hops away from

the base station via the wormhole (malicious node), in reality though they are multi hops away from the base station. This attracts traffics towards the malicious node (wormhole) thereby creating a sinkhole [1].

Wormholes are difficult to detect because they employ a private, out-of-band channel not visible to the underlying sensor network.

M. HELLO Flood Attack:

[1] Most protocols require nodes to broadcast HELLO messages to its neighboring nodes to announce its presence in the network. The adversaries can take advantage of this requirement by deploying high power devices (laptop-class attack) to transmit HELLO messages to all the neighboring nodes assuring them that they (the malicious nodes) are their neighbors, thus starting to communicate with them. The adversaries, thus, are getting access to the information shared within this compromised network.

The authors of [1] also posit that the adversary doesn't need to have the capability to establish legitimate traffic so as to be able to launch HELLO Flood attack. He/she can simply re-broadcast overhead packets to every node in the WSN.

N. Acknowledgement Spoofing Attack

Acknowledgements are vital for reliable communication among nodes. The adversary can, however, exploit this mechanism by altering the information present in the acknowledgement packets to convince the sender that the link which is actually weak is strong enough for communication which is reliable, or that the nodes that are dead are still alive [5]. Since routing of packet to dead nodes leads to dropping of packets, the adversary can effectively mount selective forwarding attack using acknowledgement spoofing.

O. Node Replication Attack/Impersonation Attack

Each and every node in WSN has a unique ID which serves as its identity in the WSN. The adversary can copy the IDs of the legitimate nodes and assign the same to his/her malicious nodes, thus creating clones of the legitimate nodes. These malicious nodes have similar capabilities as the legitimate nodes. In fact, in addition to the capabilities that the legitimate nodes have, the malicious nodes may also have additional features like the capability to send information (which are of interest to the adversaries) to the adversaries. These information could be the cryptographic keys, the routing information, etc. Making use of these information at hand, the adversary can inflict more harm to the network.

The authors of [5] posit that the Node Replication attack is different from Sybil attack. In Sybil attack one malicious node presents a number of identities but in Node Replication Attack a number of malicious nodes share a common identity.

IX. DEFENSIVE MEASURES TO ATTACKS ON WSN's

A. Denial of Service

1) Jamming Attack

One way to defend the jamming attack is to identify the jammed nodes. Newsome et al[2] suggest two ways to assure identities, direct validation and indirect validation. In indirect validation, a third party node performs the validation process, to testify whether the joining node is a valid one or not. While in direct validation, a trusted nodes performs this validation. A radio resource test is a technique employed in direct validation. In this technique, a sensor node in the WSN assigns each to each of its neighbors a different channel through which to communicate to it. It sporadically and randomly checks a channel and listens. Should there be a transmission through the channel it is assumed that it is the physical node that is responsible for this transmission otherwise it is not a physical identity.

One characteristic of jamming is that there is a high background noise that be sensed and reported. Should there be a jammed part of the WSN, the routing which is supposed to be done through this part is deviated through other unaffected part of the network.

2) Physical attacks

It is impractical to fully guarantee complete defense against physical attack to the nodes owing their large number and their distribution over large distance and area to form a WSN. Nonetheless, it is imperative to provide physical protection to them.

Nodes deployed in hostile and harsh environment are susceptible to all sort of physical damages. Hence, they should be made temper-proof with tamper-resistant material [6]. Hiding the nodes and camouflaging them can be some of the preventive measures against physical attack.

The adversaries can physically exploit the nodes to extract the critical information like codes and cryptographic keys. This type of attack can be prevented by employing some erasure mechanism which will delete these critical information stored in the nodes when they are physically exploited which in other words would mean to stop the service of the compromised node [6].

B. Collision Attack

Collision leads to alteration of packets, dropping and discarding of packets that eventually lead to retransmission of these same packets. This leads to exploitation of resources.

Collision can be averted by using Cyclic Redundancy Check to check if the integrity of the message has been breached. Error detection and correcting codes may also be

used. However, this technique comes at the cause of adding additional bits to the original message [7].

C. Exhaustion Attack

Collision is another form of resources exhaustion. Time Division Multiplexing (TDM) and Rate Limiting can be used as countermeasures to this attack [14]. TDM assigns a time slot to each an every sensor to send data in the WSN. This avoids collisions. Putting a constraint to the number of requests to access the network at a time helps in avoiding collisions. This can be achieved by implementing MAC admission control mechanism [6].

D. Neglect and Greed attack

This attack is very difficult to detect. However, to stop the negative effects (at least to reduce them) we can define alternate routes for the packets and also by using redundant messages to reduce the damage by malicious nodes. Along with these mounting of Authentication scheme, monitoring, flexible routing and three way handshake will help averting the damage because of this attack [10].

E. Homing Attack

The adversaries track the important nodes which are the cluster nodes or base station by analyzing the traffic that flows to/from them. The tracking can be made difficult by encrypting the header and the content of the messages and by having a strong access control [8].

F. Routing Information Alteration (Spoofing) Attack

CRC or MAC schemes can be used to make the packets construction secure in order to make to tempered packets easily detectable. This attack can also be averted by deploying authentication mechanism at the link layer. This technique will allow only the authorized nodes to take part in communication. The authors of [3] suggest solution to spoofing attack by using a different path for the retransmission of packets.

(The authentication and anti-replay protection scheme can take care against the interrogation attacks).

G. Black Holes/Sinkholes attack

Similar steps can be taken to counter the effects of black holes/sinkholes attack as for routing information alteration (spoofing). The requests to access the network are accepted only if they come from authorized nodes. Public key cryptography can also be used to sign and in the verification of the routing related information and their updates [6]. This scheme, however, is costly and it needs large overhead which makes its usage a difficulty.

Trust management and efficient authentication in WSN can also be achieved by employing threshold based cryptography based schemes and efficient certification mechanism.

The activities of a node can be monitored by neighboring nodes by sending dummy packets to it, and then analyze the

behavior of the WSN by checking if the packets reach their destination or not.

H. Flooding Attack

One way to counter flooding attack is by setting the limits the number of connections to the nodes. This scheme, however, has the side effect of ignoring connection even to legitimate nodes [12].

Any node/nodes who wish to establish connection/connections are presented puzzles [13]. The nodes will have to solve the puzzles to show their commitment. The adversaries who intend to perform this attack will need to have more resources. While this countermeasure may prove studious to the attacker, it also requires the legitimate nodes to have enough resources and energy (resources and energy being the downsides of WSN nodes).

I. De-Synchronization Attack

This attack can be averted by using authentication scheme for the critical parts of the packets transmission. If the receiver detects any fake messages, it ignores the instruction carried by it. The authors of [3] suggest countermeasure for this attack by using different neighbor for time synchronization.

J. Sybil Attack

It is very difficult to avert an insider attack of this kind. It is, however, possible to restrict its activities. The base station can limit the number of nodes any node can establish connections with. Any inconsistency to this rule will initiate the occurrence of error. This scheme can be augmented by mounting the identity verification onto it. This requires that all the nodes share a unique symmetric key with a trusted base station [3]. A Needham-Schroeder like protocol can then be used by any pair of nodes in their verification each other's identity so that shared key can be subsequently established between them. The pair of nodes then used this resultant key to establish an encrypted and authenticated link between them.

Newsome et al [2] describe two ways to validate the identities, direct validation and indirect validation. In direct validation, the node itself performs the testing to check if the joining node's identity is valid. In indirect validation, a third party trusted node performs this function of identity validation.

(Each node has a unique key that it share with the base station to verify its communications with the base station and with other nodes.)

K. Selective forwarding Attack

The solution to his problem is similar to that of Routing Information Alteration (Spoofing) and Black Holes/Sinkholes attacks, that is to have multipath routing scheme [6]. This ensures delivery of the packets to the destination node/nodes.

Monitoring of the network frequently enables the Wireless Sensor Network to detect any nodes that are behaving maliciously. Source routing which uses Geographical monitoring can also be used as a preventive measure against this attack.

L. Acknowledgement Spoofing Attack:

Karlof et al [1] suggest that countermeasure for this attack by deploying good encryption techniques and proper authentication scheme for secured communication.

X. CONCLUSION:

As discussed above, Wireless Sensor Networks find their application in many areas, from the smallest to the biggest and serious areas like medical and military. Along with the blessings they also come with some weaknesses that we cannot ignore. For instance, the military data are extremely confidential. Compromising this is unacceptable. As has been mentioned above, attack on confidentiality isn't the only problem we face in WSNs. Other types of attack like those on the data integrity, data freshness and Denial of Service attack are very much there against WSNs. Hence, it is imperative that security issues prevailing in WSNs be addressed. This paper has given a brief introduction to Wireless Sensor Networks and their general characters. It discusses the thread models in WSNs, the different types of attacks on WSNs and their respective countermeasures.

REFERENCES

- [1] Chris Karlof and David Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures", University of California, Berkeley, "Elsevier's AdHoc Networks Journal", 2003.
- [2] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil attack in sensor networks: analysis & defense", "Third International Symposium on Information Processing in Sensor Networks (ISIPSN 04)", ACM Press, pp. 259-268,2004.
- [3] Hemanta Kumar Kalita and AvijitKar, "Wireless Sensor Network Security Analysis", " International Journal of Next-Generation Networks (IJNGN)" , Vol.1, No.1, December 2009.
- [4] Sunil Ghildiyal, AmitKumar Mishra, Ashish Gupta, NehaGarg , " Analysis of denial of service (dos) attacks in wireless sensor networks", Uttaranchal University, Dehradun, Uttarakhand , Uttaranchal

- University, Dehradun Uttarakhand , Dev Bhoomi Institute of Technology, Dehradun Uttarakhand, Graphic Era University, Dehradun Uttarakhand , “IJRET: International Journal of Research in Engineering and Technology”, eISSN: 2319-1163 | pISSN: 2321 – 7308.
- [5] JyotiShukla, BabliKumari, “Security Threatsand Defense Approaches in Wireless Sensor Networks: An Overview”, Assistant Professor, Amity University ,M.tech Student, Amity University , “International Journal of Application or Innovation in Engineering & Management (IJAIEM)”, ISSN 2319-4847, Volume 2, Issue 3, March 2013.
- [6] Nusrat Fatema and Remus Brad, “Attacks and Counterattacks on Wireless Sensor Networks”, Faculty of Engineering, Lucian Blaga University of Sibiu, Sibiu, Romania, Lucian Blaga University of Sibiu, Sibiu, Romania, Computer Science and Electrical Engineering Department, “International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC)”, Vol.4, No.6, December 2013.
- [7] Hang Liu, Hairuo Ma, Magda El Zarki, and Sanjay Gupta, “Error control schemes for networks: An overview”, Mobile Networks and Applications, 1997.
- [8] Shahriar Mohammadi, Reza EbrahimiAtani and Hossein Jaddolesslamy ,“A Comparison of Routing Attacks on Wireless Sensor Networks”, Information Technology Engineering Group, Department of Industrial Engineering, K.N. Tossi University of Technology, Tehran, Iran , Department of Computer Engineering, “Journal of Information Assurance and Security”, ISSN 1554-1010, Volume 6 , pp. 195-215,2011.
- [9] Vaishali Pahune ,Sharda Khode , “Security issues, attacks and challenges in Wireless Sensor Network” , Department of CSE,APGCE, Nagpur , Department of CE,BDCOE , “International Journal of Engineering Sciences & Research Technology”, ISSN: 2277-9655, Wardha, June, 2015.
- [10] D.G. Anand, Dr. H.G.Chandrakanth, Dr. M.N.Giriprasad, “Security Threats & Issues in Wireless Sensor Networks”, Sri Krishna Institute of Technology, Bangalore, Karnataka, Sri Krishna Institute of Technology, Bangalore, Karnataka, Jawaharlal Nehru Technological University College of Engineering, Anantapur, Andra Pradesh, “International Journal of Engineering Research and Applications (IJERA)”, ISSN: 2248-9622 , Vol. 2, pp.911-916, Issue 1,Jan-Feb 2012.
- [11] Idrees S. Kocher, Chee-Onn Chow, Hiroshi Ishii, and Tanveer A. Zia, “Threat Models and Security Issues in Wireless Sensor Networks”, International Journal of Computer Theory and Engineering, Vol. 5, No. 5, October 2013.
- [12] Anthony D. Wood, John A. Stankovic, “Denial of Service in Sensor networks”, University of Virginia, 0018-9162/02/\$17.00 ©2002 IEEE .
- [13] T. Aura, P. Nikander, and J. Leivo, “ Dos-Resistant authentication with client puzzles,” Springer-Verlag, pp. 170-177,2001.
- [14] Chaudhari H.C. and Kadam L.U, ”Wireless Sensor Network Security Attack and Challenges”, “International Journal of Networking”, 2011, pp-04-16.
- [15] Dr.G.PadmavathiandMrsD.Shanmugpriya,”A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks”, “International Journal on Computer Science and Information Security”,2009,Vol 4.No.1&2.
- [16] Neetu Kumari, Nikita Patel, SatyajitAnand, ParthaPratim Bhattacharya, “Designing Low Power Wireless Sensor Networks: A Brief Survey”, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (An ISO 3297: 2007 Certified Organization), ISSN (Print) : 2320 – 3765 ISSN (Online): 2278 – 8875,Vol. 2, Issue 9, September 2013.
- [17] Jyoti Saraswat, NehaRathi, ParthaPratim Bhattacharya, “Techniques to Enhance Lifetime of Wireless Sensor Networks: A Survey”, Global Journal of Computer Science and Technology (E), Volume 12, Issue 14, Version 1.0, September 2012, ISSN Numbers: Online: 0975-4172, Print: 0975-4350, page: 2.
- [18] Ashish Gupta, Bhupender Singh Rautela, Binay Kumar, “Power Management in Wireless Sensor Networks”, International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Vol. 4, Issue 4, April 2014.
- [19] PankajChauhan, Tarun Kumar, “Power Optimization in Wireless Sensor Network: A Perspective”, International Journal of Engineering and Technical Research (IJETR) ISSN: 2321-0869, Volume-3, Issue-5, May 2015.
- [20] Miguel Angel Erazo Villegas, Seok Yee Tang, Yi Qian, “Wireless Sensor Network Communication Architecture for Wide-Area Large Scale Soil Moisture Estimation and Wetlands Monitoring”, Network Communications Infrastructure Group Department of Electrical and Computer Engineering University of Puerto Rico at Mayagüez, Walsap Research Project Technical Report TR-NCIG-0501, National Science Foundation under Grant No. 0424546.
- [21] Jamal N. Al-Karaki , Ahmed E. Kamal, “Routing techniques in wireless sensor networks: A Survey”, IEEE Wireless Communications, v.11 n.6, p.6-28, December 2004 [doi>10.1109/MWC.2004.1368893].

Syntactical Knowledge and Sanskrit Memamsa Principle Based Hybrid Approach for Text Summarization

¹D.Y.Sakhare, ²Raj Kumar

Abstract

The proposed approach works towards integrating syntactic knowledge and sentence fusion for abstractive multi-document summarization system. A fuzzy logic system, based on the “Paninian” Parts of Speech Tagging, is used to extract the syntactical knowledge-based informative words from English the documents. The sentences containing the informative words are selected for the further processing of abstractive summary generation. The sentence formation for the abstractive summarization is done using a neural network with features based on the Memamsa principles of the Sanskrit language. The features, such as “Upakram-Upsanhar,” “Abhyas,” “Apurvata,” “Phalam,” “Sthan,” “Prakaran” and “Samakhya” are used to form meaningful sentences. These features and the target summary of each document are given as input to train the neural network. The neural network trains the system based on the target summary of a set of documents with the same information to generate an abstractive summary for a new cluster of documents. The system performance is measured on a real data set and the DUC 2002 data set using ROUGE-1 and ROUGE-2 scores and the F-measure. The proposed Fuzzy- NN approach performs better than the existing techniques.

Keywords :Text summarization, Informative Word, Sentence Formation, Memamsa principles, Fuzzy NN, ROUGE

I. INTRODUCTION

Summarization of text documents is one of the crucial activities during the examination of large volumes of text documents. As document collections continue to grow, multi-document summarization is an increasingly important task. It helps the users to quickly find the most important and the relevant information from the huge data. A summary is formed by finding out the value adding judgments, which are instructive, from the text. For finding out the informative stuff the automatic summarizers have two different strategies[1-2]. In extractive summarization, sentences are retrieved in summary depending on the feature benchmarks. Abstractive methods require a deeper analysis of the text and the ability to make new sentences, which has intrinsic benefits for reducing redundancy and maintaining a good compression rate [3].

II. RELATED WORK

A relatively large work exists on extractive summarization as compared to abstractive summarization. [4] propose a

semantic matching for extractive summarization. Fuzzy logic based approach for extractive summarization has been elaborated by [5]. Along with Fuzzy logic the Deep learning algorithm are introduced by [6], to improve the efficiency of the extractive summary. Furthermore [7] have used fuzzy logic as well as Neural Network modules to develop the extractive models. The previous work of [8] shows that current extractive summarization systems rely heavily on the notion centrality of information. The model suggested that domain knowledge is important for substantial improvements in summarization. Sentence ranking for extractive summarization has been well carried out by [9] using Eigen vector. A Large work also exists on sentence compression and sentence fusion [10]. [11] Proposed the idea of disparate sentences fusion using one of the supervised algorithm. [12] Developed an approach for summarization by combining extractive and abstractive information. The statistical content selection, Natural Language Generation and Information Extraction based approach of [13] showed that in context of guided summarization, the complete abstraction can be achieved. [14] Show that at high controversial levels, the abstractive approach outperforms the extractive approach. A technique using diverse compression algorithms and integer linear programming is developed by[15]. [16] It developed a cluster-based method for a multi-document summarization system. This approach uses compression and coding theory to approximate the information distance between two different documents. [17] Proposed multi-lingual and multi-document text summarization using singular value decomposition as well as hierarchical clustering. The sentence selection was carried out by clustering algorithm and certain benchmark features. [18] Introduced an IE-based summarization. The system led to improvements in both manually evaluated content quality and readability. A source text Kernel-based statistical approach for multi document summarization is proposed by[19]. [20] Suggested that content selection can be applied to an abstract depiction rather than to original sentences or generated sentences.

These earlier developed models reveal that although the extractive summaries showed improved [21] ROUGE scores, the best performance require a proper language generation technique for abstractive summarization. The recent abstractive summarization approaches have focused on rewriting techniques without a careful consideration for a more complete model, which affects the abstracts significantly. A complete abstractive model can be developed if the system becomes intelligent enough, in Natural Language Processing (NLP), to determine the key contents i.e. the informative contents. For the identification of these key contents the, previously adopted text

summarization methods use information fragment that has been weighted as ‘important’ by human summaries. The systems themselves are inefficient to determine the weighted fragments. This motivates us to use the traditional Sanskrit Shastras which are rich in NLP and are considered more close to the process of cognition [22] These have a very rare remark in the field of text summarization. ‘Memamsa’, ‘Nyaya’, and ‘Vyakarana’ are the three different Sanskrit Shastras. Among which the ‘Sanskrit Memamsa’ principles were used in the ancient days for various text processing principles of Sanskrit language. In this paper the ‘Memamsa’ principles along with some of the ‘Vyakarana’ concepts used to develop the abstractive summarization system [23].

III. PROPOSED FUZZY NN TECHNIQUE

In the proposed technique, a Fuzzy logic as well as Neural Network is used to extract the informative words. In both the cases, the Neural Network is used to generate the abstract.

A. Preprocessing

Preprocessing is the filtering step which makes the document more suitable for further processing. It involves segmentation, stop word removal and stemming. In preprocessing initially the lexical analysis is done to treat various punctuation marks, symbols and type cases. Secondly the stop words, those having less semantic information, are eliminated. Eventually stemming is performed, which helps in grouping the similar words together. After preprocessing a fuzzy system is used to identify the informative words.

B. Informative word identification

When a person reads a document, unknowingly they keep on identifying some of the keywords (i.e. the informative words) in it. Identifying such informative contents is known as content selection strategy. The proposed approach uses neural network as well as fuzzy logic for this content selection.

1. Informative word detection based on a Fuzzy Logic System

A fuzzy logic system is used to identify the informative words in a sentence of a document. The inputs given to the fuzzy system are based on three functions of a word. The first function checks the words using Parts of Speech tagging based on Sanskrit Vyakaran (i.e. Paninian Grammar), which is a type of dependency grammar. The second function checks for the dependency patterns among the Subject-Verb-Object and some other variables as per the dependency grammar rules. The subject, verb and object are the most important variables to identify a sentence with informative words. According to Sanskrit Vyakarana rules, the verb is the connected to all entities in the sentences. Hence the sentence dependency structures are formed by keeping the verb at the head and subject and object at the branches. The variables used in the fuzzy logic system to identify the informative words in a sentence are the subject (f^{v1}), verb

(f^{v2}), object (f^{v3}), preposition (f^{v4}), numeric term (f^{v5}) and not a dictionary word (f^{v6}). Here the domain chosen for summarization is the news domain where numeric values play an important role. Therefore, the inclusion of numeric term variable would improve the precision of the abstract. The third function checks if it is a dictionary word. The ‘not a dictionary word’ is also an important variable because the names of most places will not be in the dictionary, and this variable also would improve the precision of the abstract. In the above conditions, the value ‘one’ represents that the sentence has the corresponding variable of the fuzzy logic system, and the value ‘zero’ indicates that the corresponding variable of the fuzzy logic system is absent in the sentence. Each sentence $\{s_1, s_2, s_3, \dots, s_b\}$, where $0 \leq b \leq B$, from each document $\{d_1, d_2, d_3, \dots, d_a\}$, where $0 \leq a \leq A$, is checked by the fuzzy logic system and assigned the corresponding values for the variables in it. The notation B gives the total number of sentences in the a^{th} document, and A indicates the total number of documents. If the words follow the SVO pattern of dependency grammar, corresponding values are assigned. Once the informative sentences are extracted the abstractive summary is generated from them. The abstractive summary is generated by concatenating the informative sentence that has the same verb and keeping the remaining informative sentences as it is. The abstractive summary generation is carried out as follows:

$$AS^a = \begin{cases} is_b^a \parallel is_{b+1}^a, & \text{if subject of } is_b^a = \text{subject of } is_{b+1}^a \\ \text{nothing}, & \text{else} \end{cases} \quad 1$$

In the above equation, AS^a is the abstractive summary of the a^{th} document. The abstract would consist of a number of informative abstractive sentences as shown below:

$$AS^a = \{SA_1^a, SA_2^a, SA_3^a, \dots, SA_c^a\} \text{ where, } 0 \leq c \leq C \quad 2$$

Here, SA_c^a represents the C^{th} informative abstractive sentence of the abstractive summary AS of the a^{th} document, and C indicates the total informative sentences in the abstractive summary. Similarly, the abstract is generated for all the other documents. Thereafter, the abstractive summaries of all the documents are given to the second-order filtering of abstractive summarization based on features.

2. Informative words identification by Neural Network

For the NN based approach, every document is represented in a form of matrix ‘M’ with a size $N \times P$ in which N represents the number of sentences in the document and P-1 represents the number of particular POS tags identified by the Paninian Vyakaran’s POS tagger. As discussed in fuzzy logic section, the weight-age is also given to ‘numeric’ terms and ‘not a dictionary word’ terms while POS tagging. The neural network is trained by applying the matrix of syntactic structure. The informative sentences then can be suggested by such syntactically trained neural network.

C. Second-order filtering of abstractive summarization based on features

After extracting the important words, the foremost task for the abstractive summaries is the sentence formation. The abstractive summary formed from each document is then presented for second-order filtering based on feature weights. The features taken for second-order filtering are the Purva and Uutar Memamsa Principles of traditional Sanskrit Shastras. This is done through a trained neural network. The ancient Sanskrit shastras are rich in grammar as well as text processing principles. These traditional Sanskrit Shastras are highly competent and have a rich capacity for the world of science. They are rich in math, psychology and logic. Thus, we must find a practical approach for these Sanskrit sciences. Some principles from Purva Memamsa and some from Uttar Memamsa are taken into account for the formation of meaningful sentences. The principles used are as follows:

Purva Memamsa Principles: Sthan, Prakaran, Samakhya.
And Uttar Memamsa Principle: Upkram - Upsanhar, Abhyas, Apurvata, Phalam

To be more specific in the summaries, the numerical value feature is also taken into account because the documents are news articles where the numbers have their own importance [24].

1. Prakaran

Prakarana is the one consistent meaning reached by a number of sentences meant to convey it, where all the sentences refer to this one idea. The Prakaran feature of an extracted document is calculated by comparing each sentence in the extracted document to the heading of that document. A check is performed to determine how many words match the title. A sentence that contains common words is ranked high.

2. Sthan

Sthana is the position reached in the discussion of a Prakarana. This feature is calculated as,

$$sthān = \frac{N-i+1}{N} * \frac{n-m+1}{n} \quad 3$$

Where N indicates the total number of paragraphs in the document and n indicates the number of sentences in the paragraph under consideration.

3. Samakhya

Samakhya means to reckon upon, consider. Many times, it is guessed that the related words co-appear together in a text, e.g., 'heavy rain', 'hot sun' etc. For calculation of this feature the information that is held in common is found out by calculating the number of words appearing together. The abhyasa feature (described in 3.3.5) is used to compute the weight of every 'samakhya'. Once the number of co appearing words are detected.

4. Upkram – Upsanhar

Upakrama are the beginning statements of the topic.
Upasamhara are the end or concluding statements of the topic.

There should be consistency in the initial and end statements of the summary. To achieve this, the Upkram Upsanhara features are evaluated together. If a word match is found in the corresponding sentences, it assigns a value of '1' for the sentence to the corresponding unique word; otherwise, it assigns '0.' A sample correlation matrix is shown below:

$$correlation\ matrix = \begin{bmatrix} 1 & r_{12} & r_{13} & r_{14} \\ r_{12} & 1 & r_{23} & r_{24} \\ r_{13} & r_{23} & 1 & r_{34} \\ r_{14} & r_{24} & r_{34} & 1 \end{bmatrix} \quad 4$$

The sentence correlation feature for each sentence is calculated for the extracted document using the correlation matrix. The sum of the first row and the sum of the first column are the same; therefore, the weight is the sum of each row or column of the matrix. The sum of each row or column represents the weight of the corresponding sentences. For example, the sum of the first row or column represents the weight of the first sentence of the extracted document.

5. Abhyasa

Abhyasa is repetition of the subject content several times in the same manner. The abhyasa calculates the weight of the sentence by comparing each word of a sentence with every word of the two neighboring sentences (the previous and next sentences) of the same extracted document.

6. Apurvata

Apurvata provides the uniqueness of the knowledge source. Every domain has a specific set of unique words associated with it. The sentences containing these domain-specific unique words are ranked high compared to other sentences.

$$Apurvata = \frac{UP_S}{UP_D} \quad 5$$

UP_D – Total number of cue-phrases in the document

UP_S – Number of cue-phrases in the sentence

7. Phalam

Phalam means the conclusion. The sentences containing the conclusive words like 'in conclusion', 'in a word', 'hence', 'briefly' etc. are important from the point view of the summary. The sentences containing such words are ranked high compared to other sentences.

8. Numerical data score

The domain selected for the summarization task at hand is the news domain. The important statistics in news articles are most often shown by numerical values within sentences. These data contribute to the selection of the sentence in the summary. The numerical data score is the ratio of data in numerical form to all of the numerical data in the sentence.

9. Summary generation

These features and the target summary of each document are given as inputs to train the neural network. For each cluster of documents, there is a target summary. Based on that target summary, the weight functions in the neural network are adjusted and the output is predicted. After training the neural network, the system is tested on a set of documents that contain the same information to generate a summary. The summary generation is same for both, Fuzzy-NN and NN-NN, approaches.

IV. RESULTS AND DISCUSSION

The Document Understanding Conference (DUC) datasets are the standard data sets that are used by the NLP researchers for evaluating summarization systems. The DUC 2002 dataset contains different sets of documents.

This section explains the evaluation measure and the performance of the proposed Fuzzy NN technique compared to some of the earlier techniques.

A. Evaluation Measure

To evaluate the performance, we used ROUGE scores. ROUGE stands for Recall-Oriented Understudy for Gisting Evaluation. ROUGE is used to measure the quality of an automatically generated summary by comparing it with a human-generated summary.

B. Performance Analysis

Performance of the proposed approach is compared with the NN-NN-based technique and the approach developed by [12]. The proposed approach uses a fuzzy logic system based on the Parts of Speech tagging of the ‘Paninian grammar’ for extraction of the informative word and based on the ‘Purva and Uttar Memamsa’ principles as features, the neural network forms the summary. The NN-NN-based technique uses the neural network for both the extraction of informative words and the formation of the summary. The performance is analyzed based on the DUC 2002 dataset and a real dataset.

C. Performance Comparison based on DUC 2002

This section shows a performance comparison using the DUC 2002 data set. Fig. 2 shows the ROUGE values obtained for the proposed technique, the NN-NN technique and the existing technique using five clusters for training and one cluster for testing on the DUC 2002 data set.

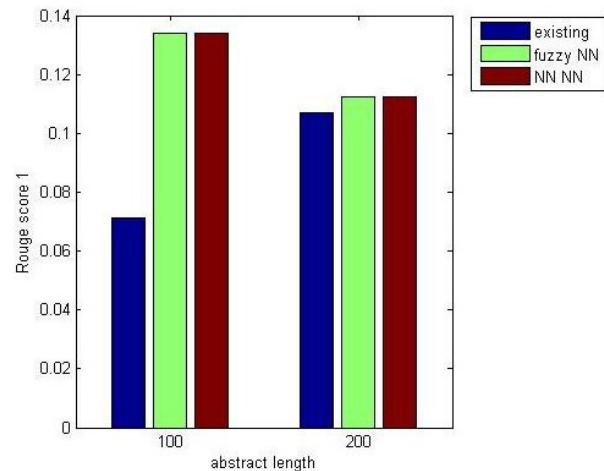


Fig. 1 Performance using DUC 2002 when training = 5 clusters and testing = 1 cluster

Fig. 1 shows the ROUGE score for a one-hundred-word-long abstract and a two-hundred-word-long abstract, i.e., the summary length is limited to one hundred and two hundred characters and five clusters are used for training and one cluster is used for testing. Here, for the one hundred length abstract, the ROUGE value using the existing technique is approximately 0.07 and the ROUGE values obtained using the proposed technique and the NN-NN technique is approximately 0.13. The ROUGE value for the two hundred length abstract using the existing technique is approximately 0.11, and it is approximately 0.12 using the proposed technique and the NN-NN technique. Overall, as shown in Fig. 1, the proposed technique and the technique using NN-NN are better than the existing technique.

D. Performance Comparison based on a real dataset

This section shows a performance comparison using a real dataset. The real dataset has 200 news articles and they are grouped in clusters each with 10 documents. Each cluster is associated with one summary developed by experts.

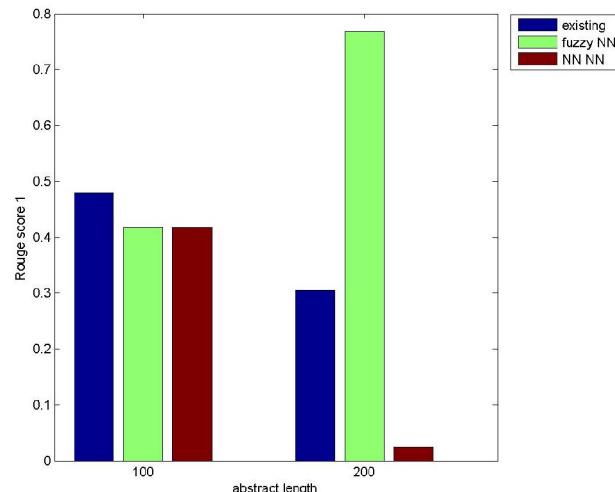


Fig. 2. Performance using a real dataset when training = 10 clusters and testing = 1 cluster

The ROUGE values shown in Fig. 2 were determined using the real dataset, and ten clusters are used for training and one cluster for testing. Here, the existing technique

performed better than the proposed technique, and the NN-NN technique based on a one hundred word length abstract. When the performance is checked based on a two hundred word length abstract, the proposed technique showed better performance than the other two techniques.

Fig. 3 shows the ROUGE-2 performance comparison when using the real dataset with fifteen clusters for training and one cluster for testing. Here, for both thresholds, the proposed technique and the NN-NN technique performed well compared to the existing technique.

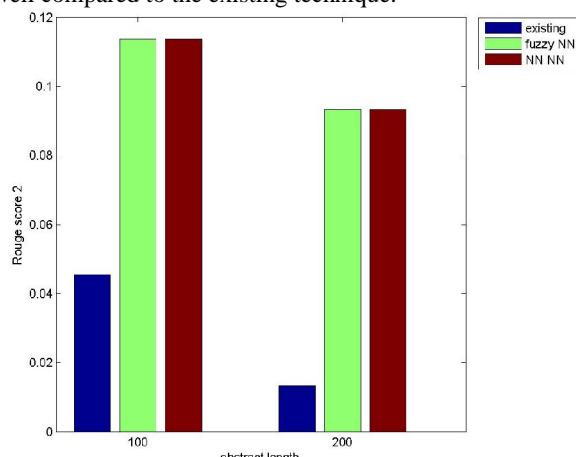


Fig. 3. ROUGE-2 performance using the real dataset when training = 15 clusters and testing = 1 cluster

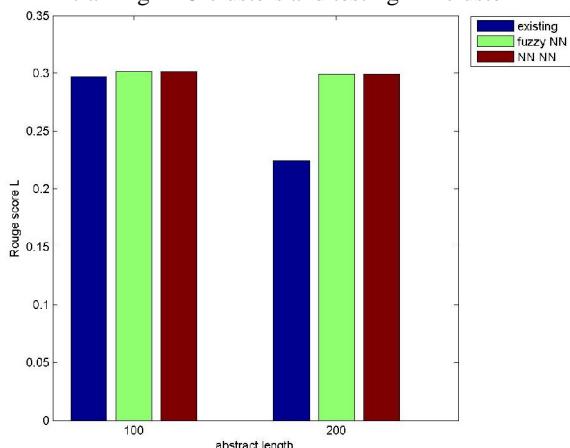


Fig. 4. ROUGE-L Performance using the real dataset when training = 15 clusters and testing = 1 cluster

Fig. 4 shows the ROUGE-L performance when using the real dataset with fifteen clusters for training and one cluster for testing. Here, the ROUGE-L performances of the proposed technique and the NN-NN approach are better than that of the existing approach.

Table 1, shows the ROUGE-1 and ROUGE-2 values of Fuzzy NN and NN-NN techniques consideration and compares them with [26]'s techniques using the DUC 2002 dataset.

TABLE 1 COMPARISON WITH OTHER TECHNIQUES

Techniques		Average Rouge-1 Value	Average Rouge-2 Value
Fuzzy-NN	100 length	0.23404	0.08163
	200 length	0.19277	0.06451
NN-NN	100 length	0.23404	0.08163

	200 length	0. 19277	0.06451
[26] (Abstractive Approach)	Baseline	0.1515	0.0308
	Opniosis	0.2831	0.0853

In Table 1, the ROUGE values for the FUZZY NN and NN-NN techniques are determined based on one hundred word length and two hundred word length abstracts using twenty clusters for training and one cluster for testing. As the limited work exists in abstractive summarization, the natural baseline is not used for comparison. Therefore the baseline used is a state of the art extractive method in [6].

TABLE 2.COMPARISON OF PROPOSED FUZZY NN APPROACH WITH THE TECHNIQUES USED IN

Techniques	Precision	Recall	F-measure
Fuzzy-NN (abstractive Approach)	0.72	0.71	0.72
(Extractive Approach)[6]	0.37	0.86	0.5

The comparison shows that the proposed approach gives a better F-measure than the Deep learning approach.

V. CONCLUSION

The system-generated summaries are compared with the human-generated summary via ROUGE measurement using the DUC 2002 data set and a real dataset. Using the DUC data set and comparing the performances using one-hundred-length and two-hundred-length abstracts, the proposed technique and the NN-NN technique showed the same performance, which is better than that of the existing technique. When comparing the performance of the proposed approach with two different classifiers such as neural network and fuzzy, the results are not varied significantly when the DUC data set is used. This is an additional advantage of the proposed approach that the performance of the proposed approach for text summarization is independent of the classifier taken and also, the proposed approach performs well for both the classifiers.

However when the Real dataset is used, where the text is not much structured, the Fuzzy NN approach performs better than an existing approach in[25] as well as NN-NN approach when the compression rate is low i.e. abstract length is more and lesser ROUGE scores are considered.

The comparison of the proposed technique with [26] shows that proposed approach gives the considerable values of ROUGE Scores. Hence it can be implemented for abstractive summarization. However deeper analysis of 'Memamsa' principles may give the better results.

LIST OF ABBREVIATIONS

1. NN- Neural Network
2. NLP- Natural Language Processing
3. DUC-Document Understanding Conference
4. ROUGE- Recall Oriented Understudy for Gisting Evaluation

COMPETING INTERESTS

The authors declare that they have no competing interests.

ACKNOWLEDGEMENT

The authors would like to thank ‘Bharati Veedyapeeth Deemed University’s College of Engineering,’ Pune, Maharashtra, India for all the support extended while carrying out the research work. The authors also would like to acknowledge DUC, “<http://www.nlpirc.nist.gov/projects/duc/guidelines.html>,” for the copyright-free online text documents databases.

REFERENCES

1. Yih Wen-tau, Joshua Goodman, Vanderwende Lucy and Suzuki Hisami, (2007), " Multi-Document Summarization by Maximizing Informative Content-Words", International joint conference on Artificial intelligence, Vol. 6(12), pp.1776-1782.
2. Sarkar Kamal, "Sentence Clustering-based Summarization of Multiple Text Documents", (2009), International Journal of Computing Science and Communication Technologies, Vol. 2 (1), pp. 325-335.
3. Foong Oi Mean, Oxley Alan , Sulaiman Suziah, "Challenges and Trends of Automatic Text Summarization", (2010), International Jproposednal of Information and Telecommunication Tech nology, Vol.1 (1), pp.34-39.
4. Shinde Rajesh D., Routela Suraj H., Jadhav Savita S., Sagare Smita R., "Enforcing Text Summarization using Fuzzy Logic ", (2014), International Journal of Computer Science and Information Technologies, Vol. 5 (6), pp. 8276-8279.
5. Dixit Rucha S., Apte S. S., "Improvement of Text Summarization using Fuzzy Logic Based Method", (2012), IOSR Journal of Computer Engineering, Vol. 5 (6), pp. 05-10.
6. G.Padmapriya, K.Duraiswam, "Association Of Deep Learning Algorithm With Fuzzy Logic For Multidocument Text Summarization", (2014).Journal of Theoretical and Applied Information Technology, Vol. 62(1), pp.167-173.
7. Megala S. Santhana ,A. Kavitha, A. Marimuthu "Enriching Text Summarization using Fuzzy Logic", (2014),International Journal of Computer Science and Information Technologies, Vol. 5 (1) , pp. 863-867.
8. Cheung Jackie Chi Kit, Penn Gerald, "To-wards robust abstractive multi-document summarization: A case frame analysis of centrality and domain", (2013), In Proceedings of the 51st Annual Meeting of the Association for Computational Linguistics, pp.1233–1242.
9. Genest Pierre Etienne, Lapalme Guy, "Fully Abstractive Approach to Guided Summarization", (2012), Meeting of the Association for Computational Linguistics, Vol.2, pp. 354–358.
10. Thadani Kapil and McKeown Kathleen, "Supervised sentence fusion with single-stage inference", (2013),In Proceedings of the Sixth International Joint Conference on Natural Language Processing, pp. 1410–1418.
11. Elsner Micha ,Santhanam Deepak, "Learning to fuse disparate sentences ",(2011), In Proceedings of the Workshop on Monolingual Text-To-Text Generation, Association for Computational Linguistics, pp. 54–63
12. Lloret Elena and Paloma Manuel, "Analyzing the Use of Word Graphs for Abstractive Text Summarization", (2011), Advances in Information Mining and Management, Vol.1 (5), pp.61-66.
13. Genest Pierre Etienne, Lapalme Guy, "Fully Abstractive Approach to Guided Summarization", (2012), Meeting of the Association for Computational Linguistics, Vol.2, pp. 354–358.
14. Carenini Giuseppe, Cheung Jackie Chi Kit, "Extractive vs. NLG-based Abstractive Summarization of Evaluative Text: The Effect of Corpus Controversiality", (2008), International Natural Language Generation Conference, Vol. 52(11), pp.33-41.
15. Liu Fei, Liu Yang, "From Extractive to Abstractive Meeting Summaries: Can It Be Done by Sentence Compression", (2009), Association for Computational Linguistics, Vol. 3(1), pp.261-264.
16. Long Chong, Huang Minlie, Zhu Xiaoyan, Li Ming, " Multi-Document Summarization by Information Distance", (2009),IEEE International Conference on Data Mining, Vol.5(2), pp.866-871.
17. Honarpisheh Mohamad Ali, Ghassem Gholamreza, Mirroshandel Sani Ghassem, "A Multi-Document Multilingual Automatic Summarization System", (2009), ACM SIGIR Conference on Research and Development in Information Retrieval, Vol. 2 (4), pp. 735-739.
18. Ji Heng, Favre Benoit, Pin Lin Wen, "Open-domain Multi-Document Summarization via Information Extraction: Challenges and Prospects", (2013), Theory and applications of natural language, Vol. 1 (9), pp. 177-183.
19. Gupta Vikrant, Chauhan Priya, Garg Sohan, "A Statistical Tool for Multi-Document Summarization", (2012), International Journal of Scientific and Research Publications, Vol. 2 (5), pp. 1-5.
20. Genest Pierre Etienne, Lapalme Guy, "Framework for Abstractive Summarization using Text-to-Text Generation", (2011), Workshop on Monolingual Text-To-Text Generation, Vol.23 (9), pp. 64–73.
21. Lin C.Y., "ROUGE: a package for automatic evaluation of summaries," (2004), in Proceedings of ACL Text Summarization Workshop, pp.74–81
22. Saxena Shashank, Agrawal Raghav, "Sanskrit as a Programming Language and Natural Language Processing", (2013), Global Journal of Management and Business Studies, Vol. 3 (10), pp. 1135-1142.
23. Phil Thibaut G., "The Arthsamgraha - An Elementary Treatise on Mimamsa", (1882), Banaras printing press.
24. Yong S. P., Abidin A. I. Z. & Chen Y. Y., "A neural-based text summarization system", (2006), WIT Transactions on Information and Communication Technologies, Vol. 37, pp. 185-196.
25. Prasad Rajesh S., Kulkarni U. V., Prasad Jayashree. R., "Connectionist Approach to Generic Text Summarization", (2009), In proceeding of 3rd International Conference on Anti-counterfeiting, Security, and Identification in Communication, DOI: 10.1109/ICASID, pp. 606-610.
26. Ganeshan Kavita, Zhai Cheng Xiang, Han Jiawei "Opnosis: A Graph-Based Approach to Abstractive Summarization of Highly Redundant Opinions", (2010), In Proceeding of the 23rd International Conference on Computational Linguistics, pp. 340–348.
27. DUC, "<http://www.nlpirc.nist.gov/projects/duc/guidelines.html>."

AUTHOR'S PROFILE

The corresponding author of this manuscript is D.Y.Sakhare. She is currently pursuing a PhD at Bharativedyapeeth Deemed University's College of Engineering, Pune,MS,India. Currently, she is also associated with the MIT Academy of Engineering, Alandi, Pune, MS, India, as an Assistant Professor.

The second contributing author, Rajkumar, is a PhD supervisor and is associated with DIAT, Khadakwasala Pune, MS, India as a Professor

IJCSIS REVIEWERS' LIST

- Assist Prof (Dr.) M. Emre Celebi, Louisiana State University in Shreveport, USA
Dr. Lam Hong Lee, Universiti Tunku Abdul Rahman, Malaysia
Dr. Shimon K. Modi, Director of Research BSPA Labs, Purdue University, USA
Dr. Jianguo Ding, Norwegian University of Science and Technology (NTNU), Norway
Assoc. Prof. N. Jaisankar, VIT University, Vellore, Tamilnadu, India
Dr. Amogh Kavimandan, The Mathworks Inc., USA
Dr. Ramasamy Mariappan, Vinayaka Missions University, India
Dr. Yong Li, School of Electronic and Information Engineering, Beijing Jiaotong University, P.R. China
Assist. Prof. Sugam Sharma, NIET, India / Iowa State University, USA
Dr. Jorge A. Ruiz-Vanoye, Universidad Autónoma del Estado de Morelos, Mexico
Dr. Neeraj Kumar, SMVD University, Katra (J&K), India
Dr Genge Bela, "Petru Maior" University of Targu Mures, Romania
Dr. Junjie Peng, Shanghai University, P. R. China
Dr. Ilhem LENGLIZ, HANA Group - CRISTAL Laboratory, Tunisia
Prof. Dr. Durgesh Kumar Mishra, Acropolis Institute of Technology and Research, Indore, MP, India
Dr. Jorge L. Hernández-Ardieta, University Carlos III of Madrid, Spain
Prof. Dr.C.Suresh Gnana Dhas, Anna University, India
Dr Li Fang, Nanyang Technological University, Singapore
Prof. Pijush Biswas, RCC Institute of Information Technology, India
Dr. Siddhivinayak Kulkarni, University of Ballarat, Ballarat, Victoria, Australia
Dr. A. Arul Lawrence, Royal College of Engineering & Technology, India
Dr. Wongyos Keardsri, Chulalongkorn University, Bangkok, Thailand
Dr. Somesh Kumar Dewangan, CCSVTU Bhilai (C.G.)/ Dimat Raipur, India
Dr. Hayder N. Jasem, University Putra Malaysia, Malaysia
Dr. A.V.Senthil Kumar, C. M. S. College of Science and Commerce, India
Dr. R. S. Karthik, C. M. S. College of Science and Commerce, India
Dr. P. Vasant, University Technology Petronas, Malaysia
Dr. Wong Kok Seng, Soongsil University, Seoul, South Korea
Dr. Praveen Ranjan Srivastava, BITS PILANI, India
Dr. Kong Sang Kelvin, Leong, The Hong Kong Polytechnic University, Hong Kong
Dr. Mohd Nazri Ismail, Universiti Kuala Lumpur, Malaysia
Dr. Rami J. Matarneh, Al-isra Private University, Amman, Jordan
Dr Ojesanmi Olusegun Ayodeji, Ajayi Crowther University, Oyo, Nigeria
Dr. Riktesh Srivastava, Skyline University, UAE
Dr. Oras F. Baker, UCSI University - Kuala Lumpur, Malaysia
Dr. Ahmed S. Ghiduk, Faculty of Science, Beni-Suef University, Egypt
and Department of Computer science, Taif University, Saudi Arabia
Dr. Tirthankar Gayen, IIT Kharagpur, India
Dr. Huei-Ru Tseng, National Chiao Tung University, Taiwan
Prof. Ning Xu, Wuhan University of Technology, China
Dr Mohammed Salem Binwahlan, Hadhramout University of Science and Technology, Yemen
& Universiti Teknologi Malaysia, Malaysia.
Dr. Aruna Ranganath, Bhoj Reddy Engineering College for Women, India
Dr. Hafeezullah Amin, Institute of Information Technology, KUST, Kohat, Pakistan

Prof. Syed S. Rizvi, University of Bridgeport, USA
Dr. Shahbaz Pervez Chattha, University of Engineering and Technology Taxila, Pakistan
Dr. Shishir Kumar, Jaypee University of Information Technology, Wakanaghata (HP), India
Dr. Shahid Mumtaz, Portugal Telecommunication, Instituto de Telecomunicações (IT) , Aveiro, Portugal
Dr. Rajesh K Shukla, Corporate Institute of Science & Technology Bhopal M P
Dr. Poonam Garg, Institute of Management Technology, India
Dr. S. Mehta, Inha University, Korea
Dr. Dilip Kumar S.M, Bangalore University, Bangalore
Prof. Malik Sikander Hayat Khiyal, Fatima Jinnah Women University, Rawalpindi, Pakistan
Dr. Virendra Gomase , Department of Bioinformatics, Padmashree Dr. D.Y. Patil University
Dr. Irraivan Elamvazuthi, University Technology PETRONAS, Malaysia
Dr. Saqib Saeed, University of Siegen, Germany
Dr. Pavan Kumar Gorakavi, IPMA-USA [YC]
Dr. Ahmed Nabih Zaki Rashed, Menoufia University, Egypt
Prof. Shishir K. Shandilya, Rukmani Devi Institute of Science & Technology, India
Dr. J. Komala Lakshmi, SNR Sons College, Computer Science, India
Dr. Muhammad Sohail, KUST, Pakistan
Dr. Manjaiah D.H, Mangalore University, India
Dr. S Santhosh Baboo, D.G.Vaishnav College, Chennai, India
Prof. Dr. Mokhtar Beldjehem, Sainte-Anne University, Halifax, NS, Canada
Dr. Deepak Laxmi Narasimha, University of Malaya, Malaysia
Prof. Dr. Arunkumar Thangavelu, Vellore Institute Of Technology, India
Dr. M. Azath, Anna University, India
Dr. Md. Rabiul Islam, Rajshahi University of Engineering & Technology (RUET), Bangladesh
Dr. Aos Alaa Zaidan Ansaef, Multimedia University, Malaysia
Dr Suresh Jain, Devi Ahilya University, Indore (MP) India,
Dr. Mohammed M. Kadhum, Universiti Utara Malaysia
Dr. Hanumanthappa. J. University of Mysore, India
Dr. Syed Ishtiaque Ahmed, Bangladesh University of Engineering and Technology (BUET)
Dr Akinola Solomon Olalekan, University of Ibadan, Ibadan, Nigeria
Dr. Santosh K. Pandey, The Institute of Chartered Accountants of India
Dr. P. Vasant, Power Control Optimization, Malaysia
Dr. Petr Ivankov, Automatika - S, Russian Federation
Dr. Utkarsh Seetha, Data Infosys Limited, India
Mrs. Priti Maheshwary, Maulana Azad National Institute of Technology, Bhopal
Dr. (Mrs) Padmavathi Ganapathi, Avinashilingam University for Women, Coimbatore
Assist. Prof. A. Neela madheswari, Anna university, India
Prof. Ganesan Ramachandra Rao, PSG College of Arts and Science, India
Mr. Kamanashis Biswas, Daffodil International University, Bangladesh
Dr. Atul Gonsai, Saurashtra University, Gujarat, India
Mr. Angkoon Phinyomark, Prince of Songkla University, Thailand
Mrs. G. Nalini Priya, Anna University, Chennai
Dr. P. Subashini, Avinashilingam University for Women, India
Assoc. Prof. Vijay Kumar Chakka, Dhirubhai Ambani IICT, Gandhinagar ,Gujarat
Mr Jitendra Agrawal, : Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal
Mr. Vishal Goyal, Department of Computer Science, Punjabi University, India
Dr. R. Baskaran, Department of Computer Science and Engineering, Anna University, Chennai

Assist. Prof, Kanwalvir Singh Dhindsa, B.B.S.B.Engg. College, Fatehgarh Sahib (Punjab), India
Dr. Jamal Ahmad Dargham, School of Engineering and Information Technology, Universiti Malaysia Sabah
Mr. Nitin Bhatia, DAV College, India
Dr. Dhavachelvan Ponnurangam, Pondicherry Central University, India
Dr. Mohd Faizal Abdollah, University of Technical Malaysia, Malaysia
Assist. Prof. Sonal Chawla, Panjab University, India
Dr. Abdul Wahid, AKG Engg. College, Ghaziabad, India
Mr. Arash Habibi Lashkari, University of Malaya (UM), Malaysia
Mr. Md. Rajibul Islam, Ibnu Sina Institute, University Technology Malaysia
Professor Dr. Sabu M. Thampi, .B.S Institute of Technology for Women, Kerala University, India
Mr. Noor Muhammed Nayeem, Université Lumière Lyon 2, 69007 Lyon, France
Dr. Himanshu Aggarwal, Department of Computer Engineering, Punjabi University, India
Prof R. Naidoo, Dept of Mathematics/Center for Advanced Computer Modelling, Durban University of Technology, Durban, South Africa
Prof. Mydhili K Nair, Visweswaraiah Technological University, Bangalore, India
M. Prabu, Adhiyamaan College of Engineering/Anna University, India
Mr. Swakkhar Shatabda, United International University, Bangladesh
Dr. Abdur Rashid Khan, ICIT, Gomal University, Dera Ismail Khan, Pakistan
Mr. H. Abdul Shabeer, I-Nautix Technologies, Chennai, India
Dr. M. Aramudhan, Perunthalaivar Kamarajar Institute of Engineering and Technology, India
Dr. M. P. Thapliyal, Department of Computer Science, HNB Garhwal University (Central University), India
Dr. Shahaboddin Shamshirband, Islamic Azad University, Iran
Mr. Zeashan Hameed Khan, Université de Grenoble, France
Prof. Anil K Ahlawat, Ajay Kumar Garg Engineering College, Ghaziabad, UP Technical University, Lucknow
Mr. Longe Olumide Babatope, University Of Ibadan, Nigeria
Associate Prof. Raman Maini, University College of Engineering, Punjabi University, India
Dr. Maslin Masrom, University Technology Malaysia, Malaysia
Sudipta Chattopadhyay, Jadavpur University, Kolkata, India
Dr. Dang Tuan NGUYEN, University of Information Technology, Vietnam National University - Ho Chi Minh City
Dr. Mary Lourde R., BITS-PILANI Dubai, UAE
Dr. Abdul Aziz, University of Central Punjab, Pakistan
Mr. Karan Singh, Gautam Budtha University, India
Mr. Avinash Pokhriyal, Uttar Pradesh Technical University, Lucknow, India
Associate Prof Dr Zuraini Ismail, University Technology Malaysia, Malaysia
Assistant Prof. Yasser M. Alginahi, Taibah University, Madinah Munawwarah, KSA
Mr. Dakshina Ranjan Kisku, West Bengal University of Technology, India
Mr. Raman Kumar, Dr B R Ambedkar National Institute of Technology, Jalandhar, Punjab, India
Associate Prof. Samir B. Patel, Institute of Technology, Nirma University, India
Dr. M. Munir Ahmed Rabbani, B. S. Abdur Rahman University, India
Asst. Prof. Koushik Majumder, West Bengal University of Technology, India
Dr. Alex Pappachen James, Queensland Micro-nanotechnology center, Griffith University, Australia
Assistant Prof. S. Hariharan, B.S. Abdur Rahman University, India
Asst Prof. Jasmine. K. S, R.V. College of Engineering, India
Mr Naushad Ali Mamode Khan, Ministry of Education and Human Resources, Mauritius
Prof. Mahesh Goyani, G H Patel College of Engg. & Tech, V.V.N. Anand, Gujarat, India
Dr. Mana Mohammed, University of Tlemcen, Algeria
Prof. Jatinder Singh, Universal Institution of Engg. & Tech. CHD, India

Mrs. M. Anandhavalli Gauthaman, Sikkim Manipal Institute of Technology, Majitar, East Sikkim
Dr. Bin Guo, Institute Telecom SudParis, France
Mrs. Maleika Mehr Nigar Mohamed Heenaye-Mamode Khan, University of Mauritius
Prof. Pijush Biswas, RCC Institute of Information Technology, India
Mr. V. Bala Dhandayuthapani, Mekelle University, Ethiopia
Dr. Irfan Syamsuddin, State Polytechnic of Ujung Pandang, Indonesia
Mr. Kavi Kumar Khedo, University of Mauritius, Mauritius
Mr. Ravi Chandiran, Zagro Singapore Pte Ltd. Singapore
Mr. Milindkumar V. Sarode, Jawaharlal Darda Institute of Engineering and Technology, India
Dr. Shamimul Qamar, KSJ Institute of Engineering & Technology, India
Dr. C. Arun, Anna University, India
Assist. Prof. M.N.Birje, Basaveshwar Engineering College, India
Prof. Hamid Reza Naji, Department of Computer Enigneering, Shahid Beheshti University, Tehran, Iran
Assist. Prof. Debasis Giri, Department of Computer Science and Engineering, Haldia Institute of Technology
Subhabrata Barman, Haldia Institute of Technology, West Bengal
Mr. M. I. Lali, COMSATS Institute of Information Technology, Islamabad, Pakistan
Dr. Feroz Khan, Central Institute of Medicinal and Aromatic Plants, Lucknow, India
Mr. R. Nagendran, Institute of Technology, Coimbatore, Tamilnadu, India
Mr. Amnach Khawne, King Mongkut's Institute of Technology Ladkrabang, Ladkrabang, Bangkok, Thailand
Dr. P. Chakrabarti, Sir Padampat Singhania University, Udaipur, India
Mr. Nafiz Imtiaz Bin Hamid, Islamic University of Technology (IUT), Bangladesh.
Shahab-A. Shamshirband, Islamic Azad University, Chalous, Iran
Prof. B. Priestly Shan, Anna Univeristy, Tamilnadu, India
Venkatramreddy Velma, Dept. of Bioinformatics, University of Mississippi Medical Center, Jackson MS USA
Akshi Kumar, Dept. of Computer Engineering, Delhi Technological University, India
Dr. Umesh Kumar Singh, Vikram University, Ujjain, India
Mr. Serguei A. Mokhov, Concordia University, Canada
Mr. Lai Khin Wee, Universiti Teknologi Malaysia, Malaysia
Dr. Awadhesh Kumar Sharma, Madan Mohan Malviya Engineering College, India
Mr. Syed R. Rizvi, Analytical Services & Materials, Inc., USA
Dr. S. Karthik, SNS Collegeof Technology, India
Mr. Syed Qasim Bukhari, CIMET (Universidad de Granada), Spain
Mr. A.D.Potgantwar, Pune University, India
Dr. Himanshu Aggarwal, Punjabi University, India
Mr. Rajesh Ramachandran, Naipunya Institute of Management and Information Technology, India
Dr. K.L. Shunmuganathan, R.M.K Engg College , Kavaraipettai ,Chennai
Dr. Prasant Kumar Pattnaik, KIST, India.
Dr. Ch. Aswani Kumar, VIT University, India
Mr. Ijaz Ali Shoukat, King Saud University, Riyadh KSA
Mr. Arun Kumar, Sir Padam Pat Singhania University, Udaipur, Rajasthan
Mr. Muhammad Imran Khan, Universiti Teknologi PETRONAS, Malaysia
Dr. Natarajan Meghanathan, Jackson State University, Jackson, MS, USA
Mr. Mohd Zaki Bin Mas'ud, Universiti Teknikal Malaysia Melaka (UTeM), Malaysia
Prof. Dr. R. Geetharamani, Dept. of Computer Science and Eng., Rajalakshmi Engineering College, India
Dr. Smita Rajpal, Institute of Technology and Management, Gurgaon, India
Dr. S. Abdul Khader Jilani, University of Tabuk, Tabuk, Saudi Arabia
Mr. Syed Jamal Haider Zaidi, Bahria University, Pakistan

Dr. N. Devarajan, Government College of Technology, Coimbatore, Tamilnadu, INDIA
Mr. R. Jagadeesh Kannan, RMK Engineering College, India
Mr. Deo Prakash, Shri Mata Vaishno Devi University, India
Mr. Mohammad Abu Naser, Dept. of EEE, IUT, Gazipur, Bangladesh
Assist. Prof. Prasun Ghosal, Bengal Engineering and Science University, India
Mr. Md. Golam Kaosar, School of Engineering and Science, Victoria University, Melbourne City, Australia
Mr. R. Mohammad Shafi, Madanapalle Institute of Technology & Science, India
Dr. F.Sagayaraj Francis, Pondicherry Engineering College, India
Dr. Ajay Goel, HIET, Kaithal, India
Mr. Nayak Sunil Kashibarao, Bahirji Smarak Mahavidyalaya, India
Mr. Suhas J Manangi, Microsoft India
Dr. Kalyankar N. V., Yeshwant Mahavidyalaya, Nanded, India
Dr. K.D. Verma, S.V. College of Post graduate studies & Research, India
Dr. Amjad Rehman, University Technology Malaysia, Malaysia
Mr. Rachit Garg, L K College, Jalandhar, Punjab
Mr. J. William, M.A.M college of Engineering, Trichy, Tamilnadu, India
Prof. Jue-Sam Chou, Nanhua University, College of Science and Technology, Taiwan
Dr. Thorat S.B., Institute of Technology and Management, India
Mr. Ajay Prasad, Sir Padampat Singhania University, Udaipur, India
Dr. Kamaljit I. Lakhtaria, Atmiya Institute of Technology & Science, India
Mr. Syed Raifiul Hussain, Ahsanullah University of Science and Technology, Bangladesh
Mrs Fazeela Tunnis, Najran University, Kingdom of Saudi Arabia
Mrs Kavita Taneja, Maharishi Markandeshwar University, Haryana, India
Mr. Maniyar Shiraz Ahmed, Najran University, Najran, KSA
Mr. Anand Kumar, AMC Engineering College, Bangalore
Dr. Rakesh Chandra Gangwar, Beant College of Engg. & Tech., Gurdaspur (Punjab) India
Dr. V V Rama Prasad, Sree Vidyanikethan Engineering College, India
Assist. Prof. Neetesh Kumar Gupta, Technocrats Institute of Technology, Bhopal (M.P.), India
Mr. Ashish Seth, Uttar Pradesh Technical University, Lucknow, UP India
Dr. V V S S Balaram, Sreenidhi Institute of Science and Technology, India
Mr Rahul Bhatia, Lingaya's Institute of Management and Technology, India
Prof. Niranjana Reddy. P, KITS, Warangal, India
Prof. Rakesh. Lingappa, Vijetha Institute of Technology, Bangalore, India
Dr. Mohammed Ali Hussain, Nimra College of Engineering & Technology, Vijayawada, A.P., India
Dr. A. Srinivasan, MNM Jain Engineering College, Rajiv Gandhi Salai, Thorapakkam, Chennai
Mr. Rakesh Kumar, M.M. University, Mullana, Ambala, India
Dr. Lena Khaled, Zarqa Private University, Aman, Jordan
Ms. Supriya Kapoor, Patni/Lingaya's Institute of Management and Tech., India
Dr. Tossapon Boongoen, Aberystwyth University, UK
Dr. Bilal Alatas, Firat University, Turkey
Assist. Prof. Jyoti Praaksh Singh, Academy of Technology, India
Dr. Ritu Soni, GNG College, India
Dr. Mahendra Kumar, Sagar Institute of Research & Technology, Bhopal, India.
Dr. Binod Kumar, Lakshmi Narayan College of Tech.(LNCT)Bhopal India
Dr. Muzhir Shaban Al-Ani, Amman Arab University Amman – Jordan
Dr. T.C. Manjunath, ATRIA Institute of Tech, India
Mr. Muhammad Zakarya, COMSATS Institute of Information Technology (CIIT), Pakistan

Assist. Prof. Harmunish Taneja, M. M. University, India
Dr. Chitra Dhawale , SICSR, Model Colony, Pune, India
Mrs Sankari Muthukaruppan, Nehru Institute of Engineering and Technology, Anna University, India
Mr. Aaqif Afzaal Abbasi, National University Of Sciences And Technology, Islamabad
Prof. Ashutosh Kumar Dubey, Trinity Institute of Technology and Research Bhopal, India
Mr. G. Appasami, Dr. Pauls Engineering College, India
Mr. M Yasin, National University of Science and Tech, karachi (NUST), Pakistan
Mr. Yaser Miaji, University Utara Malaysia, Malaysia
Mr. Shah Ahsanul Haque, International Islamic University Chittagong (IIUC), Bangladesh
Prof. (Dr) Syed Abdul Sattar, Royal Institute of Technology & Science, India
Dr. S. Sasikumar, Roever Engineering College
Assist. Prof. Monit Kapoor, Maharishi Markandeshwar University, India
Mr. Nwaocha Vivian O, National Open University of Nigeria
Dr. M. S. Vijaya, GR Govindarajulu School of Applied Computer Technology, India
Assist. Prof. Chakresh Kumar, Manav Rachna International University, India
Mr. Kunal Chadha , R&D Software Engineer, Gemalto, Singapore
Mr. Mueen Uddin, Universiti Teknologi Malaysia, UTM , Malaysia
Dr. Dhuha Basheer abdullah, Mosul university, Iraq
Mr. S. Audithan, Annamalai University, India
Prof. Vijay K Chaudhari, Technocrats Institute of Technology , India
Associate Prof. Mohd Ilyas Khan, Technocrats Institute of Technology , India
Dr. Vu Thanh Nguyen, University of Information Technology, HoChiMinh City, VietNam
Assist. Prof. Anand Sharma, MITS, Lakshmangarh, Sikar, Rajasthan, India
Prof. T V Narayana Rao, HITAM Engineering college, Hyderabad
Mr. Deepak Gour, Sir Padampat Singhania University, India
Assist. Prof. Amutharaj Joyson, Kalasalingam University, India
Mr. Ali Balador, Islamic Azad University, Iran
Mr. Mohit Jain, Maharaja Surajmal Institute of Technology, India
Mr. Dilip Kumar Sharma, GLA Institute of Technology & Management, India
Dr. Debojyoti Mitra, Sir padampat Singhania University, India
Dr. Ali Dehghantanha, Asia-Pacific University College of Technology and Innovation, Malaysia
Mr. Zhao Zhang, City University of Hong Kong, China
Prof. S.P. Setty, A.U. College of Engineering, India
Prof. Patel Rakeshkumar Kantilal, Sankalchand Patel College of Engineering, India
Mr. Biswajit Bhowmik, Bengal College of Engineering & Technology, India
Mr. Manoj Gupta, Apex Institute of Engineering & Technology, India
Assist. Prof. Ajay Sharma, Raj Kumar Goel Institute Of Technology, India
Assist. Prof. Ramveer Singh, Raj Kumar Goel Institute of Technology, India
Dr. Hanan Elazhary, Electronics Research Institute, Egypt
Dr. Hosam I. Faiq, USM, Malaysia
Prof. Dipti D. Patil, MAEER's MIT College of Engg. & Tech, Pune, India
Assist. Prof. Devendra Chack, BCT Kumaon engineering College Dwarahat Almora, India
Prof. Manpreet Singh, M. M. Engg. College, M. M. University, India
Assist. Prof. M. Sadiq ali Khan, University of Karachi, Pakistan
Mr. Prasad S. Halgaonkar, MIT - College of Engineering, Pune, India
Dr. Imran Ghani, Universiti Teknologi Malaysia, Malaysia
Prof. Varun Kumar Kakar, Kumaon Engineering College, Dwarahat, India

Assist. Prof. Nisheeth Joshi, Apaji Institute, Banasthali University, Rajasthan, India
Associate Prof. Kunwar S. Vaisla, VCT Kumaon Engineering College, India
Prof Anupam Choudhary, Bhilai School Of Engg.,Bhilai (C.G.),India
Mr. Divya Prakash Shrivastava, Al Jabal Al garbi University, Zawya, Libya
Associate Prof. Dr. V. Radha, Avinashilingam Deemed university for women, Coimbatore.
Dr. Kasarapu Ramani, JNT University, Anantapur, India
Dr. Anuraag Awasthi, Jayoti Vidyapeeth Womens University, India
Dr. C G Ravichandran, R V S College of Engineering and Technology, India
Dr. Mohamed A. Deriche, King Fahd University of Petroleum and Minerals, Saudi Arabia
Mr. Abbas Karimi, Universiti Putra Malaysia, Malaysia
Mr. Amit Kumar, Jaypee University of Engg. and Tech., India
Dr. Nikolai Stoianov, Defense Institute, Bulgaria
Assist. Prof. S. Ranichandra, KSR College of Arts and Science, Tiruchencode
Mr. T.K.P. Rajagopal, Diamond Horse International Pvt Ltd, India
Dr. Md. Ekramul Hamid, Rajshahi University, Bangladesh
Mr. Hemanta Kumar Kalita , TATA Consultancy Services (TCS), India
Dr. Messaouda Azzouzi, Ziane Achour University of Djelfa, Algeria
Prof. (Dr.) Juan Jose Martinez Castillo, "Gran Mariscal de Ayacucho" University and Acantelys research Group, Venezuela
Dr. Jatinderkumar R. Saini, Narmada College of Computer Application, India
Dr. Babak Bashari Rad, University Technology of Malaysia, Malaysia
Dr. Nighat Mir, Effat University, Saudi Arabia
Prof. (Dr.) G.M.Nasira, Sasurie College of Engineering, India
Mr. Varun Mittal, Gemalto Pte Ltd, Singapore
Assist. Prof. Mrs P. Banumathi, Kathir College Of Engineering, Coimbatore
Assist. Prof. Quan Yuan, University of Wisconsin-Stevens Point, US
Dr. Pranam Paul, Narula Institute of Technology, Agarpara, West Bengal, India
Assist. Prof. J. Ramkumar, V.L.B Janakiammal college of Arts & Science, India
Mr. P. Sivakumar, Anna university, Chennai, India
Mr. Md. Humayun Kabir Biswas, King Khalid University, Kingdom of Saudi Arabia
Mr. Mayank Singh, J.P. Institute of Engg & Technology, Meerut, India
HJ. Kamaruzaman Jusoff, Universiti Putra Malaysia
Mr. Nikhil Patrick Lobo, CADES, India
Dr. Amit Wason, Rayat-Bahra Institute of Engineering & Boi-Technology, India
Dr. Rajesh Shrivastava, Govt. Benazir Science & Commerce College, Bhopal, India
Assist. Prof. Vishal Bharti, DCE, Gurgaon
Mrs. Sunita Bansal, Birla Institute of Technology & Science, India
Dr. R. Sudhakar, Dr.Mahalingam college of Engineering and Technology, India
Dr. Amit Kumar Garg, Shri Mata Vaishno Devi University, Katra(J&K), India
Assist. Prof. Raj Gaurang Tiwari, AZAD Institute of Engineering and Technology, India
Mr. Hamed Taherdoost, Tehran, Iran
Mr. Amin Daneshmand Malayeri, YRC, IAU, Malayer Branch, Iran
Mr. Shantanu Pal, University of Calcutta, India
Dr. Terry H. Walcott, E-Promag Consultancy Group, United Kingdom
Dr. Ezekiel U OKIKE, University of Ibadan, Nigeria
Mr. P. Mahalingam, Caledonian College of Engineering, Oman
Dr. Mahmoud M. A. Abd Ellatif, Mansoura University, Egypt

Prof. Kunwar S. Vaisla, BCT Kumaon Engineering College, India
Prof. Mahesh H. Panchal, Kalol Institute of Technology & Research Centre, India
Mr. Muhammad Asad, Technical University of Munich, Germany
Mr. AliReza Shams Shafiqh, Azad Islamic university, Iran
Prof. S. V. Nagaraj, RMK Engineering College, India
Mr. Ashikali M Hasan, Senior Researcher, CelNet security, India
Dr. Adnan Shahid Khan, University Technology Malaysia, Malaysia
Mr. Prakash Gajanan Burade, Nagpur University/ITM college of engg, Nagpur, India
Dr. Jagdish B.Helonde, Nagpur University/ITM college of engg, Nagpur, India
Professor, Doctor BOUHORMA Mohammed, Univertsity Abdelmalek Essaadi, Morocco
Mr. K. Thirumalaivasan, Pondicherry Engg. College, India
Mr. Umbarkar Anantkumar Janardan, Walchand College of Engineering, India
Mr. Ashish Chaurasia, Gyan Ganga Institute of Technology & Sciences, India
Mr. Sunil Taneja, Kurukshetra University, India
Mr. Fauzi Adi Rafrastra, Dian Nuswantoro University, Indonesia
Dr. Yaduvir Singh, Thapar University, India
Dr. Ioannis V. Koskosas, University of Western Macedonia, Greece
Dr. Vasantha Kalyani David, Avinashilingam University for women, Coimbatore
Dr. Ahmed Mansour Manasrah, Universiti Sains Malaysia, Malaysia
Miss. Nazanin Sadat Kazazi, University Technology Malaysia, Malaysia
Mr. Saeed Rasouli Heikalabad, Islamic Azad University - Tabriz Branch, Iran
Assoc. Prof. Dhirendra Mishra, SVKM's NMIMS University, India
Prof. Shapor Zarei, UAE Inventors Association, UAE
Prof. B.Raja Sarath Kumar, Lenora College of Engineering, India
Dr. Bashir Alam, Jamia millia Islamia, Delhi, India
Prof. Anant J Umbarkar, Walchand College of Engg., India
Assist. Prof. B. Bharathi, Sathyabama University, India
Dr. Fokrul Alom Mazarbhuiya, King Khalid University, Saudi Arabia
Prof. T.S.Jeyali Laseeth, Anna University of Technology, Tirunelveli, India
Dr. M. Balraju, Jawahar Lal Nehru Technological University Hyderabad, India
Dr. Vijayalakshmi M. N., R.V.College of Engineering, Bangalore
Prof. Walid Moudani, Lebanese University, Lebanon
Dr. Saurabh Pal, VBS Purvanchal University, Jaunpur, India
Associate Prof. Suneet Chaudhary, Dehradun Institute of Technology, India
Associate Prof. Dr. Manuj Darbari, BBD University, India
Ms. Prema Selvaraj, K.S.R College of Arts and Science, India
Assist. Prof. Ms.S.Sasikala, KSR College of Arts & Science, India
Mr. Sukhvinder Singh Deora, NC Institute of Computer Sciences, India
Dr. Abhay Bansal, Amity School of Engineering & Technology, India
Ms. Sumita Mishra, Amity School of Engineering and Technology, India
Professor S. Viswanadha Raju, JNT University Hyderabad, India
Mr. Asghar Shahrzad Khashandarag, Islamic Azad University Tabriz Branch, India
Mr. Manoj Sharma, Panipat Institute of Engg. & Technology, India
Mr. Shakeel Ahmed, King Faisal University, Saudi Arabia
Dr. Mohamed Ali Mahjoub, Institute of Engineer of Monastir, Tunisia
Mr. Adri Jovin J.J., SriGuru Institute of Technology, India
Dr. Sukumar Senthilkumar, Universiti Sains Malaysia, Malaysia

Mr. Rakesh Bharati, Dehradun Institute of Technology Dehradun, India
Mr. Shervan Fekri Ershad, Shiraz International University, Iran
Mr. Md. Safiqul Islam, Daffodil International University, Bangladesh
Mr. Mahmudul Hasan, Daffodil International University, Bangladesh
Prof. Mandakini Tayade, UIT, RGTU, Bhopal, India
Ms. Sarla More, UIT, RGTU, Bhopal, India
Mr. Tushar Hrishikesh Jaware, R.C. Patel Institute of Technology, Shirpur, India
Ms. C. Divya, Dr G R Damodaran College of Science, Coimbatore, India
Mr. Fahimuddin Shaik, Annamacharya Institute of Technology & Sciences, India
Dr. M. N. Giri Prasad, JNTUCE,Pulivendula, A.P., India
Assist. Prof. Chintan M Bhatt, Charotar University of Science And Technology, India
Prof. Sahista Machchhar, Marwadi Education Foundation's Group of institutions, India
Assist. Prof. Navnish Goel, S. D. College Of Enginnering & Technology, India
Mr. Khaja Kamaluddin, Sirt University, Sirt, Libya
Mr. Mohammad Zaidul Karim, Daffodil International, Bangladesh
Mr. M. Vijayakumar, KSR College of Engineering, Tiruchengode, India
Mr. S. A. Ahsan Rajon, Khulna University, Bangladesh
Dr. Muhammad Mohsin Nazir, LCW University Lahore, Pakistan
Mr. Mohammad Asadul Hoque, University of Alabama, USA
Mr. P.V.Sarathchand, Indur Institute of Engineering and Technology, India
Mr. Durgesh Samadhiya, Chung Hua University, Taiwan
Dr Venu Kuthadi, University of Johannesburg, Johannesburg, RSA
Dr. (Er) Jasvir Singh, Guru Nanak Dev University, Amritsar, Punjab, India
Mr. Jasmin Cosic, Min. of the Interior of Una-sana canton, B&H, Bosnia and Herzegovina
Dr S. Rajalakshmi, Botho College, South Africa
Dr. Mohamed Sarrab, De Montfort University, UK
Mr. Basappa B. Kodada, Canara Engineering College, India
Assist. Prof. K. Ramana, Annamacharya Institute of Technology and Sciences, India
Dr. Ashu Gupta, Apeejay Institute of Management, Jalandhar, India
Assist. Prof. Shaik Rasool, Shadan College of Engineering & Technology, India
Assist. Prof. K. Suresh, Annamacharya Institute of Tech & Sci. Rajampet, AP, India
Dr . G. Singaravel, K.S.R. College of Engineering, India
Dr B. G. Geetha, K.S.R. College of Engineering, India
Assist. Prof. Kavita Choudhary, ITM University, Gurgaon
Dr. Mehrdad Jalali, Azad University, Mashhad, Iran
Megha Goel, Shamli Institute of Engineering and Technology, Shamli, India
Mr. Chi-Hua Chen, Institute of Information Management, National Chiao-Tung University, Taiwan (R.O.C.)
Assoc. Prof. A. Rajendran, RVS College of Engineering and Technology, India
Assist. Prof. S. Jaganathan, RVS College of Engineering and Technology, India
Assoc. Prof. (Dr.) A S N Chakravarthy, JNTUK University College of Engineering Vizianagaram (State University)
Assist. Prof. Deepshikha Patel, Technocrat Institute of Technology, India
Assist. Prof. Maram Balajee, GMRIT, India
Assist. Prof. Monika Bhatnagar, TIT, India
Prof. Gaurang Panchal, Charotar University of Science & Technology, India
Prof. Anand K. Tripathi, Computer Society of India
Prof. Jyoti Chaudhary, High Performance Computing Research Lab, India
Assist. Prof. Supriya Raheja, ITM University, India

Dr. Pankaj Gupta, Microsoft Corporation, U.S.A.
Assist. Prof. Panchamukesh Chandaka, Hyderabad Institute of Tech. & Management, India
Prof. Mohan H.S, SJB Institute Of Technology, India
Mr. Hossein Malekinezhad, Islamic Azad University, Iran
Mr. Zatin Gupta, Universti Malaysia, Malaysia
Assist. Prof. Amit Chauhan, Phonics Group of Institutions, India
Assist. Prof. Ajal A. J., METS School Of Engineering, India
Mrs. Omowunmi Omobola Adeyemo, University of Ibadan, Nigeria
Dr. Bharat Bhushan Agarwal, I.F.T.M. University, India
Md. Nazrul Islam, University of Western Ontario, Canada
Tushar Kanti, L.N.C.T, Bhopal, India
Er. Aumreesh Kumar Saxena, SIRTs College Bhopal, India
Mr. Mohammad Monirul Islam, Daffodil International University, Bangladesh
Dr. Kashif Nisar, University Utara Malaysia, Malaysia
Dr. Wei Zheng, Rutgers Univ/ A10 Networks, USA
Associate Prof. Rituraj Jain, Vyas Institute of Engg & Tech, Jodhpur – Rajasthan
Assist. Prof. Apoorvi Sood, I.T.M. University, India
Dr. Kayhan Zrar Ghafoor, University Technology Malaysia, Malaysia
Mr. Swapnil Soner, Truba Institute College of Engineering & Technology, Indore, India
Ms. Yogita Gigras, I.T.M. University, India
Associate Prof. Neelima Sadineni, Pydha Engineering College, India Pydha Engineering College
Assist. Prof. K. Deepika Rani, HITAM, Hyderabad
Ms. Shikha Maheshwari, Jaipur Engineering College & Research Centre, India
Prof. Dr V S Giridhar Akula, Avanthi's Scientific Tech. & Research Academy, Hyderabad
Prof. Dr.S.Saravanan, Muthayammal Engineering College, India
Mr. Mehdi Golsorkhtabar Amiri, Islamic Azad University, Iran
Prof. Amit Sadanand Savyanavar, MITCOE, Pune, India
Assist. Prof. P.Oliver Jayaprakash, Anna University,Chennai
Assist. Prof. Ms. Sujata, ITM University, Gurgaon, India
Dr. Asoke Nath, St. Xavier's College, India
Mr. Masoud Rafighi, Islamic Azad University, Iran
Assist. Prof. RamBabu Pemula, NIMRA College of Engineering & Technology, India
Assist. Prof. Ms Rita Chhikara, ITM University, Gurgaon, India
Mr. Sandeep Maan, Government Post Graduate College, India
Prof. Dr. S. Muralidharan, Mepco Schlenk Engineering College, India
Associate Prof. T.V.Sai Krishna, QIS College of Engineering and Technology, India
Mr. R. Balu, Bharathiar University, Coimbatore, India
Assist. Prof. Shekhar. R, Dr.SM College of Engineering, India
Prof. P. Senthilkumar, Vivekanandha Institue of Engineering and Techology for Woman, India
Mr. M. Kamarajan, PSNA College of Engineering & Technology, India
Dr. Angajala Srinivasa Rao, Jawaharlal Nehru Technical University, India
Assist. Prof. C. Venkatesh, A.I.T.S, Rajampet, India
Mr. Afshin Rezakhani Roozbahani, Ayatollah Boroujerdi University, Iran
Mr. Laxmi chand, SCTL, Noida, India
Dr. Dr. Abdul Hannan, Vivekanand College, Aurangabad
Prof. Mahesh Panchal, KITRC, Gujarat
Dr. A. Subramani, K.S.R. College of Engineering, Tiruchengode

Assist. Prof. Prakash M, Rajalakshmi Engineering College, Chennai, India
Assist. Prof. Akhilesh K Sharma, Sir Padampat Singhania University, India
Ms. Varsha Sahni, Guru Nanak Dev Engineering College, Ludhiana, India
Associate Prof. Trilochan Rout, NM Institute of Engineering and Technology, India
Mr. Srikanta Kumar Mohapatra, NMIFT, Orissa, India
Mr. Waqas Haider Bangyal, Iqra University Islamabad, Pakistan
Dr. S. Vijayaragavan, Christ College of Engineering and Technology, Pondicherry, India
Prof. Elboukhari Mohamed, University Mohammed First, Oujda, Morocco
Dr. Muhammad Asif Khan, King Faisal University, Saudi Arabia
Dr. Nagy Ramadan Darwish Omran, Cairo University, Egypt.
Assistant Prof. Anand Nayyar, KCL Institute of Management and Technology, India
Mr. G. Premsankar, Ericsson, India
Assist. Prof. T. Hemalatha, VELS University, India
Prof. Tejaswini Apte, University of Pune, India
Dr. Edmund Ng Giap Weng, Universiti Malaysia Sarawak, Malaysia
Mr. Mahdi Nouri, Iran University of Science and Technology, Iran
Associate Prof. S. Asif Hussain, Annamacharya Institute of technology & Sciences, India
Mrs. Kavita Pabreja, Maharaja Surajmal Institute (an affiliate of GGSIP University), India
Mr. Vorugunti Chandra Sekhar, DA-IICT, India
Mr. Muhammad Najmi Ahmad Zabidi, Universiti Teknologi Malaysia, Malaysia
Dr. Aderemi A. Atayero, Covenant University, Nigeria
Assist. Prof. Osama Sohaib, Balochistan University of Information Technology, Pakistan
Assist. Prof. K. Suresh, Annamacharya Institute of Technology and Sciences, India
Mr. Hassen Mohammed Abdulla Alsaifi, International Islamic University Malaysia (IIUM) Malaysia
Mr. Robail Yasrab, Virtual University of Pakistan, Pakistan
Mr. R. Balu, Bharathiar University, Coimbatore, India
Prof. Anand Nayyar, KCL Institute of Management and Technology, Jalandhar
Assoc. Prof. Vivek S Deshpande, MIT College of Engineering, India
Prof. K. Saravanan, Anna university Coimbatore, India
Dr. Ravendra Singh, MJP Rohilkhand University, Bareilly, India
Mr. V. Mathivanan, IBRA College of Technology, Sultanate of OMAN
Assoc. Prof. S. Asif Hussain, AITS, India
Assist. Prof. C. Venkatesh, AITS, India
Mr. Sami Ulhaq, SZABIST Islamabad, Pakistan
Dr. B. Justus Rabi, Institute of Science & Technology, India
Mr. Anuj Kumar Yadav, Dehradun Institute of technology, India
Mr. Alejandro Mosquera, University of Alicante, Spain
Assist. Prof. Arjun Singh, Sir Padampat Singhania University (SPSU), Udaipur, India
Dr. Smriti Agrawal, JB Institute of Engineering and Technology, Hyderabad
Assist. Prof. Swathi Sambangi, Visakha Institute of Engineering and Technology, India
Ms. Prabhjot Kaur, Guru Gobind Singh Indraprastha University, India
Mrs. Samaher AL-Hothali, Yanbu University College, Saudi Arabia
Prof. Rajneeshkaur Bedi, MIT College of Engineering, Pune, India
Mr. Hassen Mohammed Abdulla Alsaifi, International Islamic University Malaysia (IIUM)
Dr. Wei Zhang, Amazon.com, Seattle, WA, USA
Mr. B. Santhosh Kumar, C S I College of Engineering, Tamil Nadu
Dr. K. Reji Kumar, , N S S College, Pandalam, India

Assoc. Prof. K. Seshadri Sastry, EIILM University, India
Mr. Kai Pan, UNC Charlotte, USA
Mr. Ruikar Sachin, SGGSIET, India
Prof. (Dr.) Vinodani Katiyar, Sri Ramswaroop Memorial University, India
Assoc. Prof., M. Giri, Sreenivasa Institute of Technology and Management Studies, India
Assoc. Prof. Labib Francis Gergis, Misr Academy for Engineering and Technology (MET), Egypt
Assist. Prof. Amanpreet Kaur, ITM University, India
Assist. Prof. Anand Singh Rajawat, Shri Vaishnav Institute of Technology & Science, Indore
Mrs. Hadeel Saleh Haj Aliwi, Universiti Sains Malaysia (USM), Malaysia
Dr. Abhay Bansal, Amity University, India
Dr. Mohammad A. Mezher, Fahad Bin Sultan University, KSA
Assist. Prof. Nidhi Arora, M.C.A. Institute, India
Prof. Dr. P. Suresh, Karpagam College of Engineering, Coimbatore, India
Dr. Kannan Balasubramanian, Mepco Schlenk Engineering College, India
Dr. S. Sankara Gomathi, Panimalar Engineering college, India
Prof. Anil Kumar Suthar, Gujarat Technological University, L.C. Institute of Technology, India
Assist. Prof. R. Hubert Rajan, NOORUL ISLAM UNIVERSITY, India
Assist. Prof. Dr. Jyoti Mahajan, College of Engineering & Technology
Assist. Prof. Homam Reda El-Taj, College of Network Engineering, Saudi Arabia & Malaysia
Mr. Bijan Paul, Shahjalal University of Science & Technology, Bangladesh
Assoc. Prof. Dr. Ch V Phani Krishna, KL University, India
Dr. Vishal Bhatnagar, Ambedkar Institute of Advanced Communication Technologies & Research, India
Dr. Lamri LAOUAMER, Al Qassim University, Dept. Info. Systems & European University of Brittany, Dept. Computer Science, UBO, Brest, France
Prof. Ashish Babanrao Sasankar, G.H.Raisoni Institute Of Information Technology, India
Prof. Pawan Kumar Goel, Shamli Institute of Engineering and Technology, India
Mr. Ram Kumar Singh, S.V Subharti University, India
Assistant Prof. Sunish Kumar O S, Amaljyothi College of Engineering, India
Dr Sanjay Bhargava, Banasthali University, India
Mr. Pankaj S. Kulkarni, AVEW's Shatabdi Institute of Technology, India
Mr. Roohollah Etemadi, Islamic Azad University, Iran
Mr. Oloruntoyin Sefiu Taiwo, Emmanuel Alayande College Of Education, Nigeria
Mr. Sumit Goyal, National Dairy Research Institute, India
Mr Jaswinder Singh Dilawari, Geeta Engineering College, India
Prof. Raghuraj Singh, Harcourt Butler Technological Institute, Kanpur
Dr. S.K. Mahendran, Anna University, Chennai, India
Dr. Amit Wason, Hindustan Institute of Technology & Management, Punjab
Dr. Ashu Gupta, Apeejay Institute of Management, India
Assist. Prof. D. Asir Antony Gnana Singh, M.I.E.T Engineering College, India
Mrs Mina Farmanbar, Eastern Mediterranean University, Famagusta, North Cyprus
Mr. Maram Balajee, GMR Institute of Technology, India
Mr. Moiz S. Ansari, Isra University, Hyderabad, Pakistan
Mr. Adebayo, Olawale Surajudeen, Federal University of Technology Minna, Nigeria
Mr. Jasvir Singh, University College Of Engg., India
Mr. Vivek Tiwari, MANIT, Bhopal, India
Assoc. Prof. R. Navaneethakrishnan, Bharathiyar College of Engineering and Technology, India
Mr. Somdip Dey, St. Xavier's College, Kolkata, India

Mr. Souleymane Balla-Arabé, Xi'an University of Electronic Science and Technology, China
Mr. Mahabub Alam, Rajshahi University of Engineering and Technology, Bangladesh
Mr. Sathyaprakash P., S.K.P Engineering College, India
Dr. N. Karthikeyan, SNS College of Engineering, Anna University, India
Dr. Binod Kumar, JSPM's, Jayawant Technical Campus, Pune, India
Assoc. Prof. Dinesh Goyal, Suresh Gyan Vihar University, India
Mr. Md. Abdul Ahad, K L University, India
Mr. Vikas Bajpai, The LNM IIT, India
Dr. Manish Kumar Anand, Salesforce (R & D Analytics), San Francisco, USA
Assist. Prof. Dheeraj Murari, Kumaon Engineering College, India
Assoc. Prof. Dr. A. Muthukumaravel, VELS University, Chennai
Mr. A. Siles Balasingh, St.Joseph University in Tanzania, Tanzania
Mr. Ravindra Daga Badgujar, R C Patel Institute of Technology, India
Dr. Preeti Khanna, SVKM's NMIMS, School of Business Management, India
Mr. Kumar Dayanand, Cambridge Institute of Technology, India
Dr. Syed Asif Ali, SMI University Karachi, Pakistan
Prof. Pallvi Pandit, Himachal Pradesh University, India
Mr. Ricardo Verschueren, University of Gloucestershire, UK
Assist. Prof. Mamta Juneja, University Institute of Engineering and Technology, Panjab University, India
Assoc. Prof. P. Surendra Varma, NRI Institute of Technology, JNTU Kakinada, India
Assist. Prof. Gaurav Shrivastava, RGPV / SVITS Indore, India
Dr. S. Sumathi, Anna University, India
Assist. Prof. Ankita M. Kapadia, Charotar University of Science and Technology, India
Mr. Deepak Kumar, Indian Institute of Technology (BHU), India
Dr. Dr. Rajan Gupta, GGSIP University, New Delhi, India
Assist. Prof M. Anand Kumar, Karpagam University, Coimbatore, India
Mr. Mr Arshad Mansoor, Pakistan Aeronautical Complex
Mr. Kapil Kumar Gupta, Ansal Institute of Technology and Management, India
Dr. Neeraj Tomer, SINE International Institute of Technology, Jaipur, India
Assist. Prof. Trunal J. Patel, C.G.Patel Institute of Technology, Uka Tarsadia University, Bardoli, Surat
Mr. Sivakumar, Codework solutions, India
Mr. Mohammad Sadegh Mirzaei, PGNR Company, Iran
Dr. Gerard G. Dumancas, Oklahoma Medical Research Foundation, USA
Mr. Varadala Sridhar, Varadhaman College Engineering College, Affiliated To JNTU, Hyderabad
Assist. Prof. Manoj Dhawan, SVITS, Indore
Assoc. Prof. Chitreshh Banerjee, Suresh Gyan Vihar University, Jaipur, India
Dr. S. Santhi, SCSVMV University, India
Mr. Davood Mohammadi Souran, Ministry of Energy of Iran, Iran
Mr. Shamim Ahmed, Bangladesh University of Business and Technology, Bangladesh
Mr. Sandeep Reddivari, Mississippi State University, USA
Assoc. Prof. Ousmane Thiare, Gaston Berger University, Senegal
Dr. Hazra Imran, Athabasca University, Canada
Dr. Setu Kumar Chaturvedi, Technocrats Institute of Technology, Bhopal, India
Mr. Mohd Dilshad Ansari, Jaypee University of Information Technology, India
Ms. Jaspreet Kaur, Distance Education LPU, India
Dr. D. Nagarajan, Salalah College of Technology, Sultanate of Oman
Dr. K.V.N.R.Sai Krishna, S.V.R.M. College, India

Mr. Himanshu Pareek, Center for Development of Advanced Computing (CDAC), India
Mr. Khaldi Amine, Badji Mokhtar University, Algeria
Mr. Mohammad Sadegh Mirzaei, Scientific Applied University, Iran
Assist. Prof. Khyati Chaudhary, Ram-eesh Institute of Engg. & Technology, India
Mr. Sanjay Agal, Pacific College of Engineering Udaipur, India
Mr. Abdul Mateen Ansari, King Khalid University, Saudi Arabia
Dr. H.S. Behera, Veer Surendra Sai University of Technology (VSSUT), India
Dr. Shrikant Tiwari, Shri Shankaracharya Group of Institutions (SSGI), India
Prof. Ganesh B. Regulwar, Shri Shankarprasad Agnihotri College of Engg, India
Prof. Pinnamaneni Bhanu Prasad, Matrix vision GmbH, Germany
Dr. Shrikant Tiwari, Shri Shankaracharya Technical Campus (SSTC), India
Dr. Siddesh G.K., : Dayananada Sagar College of Engineering, Bangalore, India
Dr. Nadir Bouchama, CERIST Research Center, Algeria
Dr. R. Sathishkumar, Sri Venkateswara College of Engineering, India
Assistant Prof (Dr.) Mohamed Moussaoui, Abdelmalek Essaadi University, Morocco
Dr. S. Malathi, Panimalar Engineering College, Chennai, India
Dr. V. Subedha, Panimalar Institute of Technology, Chennai, India
Dr. Prashant Panse, Swami Vivekanand College of Engineering, Indore, India
Dr. Hamza Aldabbas, Al-Balqa'a Applied University, Jordan
Dr. G. Rasitha Banu, Vel's University, Chennai
Dr. V. D. Ambeth Kumar, Panimalar Engineering College, Chennai
Prof. Anuranjan Misra, Bhagwant Institute of Technology, Ghaziabad, India
Ms. U. Sirthuja, PSG college of arts &science, India
Dr. Ehsan Saradar Torshizi, Urmia University, Iran
Dr. Shamneesh Sharma, APG Shimla University, Shimla (H.P.), India
Assistant Prof. A. S. Syed Navaz, Muthayammal College of Arts & Science, India
Assistant Prof. Ranjit Panigrahi, Sikkim Manipal Institute of Technology, Majitar, Sikkim
Dr. Khaled Eskaf, Arab Academy for Science ,Technology & Maritime Transportation, Egypt
Dr. Nishant Gupta, University of Jammu, India
Assistant Prof. Nagarajan Sankaran, Annamalai University, Chidambaram, Tamilnadu, India
Assistant Prof. Tribikram Pradhan, Manipal Institute of Technology, India
Dr. Nasser Lotfi, Eastern Mediterranean University, Northern Cyprus
Dr. R. Manavalan, K S Rangasamy college of Arts and Science, Tamilnadu, India
Assistant Prof. P. Krishna Sankar, K S Rangasamy college of Arts and Science, Tamilnadu, India
Dr. Rahul Malik, Cisco Systems, USA
Dr. S. C. Lingareddy, ALPHA College of Engineering, India
Assistant Prof. Mohammed Shuaib, Interl University, Lucknow, India
Dr. Sachin Yele, Sanghvi Institute of Management & Science, India
Dr. T. Thambidurai, Sun Univercell, Singapore
Prof. Anandkumar Telang, BKIT, India
Assistant Prof. R. Poorvadevi, SCVMV University, India
Dr Uttam Mande, Gitam University, India
Dr. Poornima Girish Naik, Shahu Institute of Business Education and Research (SIBER), India
Prof. Md. Abu Kausar, Jaipur National University, Jaipur, India
Dr. Mohammed Zuber, AISECT University, India
Prof. Kalum Priyanath Udagepola, King Abdulaziz University, Saudi Arabia
Dr. K. R. Ananth, Velalar College of Engineering and Technology, India

Assistant Prof. Sanjay Sharma, Roorkee Engineering & Management Institute Shamli (U.P), India
Assistant Prof. Panem Charan Arur, Priyadarshini Institute of Technology, India
Dr. Ashwak Mahmood muhsen alabaichi, Karbala University / College of Science, Iraq
Dr. Urmila Shrawankar, G H Raisoni College of Engineering, Nagpur (MS), India
Dr. Krishan Kumar Paliwal, Panipat Institute of Engineering & Technology, India
Dr. Mukesh Negi, Tech Mahindra, India
Dr. Anuj Kumar Singh, Amity University Gurgaon, India
Dr. Babar Shah, Gyeongsang National University, South Korea
Assistant Prof. Jayprakash Upadhyay, SRI-TECH Jabalpur, India
Assistant Prof. Varadala Sridhar, Vidya Jyothi Institute of Technology, India
Assistant Prof. Parameshachari B D, KSIT, Bangalore, India
Assistant Prof. Ankit Garg, Amity University, Haryana, India
Assistant Prof. Rajashe Karappa, SDMCET, Karnataka, India
Assistant Prof. Varun Jasuja, GNIT, India
Assistant Prof. Sonal Honale, Abha Gaikwad Patil College of Engineering Nagpur, India
Dr. Pooja Choudhary, CT Group of Institutions, NIT Jalandhar, India
Dr. Faouzi Hidoussi, UHL Batna, Algeria
Dr. Naseer Ali Husieen, Wasit University, Iraq
Assistant Prof. Vinod Kumar Shukla, Amity University, Dubai
Dr. Ahmed Farouk Metwaly, K L University
Mr. Mohammed Noaman Murad, Cihan University, Iraq
Dr. Suxing Liu, Arkansas State University, USA
Dr. M. Gomathi, Velalar College of Engineering and Technology, India
Assistant Prof. Sumardiono, College PGRI Blitar, Indonesia
Dr. Latika Kharb, Jagan Institute of Management Studies (JIMS), Delhi, India
Associate Prof. S. Raja, Pauls College of Engineering and Technology, Tamilnadu, India
Assistant Prof. Seyed Reza Pakize, Shahid Sani High School, Iran
Dr. Thiyyagu Nagaraj, University-INOU, India
Assistant Prof. Noreen Sarai, Harare Institute of Technology, Zimbabwe
Assistant Prof. Gajanand Sharma, Suresh Gyan Vihar University Jaipur, Rajasthan, India
Assistant Prof. Mapari Vikas Prakash, Siddhant COE, Sudumbare, Pune, India
Dr. Devesh Katiyar, Shri Ramswaroop Memorial University, India
Dr. Shenshen Liang, University of California, Santa Cruz, US
Assistant Prof. Mohammad Abu Omar, Limkokwing University of Creative Technology- Malaysia
Mr. Snehasis Banerjee, Tata Consultancy Services, India
Assistant Prof. Kibona Lusekelo, Ruaha Catholic University (RUCU), Tanzania
Assistant Prof. Adib Kabir Chowdhury, University College Technology Sarawak, Malaysia
Dr. Ying Yang, Computer Science Department, Yale University, USA
Dr. Vinay Shukla, Institute Of Technology & Management, India
Dr. Liviu Octavian Mafteiu-Scai, West University of Timisoara, Romania
Assistant Prof. Rana Khudhair Abbas Ahmed, Al-Rafidain University College, Iraq
Assistant Prof. Nitin A. Naik, S.R.T.M. University, India
Dr. Timothy Powers, University of Hertfordshire, UK
Dr. S. Prasath, Bharathiar University, Erode, India
Dr. Ritu Shrivastava, SIRTS Bhopal, India
Prof. Rohit Shrivastava, Mittal Institute of Technology, Bhopal, India
Dr. Gianina Mihai, Dunarea de Jos" University of Galati, Romania

Assistant Prof. Ms. T. Kalai Selvi, Erode Sengunthar Engineering College, India
Assistant Prof. Ms. C. Kavitha, Erode Sengunthar Engineering College, India
Assistant Prof. K. Sinivasamoorthi, Erode Sengunthar Engineering College, India
Assistant Prof. Mallikarjun C Sarsamba Bheemnna Khandre Institute Technology, Bhalki, India
Assistant Prof. Vishwanath Chikaraddi, Veermata Jijabai technological Institute (Central Technological Institute), India
Assistant Prof. Dr. Ikvinderpal Singh, Trai Shatabdi GGS Khalsa College, India
Assistant Prof. Mohammed Noaman Murad, Cihan University, Iraq
Professor Yousef Farhaoui, Moulay Ismail University, Errachidia, Morocco
Dr. Parul Verma, Amity University, India
Professor Yousef Farhaoui, Moulay Ismail University, Errachidia, Morocco
Assistant Prof. Madhavi Dhingra, Amity University, Madhya Pradesh, India
Assistant Prof.. G. Selvavinayagam, SNS College of Technology, Coimbatore, India
Assistant Prof. Madhavi Dhingra, Amity University, MP, India
Professor Kartheesan Log, Anna University, Chennai
Professor Vasudeva Acharya, Shri Madhwa vadira Institute of Technology, India
Dr. Asif Iqbal Hajamydeen, Management & Science University, Malaysia
Assistant Prof., Mahendra Singh Meena, Amity University Haryana
Assistant Professor Manjeet Kaur, Amity University Haryana
Dr. Mohamed Abd El-Basset Matwalli, Zagazig University, Egypt
Dr. Ramani Kannan, Universiti Teknologi PETRONAS, Malaysia
Assistant Prof. S. Jagadeesan Subramaniam, Anna University, India
Assistant Prof. Dharmendra Choudhary, Tripura University, India
Assistant Prof. Deepika Vodnala, SR Engineering College, India
Dr. Kai Cong, Intel Corporation & Computer Science Department, Portland State University, USA
Dr. Kailas R Patil, Vishwakarma Institute of Information Technology (VIIT), India
Dr. Omar A. Alzubi, Faculty of IT / Al-Balqa Applied University, Jordan
Assistant Prof. Kareemullah Shaik, Nimra Institute of Science and Technology, India
Assistant Prof. Chirag Modi, NIT Goa
Dr. R. Ramkumar, Nandha Arts And Science College, India
Dr. Priyadarshini Vydhalingam, Harathiar University, India
Dr. P. S. Jagadeesh Kumar, DBIT, Bangalore, Karnataka
Dr. Vikas Thada, AMITY University, Pachgaon
Dr. T. A. Ashok Kumar, Institute of Management, Christ University, Bangalore
Dr. Shaheera Rashwan, Informatics Research Institute
Dr. S. Preetha Gunasekar, Bharathiyar University, India
Asst Professor Sameer Dev Sharma, Uttarakhand University, Dehradun
Dr. Zhihan Lv, Chinese Academy of Science, China
Dr. Ikvinderpal Singh, Trai Shatabdi GGS Khalsa College, Amritsar
Dr. Umar Ruhi, University of Ottawa, Canada
Dr. Jasmin Cosic, University of BiHac, Bosnia and Herzegovina
Dr. Homam Reda El-Taj, University of Tabuk, Kingdom of Saudi Arabia
Dr. Mostafa Ghobaei Arani, Islamic Azad University, Iran
Dr. Ayyasamy Ayyanar, Annamalai University, India
Dr. Selvakumar Manickam, Universiti Sains Malaysia, Malaysia
Dr. Murali Krishna Namana, GITAM University, India
Dr. Smriti Agrawal, Chaitanya Bharathi Institute of Technology, Hyderabad, India
Professor Vimalathithan Rathinasabapathy, Karpagam College Of Engineering, India

Dr. Sushil Chandra Dimri, Graphic Era University, India
Dr. Dinh-Sinh Mai, Le Quy Don Technical University, Vietnam
Dr. S. Rama Sree, Aditya Engg. College, India
Dr. Ehab T. Alnfrawy, Sadat Academy, Egypt
Dr. Patrick D. Cerna, Haramaya University, Ethiopia
Dr. Vishal Jain, Bharati Vidyapeeth's Institute of Computer Applications and Management (BVICAM), India
Associate Prof. Dr. Jiliang Zhang, North Eastern University, China
Dr. Sharefa Murad, Middle East University, Jordan
Dr. Ajeet Singh Poonia, Govt. College of Engineering & technology, Rajasthan, India
Dr. Vahid Esmaeelzadeh, University of Science and Technology, Iran
Dr. Jacek M. Czerniak, Casimir the Great University in Bydgoszcz, Institute of Technology, Poland
Associate Prof. Anisur Rehman Nasir, Jamia Millia Islamia University
Assistant Prof. Imran Ahmad, COMSATS Institute of Information Technology, Pakistan
Professor Ghulam Qasim, Preston University, Islamabad, Pakistan
Dr. Parameshachari B D, GSSS Institute of Engineering and Technology for Women
Dr. Wencan Luo, University of Pittsburgh, US
Dr. Musa PEKER, Faculty of Technology, Mugla Sitki Kocman University, Turkey
Dr. Gunasekaran Shanmugam, Anna University, India
Dr. Binh P. Nguyen, National University of Singapore, Singapore
Dr. Rajkumar Jain, Indian Institute of Technology Indore, India
Dr. Imtiaz Ali Halepoto, QUEST Nawabshah, Pakistan
Dr. Shaligram Prajapat, Devi Ahilya University Indore India
Dr. Sunita Singhal, Birla Institute of Technologyand Science, Pilani, India
Dr. Ijaz Ali Shoukat, King Saud University, Saudi Arabia
Dr. Anuj Gupta, IKG Punjab Technical University, India
Dr. Sonali Saini, IES-IPS Academy, India
Dr. Krishan Kumar, MotiLal Nehru National Institute of Technology, Allahabad, India
Dr. Z. Faizal Khan, College of Engineering, Shaqra University, Kingdom of Saudi Arabia
Prof. M. Padmavathamma, S.V. University Tirupati, India
Prof. A. Velayudham, Cape Institute of Technology, India
Prof. Seifeide Kadry, American University of the Middle East
Dr. J. Durga Prasad Rao, Pt. Ravishankar Shukla University, Raipur
Assistant Prof. Najam Hasan, Dhofar University
Dr. G. Suseendran, Vels University, Pallavaram, Chennai
Prof. Ankit Faldu, Gujarat Technological Universiry- Atmiya Institute of Technology and Science
Dr. Ali Habiboghi, Islamic Azad University
Dr. Deepak Dembla, JECRC University, Jaipur, India
Dr. Pankaj Rajan, Walmart Labs, USA
Assistant Prof. Radoslava Kraleva, South-West University "Neofit Rilski", Bulgaria
Assistant Prof. Medhavi Shriwas, Shri vaishnav institute of Technology, India
Associate Prof. Sedat Akleylek, Ondokuz Mayis University, Turkey
Dr. U.V. Arivazhagu, Kingston Engineering College Affiliated To Anna University, India
Dr. Touseef Ali, University of Engineering and Technology, Taxila, Pakistan
Assistant Prof. Naren Jeeva, SASTRA University, India
Dr. Riccardo Colella, University of Salento, Italy
Dr. Enache Maria Cristina, University of Galati, Romania
Dr. Senthil P, Kurinji College of Arts & Science, India

CALL FOR PAPERS

International Journal of Computer Science and Information Security

IJCSIS 2016
ISSN: 1947-5500
<http://sites.google.com/site/ijcsis/>

International Journal Computer Science and Information Security, IJCSIS, is the premier scholarly venue in the areas of computer science and security issues. IJCSIS 2011 will provide a high profile, leading edge platform for researchers and engineers alike to publish state-of-the-art research in the respective fields of information technology and communication security. The journal will feature a diverse mixture of publication articles including core and applied computer science related topics.

Authors are solicited to contribute to the special issue by submitting articles that illustrate research results, projects, surveying works and industrial experiences that describe significant advances in the following areas, but are not limited to. Submissions may span a broad range of topics, e.g.:

Track A: Security

Access control, Anonymity, Audit and audit reduction & Authentication and authorization, Applied cryptography, Cryptanalysis, Digital Signatures, Biometric security, Boundary control devices, Certification and accreditation, Cross-layer design for security, Security & Network Management, Data and system integrity, Database security, Defensive information warfare, Denial of service protection, Intrusion Detection, Anti-malware, Distributed systems security, Electronic commerce, E-mail security, Spam, Phishing, E-mail fraud, Virus, worms, Trojan Protection, Grid security, Information hiding and watermarking & Information survivability, Insider threat protection, Integrity
Intellectual property protection, Internet/Intranet Security, Key management and key recovery, Language-based security, Mobile and wireless security, Mobile, Ad Hoc and Sensor Network Security, Monitoring and surveillance, Multimedia security ,Operating system security, Peer-to-peer security, Performance Evaluations of Protocols & Security Application, Privacy and data protection, Product evaluation criteria and compliance, Risk evaluation and security certification, Risk/vulnerability assessment, Security & Network Management, Security Models & protocols, Security threats & countermeasures (DDoS, MiM, Session Hijacking, Replay attack etc.,) Trusted computing, Ubiquitous Computing Security, Virtualization security, VoIP security, Web 2.0 security, Submission Procedures, Active Defense Systems, Adaptive Defense Systems, Benchmark, Analysis and Evaluation of Security Systems, Distributed Access Control and Trust Management, Distributed Attack Systems and Mechanisms, Distributed Intrusion Detection/Prevention Systems, Denial-of-Service Attacks and Countermeasures, High Performance Security Systems, Identity Management and Authentication, Implementation, Deployment and Management of Security Systems, Intelligent Defense Systems, Internet and Network Forensics, Large-scale Attacks and Defense, RFID Security and Privacy, Security Architectures in Distributed Network Systems, Security for Critical Infrastructures, Security for P2P systems and Grid Systems, Security in E-Commerce, Security and Privacy in Wireless Networks, Secure Mobile Agents and Mobile Code, Security Protocols, Security Simulation and Tools, Security Theory and Tools, Standards and Assurance Methods, Trusted Computing, Viruses, Worms, and Other Malicious Code, World Wide Web Security, Novel and emerging secure architecture, Study of attack strategies, attack modeling, Case studies and analysis of actual attacks, Continuity of Operations during an attack, Key management, Trust management, Intrusion detection techniques, Intrusion response, alarm management, and correlation analysis, Study of tradeoffs between security and system performance, Intrusion tolerance systems, Secure protocols, Security in wireless networks (e.g. mesh networks, sensor networks, etc.), Cryptography and Secure Communications, Computer Forensics, Recovery and Healing, Security Visualization, Formal Methods in Security, Principles for Designing a Secure Computing System, Autonomic Security, Internet Security, Security in Health Care Systems, Security Solutions Using Reconfigurable Computing, Adaptive and Intelligent Defense Systems, Authentication and Access control, Denial of service attacks and countermeasures, Identity, Route and

Location Anonymity schemes, Intrusion detection and prevention techniques, Cryptography, encryption algorithms and Key management schemes, Secure routing schemes, Secure neighbor discovery and localization, Trust establishment and maintenance, Confidentiality and data integrity, Security architectures, deployments and solutions, Emerging threats to cloud-based services, Security model for new services, Cloud-aware web service security, Information hiding in Cloud Computing, Securing distributed data storage in cloud, Security, privacy and trust in mobile computing systems and applications, **Middleware security & Security features:** middleware software is an asset on

its own and has to be protected, interaction between security-specific and other middleware features, e.g., context-awareness, **Middleware-level security monitoring and measurement:** metrics and mechanisms for quantification and evaluation of security enforced by the middleware, **Security co-design:** trade-off and co-design between application-based and middleware-based security, **Policy-based management:** innovative support for policy-based definition and enforcement of security concerns, **Identification and authentication mechanisms:** Means to capture application specific constraints in defining and enforcing access control rules, **Middleware-oriented security patterns:** identification of patterns for sound, reusable security, **Security in aspect-based middleware:** mechanisms for isolating and enforcing security aspects, **Security in agent-based platforms:** protection for mobile code and platforms, Smart Devices: Biometrics, National ID cards, Embedded Systems Security and TPMs, RFID Systems Security, Smart Card Security, Pervasive Systems: Digital Rights Management (DRM) in pervasive environments, Intrusion Detection and Information Filtering, Localization Systems Security (Tracking of People and Goods), Mobile Commerce Security, Privacy Enhancing Technologies, Security Protocols (for Identification and Authentication, Confidentiality and Privacy, and Integrity), Ubiquitous Networks: Ad Hoc Networks Security, Delay-Tolerant Network Security, Domestic Network Security, Peer-to-Peer Networks Security, Security Issues in Mobile and Ubiquitous Networks, Security of GSM/GPRS/UMTS Systems, Sensor Networks Security, Vehicular Network Security, Wireless Communication Security: Bluetooth, NFC, WiFi, WiMAX, WiMedia, others

This Track will emphasize the design, implementation, management and applications of computer communications, networks and services. Topics of mostly theoretical nature are also welcome, provided there is clear practical potential in applying the results of such work.

Track B: Computer Science

Broadband wireless technologies: LTE, WiMAX, WiRAN, HSDPA, HSUPA, Resource allocation and interference management, Quality of service and scheduling methods, Capacity planning and dimensioning, Cross-layer design and Physical layer based issue, Interworking architecture and interoperability, Relay assisted and cooperative communications, Location and provisioning and mobility management, Call admission and flow/congestion control, Performance optimization, Channel capacity modeling and analysis, Middleware Issues: Event-based, publish/subscribe, and message-oriented middleware, Reconfigurable, adaptable, and reflective middleware approaches, Middleware solutions for reliability, fault tolerance, and quality-of-service, Scalability of middleware, Context-aware middleware, Autonomic and self-managing middleware, Evaluation techniques for middleware solutions, Formal methods and tools for designing, verifying, and evaluating, middleware, Software engineering techniques for middleware, Service oriented middleware, Agent-based middleware, Security middleware, Network Applications: Network-based automation, Cloud applications, Ubiquitous and pervasive applications, Collaborative applications, RFID and sensor network applications, Mobile applications, Smart home applications, Infrastructure monitoring and control applications, Remote health monitoring, GPS and location-based applications, Networked vehicles applications, Alert applications, Embedded Computer System, Advanced Control Systems, and Intelligent Control : Advanced control and measurement, computer and microprocessor-based control, signal processing, estimation and identification techniques, application specific IC's, nonlinear and adaptive control, optimal and robot control, intelligent control, evolutionary computing, and intelligent systems, instrumentation subject to critical conditions, automotive, marine and aero-space control and all other control applications, Intelligent Control System, Wiring/Wireless Sensor, Signal Control System. Sensors, Actuators and Systems Integration : Intelligent sensors and actuators, multisensor fusion, sensor array and multi-channel processing, micro/nano technology, microsensors and microactuators, instrumentation electronics, MEMS and system integration, wireless sensor, Network Sensor, Hybrid

Sensor, Distributed Sensor Networks. Signal and Image Processing : Digital signal processing theory, methods, DSP implementation, speech processing, image and multidimensional signal processing, Image analysis and processing, Image and Multimedia applications, Real-time multimedia signal processing, Computer vision, Emerging signal processing areas, Remote Sensing, Signal processing in education. Industrial Informatics: Industrial applications of neural networks, fuzzy algorithms, Neuro-Fuzzy application, bioInformatics, real-time computer control, real-time information systems, human-machine interfaces, CAD/CAM/CAT/CIM, virtual reality, industrial communications, flexible manufacturing systems, industrial automated process, Data Storage Management, Harddisk control, Supply Chain Management, Logistics applications, Power plant automation, Drives automation. Information Technology, Management of Information System : Management information systems, Information Management, Nursing information management, Information System, Information Technology and their application, Data retrieval, Data Base Management, Decision analysis methods, Information processing, Operations research, E-Business, E-Commerce, E-Government, Computer Business, Security and risk management, Medical imaging, Biotechnology, Bio-Medicine, Computer-based information systems in health care, Changing Access to Patient Information, Healthcare Management Information Technology. Communication/Computer Network, Transportation Application : On-board diagnostics, Active safety systems, Communication systems, Wireless technology, Communication application, Navigation and Guidance, Vision-based applications, Speech interface, Sensor fusion, Networking theory and technologies, Transportation information, Autonomous vehicle, Vehicle application of affective computing, Advance Computing technology and their application : Broadband and intelligent networks, Data Mining, Data fusion, Computational intelligence, Information and data security, Information indexing and retrieval, Information processing, Information systems and applications, Internet applications and performances, Knowledge based systems, Knowledge management, Software Engineering, Decision making, Mobile networks and services, Network management and services, Neural Network, Fuzzy logics, Neuro-Fuzzy, Expert approaches, Innovation Technology and Management : Innovation and product development, Emerging advances in business and its applications, Creativity in Internet management and retailing, B2B and B2C management, Electronic transceiver device for Retail Marketing Industries, Facilities planning and management, Innovative pervasive computing applications, Programming paradigms for pervasive systems, Software evolution and maintenance in pervasive systems, Middleware services and agent technologies, Adaptive, autonomic and context-aware computing, Mobile/Wireless computing systems and services in pervasive computing, Energy-efficient and green pervasive computing, Communication architectures for pervasive computing, Ad hoc networks for pervasive communications, Pervasive opportunistic communications and applications, Enabling technologies for pervasive systems (e.g., wireless BAN, PAN), Positioning and tracking technologies, Sensors and RFID in pervasive systems, Multimodal sensing and context for pervasive applications, Pervasive sensing, perception and semantic interpretation, Smart devices and intelligent environments, Trust, security and privacy issues in pervasive systems, User interfaces and interaction models, Virtual immersive communications, Wearable computers, Standards and interfaces for pervasive computing environments, Social and economic models for pervasive systems, Active and Programmable Networks, Ad Hoc & Sensor Network, Congestion and/or Flow Control, Content Distribution, Grid Networking, High-speed Network Architectures, Internet Services and Applications, Optical Networks, Mobile and Wireless Networks, Network Modeling and Simulation, Multicast, Multimedia Communications, Network Control and Management, Network Protocols, Network Performance, Network Measurement, Peer to Peer and Overlay Networks, Quality of Service and Quality of Experience, Ubiquitous Networks, Crosscutting Themes – Internet Technologies, Infrastructure, Services and Applications; Open Source Tools, Open Models and Architectures; Security, Privacy and Trust; Navigation Systems, Location Based Services; Social Networks and Online Communities; ICT Convergence, Digital Economy and Digital Divide, Neural Networks, Pattern Recognition, Computer Vision, Advanced Computing Architectures and New Programming Models, Visualization and Virtual Reality as Applied to Computational Science, Computer Architecture and Embedded Systems, Technology in Education, Theoretical Computer Science, Computing Ethics, Computing Practices & Applications

Authors are invited to submit papers through e-mail ijcsiseditor@gmail.com. Submissions must be original and should not have been published previously or be under consideration for publication while being evaluated by IJCSIS. Before submission authors should carefully read over the journal's Author Guidelines, which are located at <http://sites.google.com/site/ijcsis/authors-notes>.

**© IJCSIS PUBLICATION 2016
ISSN 1947 5500
<http://sites.google.com/site/ijcsis/>**