4-21-2012

International Conference on Computer Science & Information Technology

Prof.Srikanta Patnaik Mentor
IRNet India, patnaik_srikanta@yahoo.co.in

Proceedings

of

International Conference

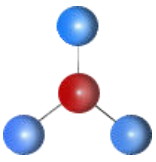
on

COMPUTER SCIENCE & INFORMATION TECHNOLOGY

*IC*CSIT

April 21st, 2012.

Organised By :



Interscience Research Network (IRNet)

Bhubaneswar, India

Mail To: irnet.chapter@gmail.com

About **ICCSIT-2012**

Computer Science and Information Technology have a profound influence on all branch of science, engineering, management as well. New technologies are constantly emerging, which are enabling applications in various domains and services. International Conference on Computer Science and Information Technology (CSIT) is organized by IOAJ for the presentation of technological advancement and research results in the fields of theoretical, experimental, and applied area of Computer Science and Information Technology. CSIT aims to bring together developers, users, academicians and researchers in the information technology and computer science for sharing and exploring new areas of research and development and to discuss emerging issues faced by them. *Topics of interest for submission include, but are not limited to*:

Algorithms
Artificial Intelligence
Automated Software Engineering
Bio-informatics
Bioinformatics and Scientific Computing
Biomedical Engineering
Compilers and Interpreters
Computational Intelligence
Computer Animation
Computer Architecture & VLSI
Computer Architecture and Embedded Systems
Computer Based Education
Computer Games
Computer Graphics & Virtual Reality
Computer Graphics and Multimedia
Computer Modeling
Computer Networks
Computer Networks and Data Communication
Computer Security
Computer Simulation
Computer Vision
Computer-aided Design/Manufacturing
Computing Ethics
Computing Practices & Applications
Control Systems
Data Communications
Data Compression
Data Encryption
Data Mining
Database Systems
Digital Library
Digital Signal and Image Processing
Digital System and Logic Design
Distributed and Parallel Processing
Distributed Systems
E-commerce and E-governance
Event Driven Programming
Expert Systems
High Performance Computing
Human Computer Interaction
Image Processing
Information Retrieval
Information Systems
Internet and Web Applications
Knowledge Data Engineering
Mobile Computing
Multimedia Applications
Natural Language Processing
Neural Networks
Parallel and Distributed Computing
Pattern Recognition
Performance Evaluation
Programming Languages
Reconfigurable Computing Systems
Robotics and Automation
Security & Cryptography
Software Engineering & CASE
System Security
Technology in Education
Technology Management
Theoretical Computer Science
Ubiquitous Computing
Wireless Sensor Networks
Wireless Communication and Mobile Computing

Organizing Committee

Programmme Chair

Prof. (Dr.) Srikanta Patnaik
Chairman, I.I.M.T., Bhubaneswar
Intersceince Campus,
At/Po.: Kantabada, Via-Janla, Dist-Khurda
Bhubaneswar, Pin:752054. Orissa, INDIA.

Team IOAJ:

Secretary:
Prof. Mritunjay Sharma
IOAJ, Bhubaneswar

Conference Coordinator;
Mr. Ajit Dash
IOAJ,Bhubaneswar
Mob:09582447024

Team Members:

Prof. Sharada Prasad Sahoo
Mr. Bikash chandra Rout
Ms. Susobhita Rani Rath
Mr. Rashmi Ranjan Nath
Mr. Prasannajit Rout
Ms Abhilipsa Mohanty
Ms. Neelima Sutar

Technical Programme Committee

Prof. Sushanta Panigrahi, IIMT, Bhubaneswar
Prof. Debashish Sahoo, IIMT, Bhubaneswar
Prof. Chittaranjan Panda, MIET, Bhubaneswar
Prof. Sanjay Sharma IIMT, Bhubaneswar

Post Conference Coordinator:
Miss Litun Pradhan
Mobile No: +91 8895995279

First Impression : 2012

Proceedings of International Conference on

COMPUTER SCIENCE & INFORMATION TECHNOLOGY

DISCLAIMER

The authors are solely responsible for the contents of the papers complied in this volume. The publishers or editors do not take any responsibility for the same in any manner. Errors, if any, are purely unintentional and readers are requested to communicate such errors to the editors or publishers to avoid discrepancies in future.

ISBN: 978-93-81693-54-4

Published by :

IOAJ
At/PO.: Kantabada, Via: Janla, Dist: Khurda, Pin- 752054
Publisher's Website : www.interscience.in
E-mail: ipm.bbsr@gmail.com

Typeset & Printed by :
IPM PVT. LTD.

TABLE OF CONTENTS

Editorial

The mushrooming growth of the IT industry in the 21st century determines the pace of research and innovation across the globe. In a similar fashion Computer Science has acquired a path breaking trend by making a swift in a number of cross functional disciplines like Bio-Science, Health Science, Performance Engineering, Applied Behavioral Science, and Intelligence. Still there remains a substantial relativity in both the disciplines which underscores further extension of existing literature to augment the socio-economic relevancy of these two fields of study. The IT tycoon Microsoft addressing at the annual Worldwide Partner Conference in Los Angeles introduced Cloud ERP (Enterprise Resource Planning,) and updated CRM (Customer Relationship Management) software which emphasizes the ongoing research on capacity building of the Internal Business Process. It is worth mentioning here that Hewlett-Packard has been with flying colors with 4G touch pad removing comfort ability barriers with 2G and 3G. If we progress, the discussion will never limit because advancement is seamlessly flowing at the most efficient and state-of-the art universities and research labs like Laboratory for Advanced Systems Research, University of California. Unquestionably apex bodies like UNO, WTO and IBRD include these two disciplines in their millennium development agenda, realizing the aftermath of the various application projects like VSAT, POLNET, EDUSAT and many more. 'IT' has magnified the influence of knowledge management and congruently responding to social and industrial revolution.

The conference is designed to stimulate the young minds including Research Scholars, Academicians, and Practitioners to contribute their ideas, thoughts and nobility in these two integrated disciplines. Even a fraction of active participation deeply influences the magnanimity of this international event. I must acknowledge your response to this conference. I ought to convey that this conference is only a little step towards knowledge, network and relationship. We must concertedly prove ***"When Knowledge is Power Sky has the limit,"*** The areas covered under the auspices of this conference are:

Algorithms	Artificial Intelligence
Automated Software Engineering	Bio-informatics
Bioinformatics and Scientific Computing	Biomedical Engineering
Compilers and Interpreters	Computational Intelligence
Computer Animation	Computer Architecture & VLSI
Computer Architecture and Embedded Systems	Computer Based Education
Computer Games	Computer Graphics & Virtual Reality
Computer Graphics and Multimedia	Computer Modeling
Computer Networks	Computer Networks and Data Communication
Computer Security	Computer Simulation
Computer Vision	Computer-aided Design/Manufacturing
Computing Ethics	Computing Practices & Applications

Control Systems	Data Communications
Data Compression	Data Encryption
Data Mining	Database Systems
Digital Library	Digital Signal and Image Processing
Digital System and Logic Design	Distributed and Parallel Processing
Distributed Systems	E-commerce and E-governance
Event Driven Programming	Expert Systems
High Performance Computing	Human Computer Interaction
Image Processing	Information Retrieval
Information Systems	Internet and Web Applications
Knowledge Data Engineering	Mobile Computing
Multimedia Applications	Natural Language Processing
Neural Networks	Parallel and Distributed Computing
Pattern Recognition	Performance Evaluation
Programming Languages	Reconfigurable Computing Systems
Robotics and Automation	Security & Cryptography
Software Engineering & CASE	System Security
Technology in Education	Technology Management
Theoretical Computer Science	Ubiquitous Computing
Wireless Sensor Networks	Wireless Communication and Mobile Computing

The conference is first of its kind and gets granted with lot of blessings. About 150 papers were received and after scrutiny 35 papers were selected for publication in the proceedings. I wish all success to the paper presenters. The papers qualifying the review process will be published in the forthcoming IOAJ journal.

I congratulate the participants for getting selected at this conference. I extend heart full thanks to members of faculty from different institutions, research scholars, delegates, IOAJ Family members, members of the technical and organizing committee. Above all I note the salutation towards the almighty.

Editor-in-Chief

Prof. (Dr.) Srikanta Patnaik
Chairman, I.I.M.T., Bhubaneswar
Intersceince Campus,
At/Po.: Kantabada, Via-Janla, Dist-Khurda
Bhubaneswar, Pin:752054. Orissa, INDIA.

An Efficient Routing Security through Cyptographic and Trust-Based methods for MANET

V. Anitha & A.Gayathri

Computer Science and Engineering ,Sri Venkateswara College of Engineering, Chennai, India
E-mail : anithavenugopaal@gmail.com & replygayathri@gmail.com

Abstract - Mobile ad-hoc networks (MANETs) allows wireless nodes to form a network without requiring a fixed infrastructure. This new generation of networks is different from the earlier one in many aspects like network infrastructure, resources and routing protocols, routing devices etc. These networks are bandwidth and resources constrained with no network infrastructure and dedicated routing devices. Every node in such networks has to take care of its routing module itself. These characteristics become reasons for the importance of security in mobile ad-hoc networks as there is a very high probability of attacks in such networks. Some work has been done to compare different protocols on basis of security but keeping in view the resource limitations in such networks, evaluation based in networking context is also important. The present paper details the newly proposed SAODV using Elliptic Curve Cryptography instead of RSA and TAODV and compares these protocols which address routing security through cryptographic and trust-based means respectively.

Keywords – *Security, Routing, Cryptography, SAODV, TAODV, Elliptic Curve Cryptography.*

I. INTRODUCTION

Mobile Ad hoc Network (MANET) is a collection of communication devices or nodes that wish to communicate without any fixed infrastructure and pre-determined organization of available links. A MANET is referred as an infrastructure less network, because the mobile nodes in the network dynamically set up paths among themselves to transmit packets. Application of MANET includes battlefield applications, search and rescue operations as well as civilian applications such as e-commerce, business, vehicular services and shopping and other networking applications. The main challenges of MANET are Absence of infrastructure, Wireless links between nodes, Limited physical protection, Lack of centralized monitoring, Security, Routing, Quality of Services (QoS) and Reliability. Of which, Security is an important issue for Mobile ad hoc Network. Basic security requirements of MANET are Authentication, Confidentiality, Integrity, Non repudiation and availability. Security is considered as an important requirement due to the reason that many upcoming applications demand high security infrastructure. Since there is no fixed infrastructure, the nodes in the network forward traffic for one another in order to allow communication between nodes that are not within physical radio range. Nodes must also be able to change how they forward data over the network as individual nodes move around and acquire or lose neighbors i.e. nodes within radio range. Routing protocols are used to determine how to forward the data as well as how to adapt to topology changes resulting from mobility. Initial MANET routing protocols, such as AODV, were not designed to withstand malicious nodes within the network or outside attackers with malicious intent. Subsequent protocols and protocol extension have been proposed to address the issues of security. It is in this context that this paper considers two proposed protocol extension to secure MANET. The first, SAODV uses cryptographic method to secure the routing information in the AODV protocol. Key Management is the core component of the security infrastructure. For an effective routing, Elliptic Curve Cryptography is used in SAODV protocol which increases faster processing time, lower demands on memory and bandwidth since it is mobile nodes it has limited battery power and limited computational power. Consequently this type DoS attack allows for an attacker effectively shutdowns nodes or otherwise disrupt the network. The second, TAODV uses trust metrics to allow for better routing decisions and penalize uncooperative nodes. While some applications may be able to accept SAODV's vulnerability to DoS or TAODV's weak preventative

security, most will require an intermediate protocol tailored to the specific point on the DoS/security trade-off that fits the application. The tailored protocols for these applications will also require performance that falls between that of SAODV and TAODV. Understanding how the SAODV and TAODV protocols perform on simulation and to what extent there exists a performance gap is a prerequisite for being able to develop the intermediate protocols. Such evaluation is not only required for developing intermediate protocols, but also for determining the direction for development of new trust metrics for ad-hoc networks.

II. RELATED WORK

Several protocols have been proposed for ad hoc routing. Overview of the existing protocols and their comparisons. C.E Perkins and E.M Royer proposed Ad-hoc On-Demand Distance Vector Routing (AODV) [3] routing protocol for mobile ad hoc networks. This protocol is focused on problems that mobility presented to accurate determination on routing information. The problem in AODV is that it is not designed to withstand malicious nodes within the network or outside hackers with malicious intent. N. Asokan and M.G Zapata proposed secure ad hoc routing protocol for securing AODV protocol [4]. SAODV allows authenticating the AODV routing data. Cryptographic functions are used to secure AODV through digital signatures and hash function for RREQ, RREP or HELLO messages. SAODV requires heavyweight asymmetric cryptographic operations. This gets worse when double signature mechanism is used because of two signatures for a single message. Jared Cordasco, Susanne Wetzel proposed Cryptographic versus Trust based method for MANET routing security [7] which shows the comparison results of SAODV and TAODV. In SAODV, Digital Signature performed is 512 bit RSA key pair which increases the processing time for Digital Signature generation/verification in every node. It is also implemented that SAODV uses 256 bit RSA key pair for DSA which reduces the security where a malicious node can quickly verify the signature. In TAODV, the trust metric used should be more secure i.e. instead of finding the shortest path more secured path is to be chosen. Mohd Anuar, Jaafar and Zuritai Ahmad Zukarnain proposed Performance Comparisons of AODV, Secure AODV and Adaptive Secure AODV routing protocols [10] is compared in free attack simulation environment. But it is not simulated when a malicious nodes attack the routing data. F. Maan, Y. Abbas, N. Mazhar proposed Vulnerability Assessment of AODV and SAODV Routing protocols Against Network Routing Attacks [1] proposed security scheme called R-SAODV is able to address the security flaws of SAODV and allows to counter the replay attacks. However SAODV and R-SAODV have similar performance which implies that are able to achieve more security with R-SAODV at marginal additional cost.

III. PROBLEM FORMULATION

The main problem addressed in the existing paper is formulated as follows. In SAODV specification, the longest key length that can be used for the digital signature is 512 bit- RSA key pair. Due to the longest key size, processing time for signature in every node is high. The problem is the increased message size. For example, with SAODV's most basic signature method, the Single Signature Extension (SSE), and a 512 bit RSA key, a 24 byte RREQ message is extended to 198 bytes and 20 byte RREP and HELLO message become 194 bytes in length. Due to the increased byte length it reduces processing power, storage space, and bandwidth. So power consumption is more because it is mobile nodes.

IV. OVERVIEW OF AODV

The AODV routing protocol [2] is an on-demand variation of the distance vector routing protocol. When a source node desires to send a message to a certain destination node to which it does not have a valid route, it initiates a route discovery process. The source node broadcast an RREQ (Route REQuest) message to its neighbors, which then forward the request to their neighbors, and so on, until either the destination in its routing table is reached. During the process of forwarding the RREQ, an intermediate node record in its routing table (i.e. precursor lost) the address of the neighbor from which the first copy of the broadcast packet is received, thereby establishing a reverse path. Additional copies of the same RREQ receiver later are discarded. Once the RREQ reaches the destination or an intermediate node with a route, the respective node responds by unicasting an RREP (Route REPly) message back to the neighbor from which it first received the RREQ, which relays the RREP backward via the precursor node to the source node. Routes are maintained as follows: HELLO beacons are sent periodically via broadcast to the neighboring nodes. When a source node moves, it has to re-initiate the route discovery protocol to find a new route to the destination. On the other hand, when an intermediate node along the route moves, its upstream neighbor will notice route breakage due to the movement and propagate an RERR (Route ERROR) message to each of its active upstream neighbors. These nodes in turn propagate the RERR packet to their upstream neighbors, and so on until the source node is reached. The source node may then choose to re-initiate the route discovery for that destination if a route is still desired. SECURITY ISSUES IN AODV In this section, analyze the security

threats and describe the requirements for AODV routing protocol to mitigate these threats. A node is malicious if it is an attacker that cannot authenticate itself as a legitimate node due to the lack of valid cryptographic information. A node is compromised if it is an inside attacker who is behaving maliciously but can be authenticated by the network as a legitimate node and is being trusted by other nodes. A node is selfish when it tends to deny providing services for the benefit of other nodes in order to save its own resources. Several attacks [2, 1] can be launched against the AODV routing protocol:

1. Message tampering attack

2. Message dropping attack

3. Message Replay (or Wormhole) attack

The security requirements [1] for AODV routing protocol include:

1. Source Authentication: The receiver should be able to confirm that the identity of the source is indeed who or what it claims to be

2. Neighbor Authentication: The receiver should be able to confirm that the identity of the sender (i.e. one hop previous node) is indeed who or what it claims to be.

3. Message Integrity: The receiver should be able to verify that the content of a message has not been altered either maliciously or accidently in transit.

4. Access Control: It is necessary to ensure that mobile nodes seeking to gain access to the network have the appropriate access rights.

V. PROPOSED METHOD SAODV USING ECC METHOD

Proposed Work is to focus on faster computations, as well as memory and bandwidth savings. This is done through the reduced key size implementing ECC in SAODV. Secure AODV (SAODV) extends the AODV message format to include security parameter for securing the routing message. Considering RREQ and RREP or RERR message in SAODV protocol there are two alternatives for ensuring secured route discovery; first, only destination is allowed to reply a RREP and the second, any intermediate node which has valid routing information allowed to reply a RREP. Two mechanisms are used to secure the message. Digital Signatures is used to authenticate non-mutable field and Hash chain to secure mutable field like hop count information. Here the Digital Signature is performed using 112 bit ECC key pair. Elliptic Curve Cryptography (ECC) [5] is emerging as an attractive public key cryptosystem for mobile and wireless environments. ECC offers equivalent security with smaller key sizes, when compared to RSA method. An ECC operates over points on an Elliptic curve. The way that the elliptic curve operations are defined is what gives ECC its higher security at smaller key size. An elliptic curve is defined in a standard, two dimensional (x, y). Cartesian coordinate system by an equation of the form, $y^2 = x^3 + ax + b \pmod p$ KEY GENERATION:

1. Select a random or pseudorandom in the interval

[n-1].

2. Compute the product Q=dG.

3. A's public key is Q and A's private key is d.

As per SAODV specification, the longest key length that can be used for digital signature is only 512 bits. There are two main issues with using stronger key lengths. The first is obviously the computational overhead required for the larger key length. The other is more important in ad-hoc networks than in other settings where communication medium is more reliable. The problem is increased message size and increases computational power. This can be reduced by using ECC- 112 bit key length which offers more secure with decreased key size. For example, using 112 bit ECC key, 198 bytes RREQ message becomes 144 bytes and 196 bytes RREP message becomes 140 bytes.

For non-mutable field the authentication is done in an End-to-end manner. The hash chain mechanism helps any intermediate node to verify that the hop count has not been decreased by any malicious node. A hash chain is formed by applying a one-way hash function repeatedly to a seed (random number). Since SAODV uses two way for performing verifying authentication message, signing and verifying mechanism by sender and receiver also differs up to some extent. In the first one, where only destination is allowed to reply, every time a RREQ is sent, the sender signs the message with its private key. An intermediate node verifies the

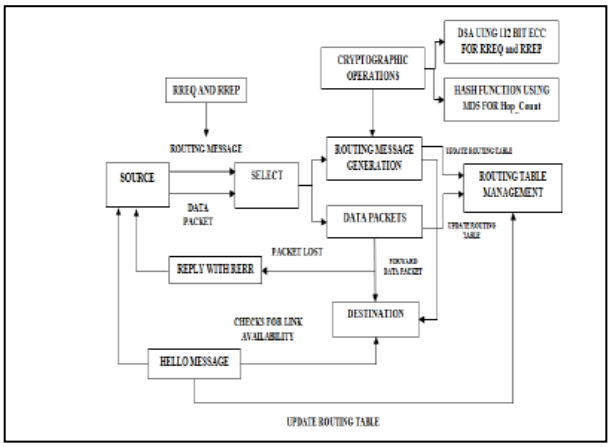


Figure 1: Architecture Diagram for SAODV using ECC

signature before creating or updating the reserve path to the source and stores it only if verification is successful. For RREP message the final destination node sign the message using its private key. Intermediate and final node again verifies the signature before creating a route to that host. In the second, RREQ message has a second signature that is always stored in the reserve path route. The second signature is needed to de added in the gratuitous reply. Of that RREQ and in regular RREPs to future RREQs that node might reply as an intermediate node. An intermediate that wants to reply a RREP needs not only the correct route, but also the signature corresponding to that route to add in the RREP and the lifetime and the originator IP address fields that work with that signature. All the nodes that receive the RREP and that update the route; store the signature, the lifetime and originator IP address with that route. SAODV does not take help of any extra message for security. The route discovery mechanism of SAODV has been concisely discussed in algorithm

Algorithm : SAODV Route Discovery algorithm

1. Sender Generates RREQ packet;
2. Sender signs all non-mutable fields (except hop count and hash chain fields) with its private key by ECC; Apply Hash to a seed to generate hash chain field;
   if (intermediate can reply) {
   clear destination only tag;
   include second signature in the signature extension;
   }
   Append signature extension to RREQ packet;
3. Broadcast RREQ to all neighbor nodes;
4. Intermediate node receives RREQ packet;
5. Node verifies signature with public key of source (from RREQ packet);
   If (valid packet)
   Then update routing information of source in any (establishment of reserve path);
6. if (destination I.P = = node I.P) {
   Generate RREP;
   Sign all the non- mutable fields (except hop count and Hash chain fields) with its private key;
   Apply Hash to a seed to generate hash chain field;
   Append signature extension to RREP packet;
   Unicast RREP to the neighbor which is the reserve path for the source node.
   }
   Else if (node has valid route for destination && !(Destination only tag)) {
   Generate RREP;
   Copy the signature and other necessary field of source to the signature extension; Sign all the non-mutable (except hop count and hash chain fields) with its private key;
   Apply Hash to a seed to generate hash chain field;
   Append signature extension to RREP packet;
   Unicast RREP to the neighbor which is the reserve path for the source node;
   }
   Else
   Forward RREQ to all its neighbouring node;

COMPARISON OF SAODV USING RSA AND SOADV USING ECC

The purpose of the section is to compare the processing time for digital signature generation/verification for RREQ and RREP or RERR messages while broadcasting to the destination. The AODV allow intermediate nodes to send back RREP messages. This complicates the digital signature signing process, due to the difficulties to verify the authenticity of this kind of RREPs. For SAODV, disable the intermediate nodes capability of sending RREPs. Only the route destination node will send a signed RREP message. Here the analysis is performed in NS2 simulation. The simulations were done with 20 nodes moving at a maximum speed of 10 meters per second. The below simulation shows that before broadcasting RREQ to destination it should be digitally signed by source with the use of public key crypto system. Here it evaluates the time taken for a node to sign the routing message by 512 bit RSA and 112 bit ECC key pair.

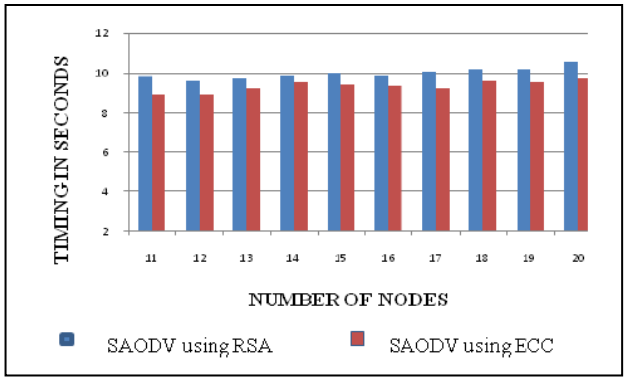


Figure 4: Processing Time For Digital Signature Generation Method For RREQ And RREP

The below simulation analysis that the amount of time taken for a node to verify the signature which is signed for RREQ and RREP message.

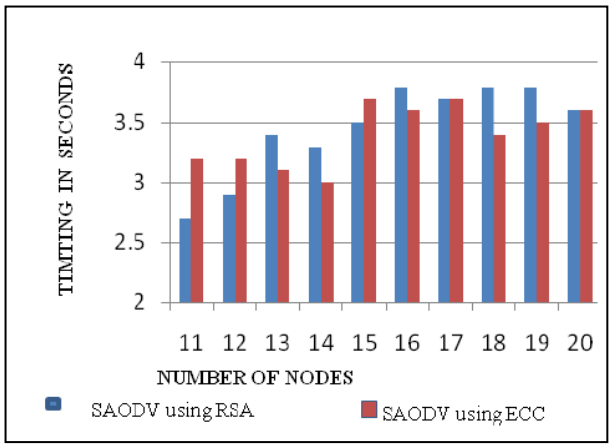


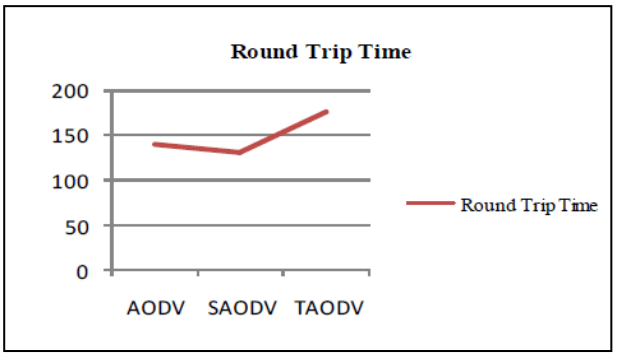
Figure 4: Processing Time For Digital Signature Verification Method For RREQ And RREP

TRUST-BASED AODV (TAODV)

A secure variant of the AODV protocol, SAODV, uses one way hash chains and digital signatures. But even SAODV fails to provide any information on route dependability. It only guarantees message authenticity. Security and robustness of the protocol would be improved if nodes could make informed decisions regarding route selection based on transmitted route request and additional information contained in received route replies. Thus, additional information on the nature of routes would enable the source node to choose a route that best serves its purpose. The source node could utilize route dependability information to increase the probability of its packets reaching the destination. In this paper, TAODV [10] protocol provides a Trust-based framework which uses Route Trust as a metric for the source node to make such informed route selection decisions.

VI. PERFORMANCE COMPARISON

Performance Comparison of protocols (AODV, SAODV, and TAODV) was done to determine the relative performance of AODV and its secure variants. Comparison is done in network simulator (ns2-2.30). Total number of nodes was varied from 20-100, with maximum speed of 20m/s for CBR traffic. In SAODV tests, measures the generation and validation of the SSE which requires hash computation and a digital signature/verification. The hash function used for the test is MD5 and the digital signature/verification performed using 112-bit ECC key pair. It measures how long a node able to generate SSE for RREQ, RREP or RERR messages. In TAODV test, an extra field is created in the route request format. This trust Value is updated on every successful communication. The forthcoming communication is based on the route selection value calculated for each RREQ path. This route selection value is used to select most trusted path rather than selecting shortest or longest path. This significantly improves the trust factor on the neighboring nodes in the network. This is useful in forthcoming communication in the network. This improves the security level and also prevents malicious node attack in the network. It is analyzed that TAODV is more faster than SAODV to send a data from source to destination because it does not incur any cryptographic operations. Based on the application, it selects which protocol to be implemented. While there is some expense for the trust calculations, it is not nearly as expense as the cryptographic operations. The analyses show that TAODV is indeed at the opposite end of the trade-off from SAODV. This is due to the fact that the TAODV information itself in each packet is not secured. Overall it states that there is indeed a wide spectrum in the tradeoff between cryptographic security and DoS. By adding an appropriate lightweight security mechanism to secure the trust information in the routing packets a hybrid protocol can be created which is less expensive than SAODV and more secure than TAODV.



VII. CONCLUSION

In this paper, the result shows the comparison of SAODV and TAODV for securing ad-hoc network routing. The results are shown in simulation. The experiment shows that there is significant room between the two protocols for a secure hybrid protocol to be developed which takes the advantage of the strongest points of both. Further protocol design should seek to use various new combinations of smarter, trust-based metrics and lightweight security mechanism in order to develop hybrid protocols.

REFERENCES

[1] Y. Abbas, F. Maan, N. Mazhar ,"Vulnerability Assessment of AODV and SAODV Routing Protocols Against Network Routing Attacks and Performance Comparisons", In Wireless advanced (WiAd), 978-1-4577- 0110-8 © 2011 IEEE.

[2] H.S. Al-Raweshidy and M. F. Juwad, "Experimental Performance Comparisons between SAODV & AODV", IEEE Second Asia International Conference on Modelling & Simulation, 2008.

[3] Alessandro Ghioni and Davide Cerri, "Securing AODV: The A-SAODV Secure Routing Prototype", 0163-6804/08 © 2008 IEEE, IEEE Communications Magazine, February 2008.

[4] N. Asokan and M. G. Zapata, "Securing ad hoc routing protocols", In WiSE '02: Proceedings of the ACM workshop on Wireless security. ACM Press, 2002.

[5] Ertaul. L and W. Lu, "ECC Based Threshold Cryptography for Secure Data Forwarding and Secure Key Exchange in MANET (I)," Networking 2005, LCNS 3462, University of Waterloo, Canada, May 2005, pp.102-113.

[6] M. Jakobsson, S. Wetzel, and B. Yener. Stealth attacks on ad hoc wireless networks. In proceedings of VTC, 2003, 2003.

[7] Jared Cordasco, Susanne Wetzel (2008). Cryptographic Versus Trust-based Methods for MANET Routing Security, on Electronic Notes in Theoretical Computer Science 197 pp: 131–140, in Hoboken, New Jersey USA.

[8] Junaid Arshad and Mohammad Ajmal Azad, "Performance Evaluation of Secure on-Demand Routing Protocols for Mobile Ad-hoc Networks", 1-4244- 0626-9/06 © 2006 IEEE.

[9] R. S. Mangrulkar , Dr. Mohammad Atique, "Trust Based Secured Adhoc on Demand Distance Vector Routing Protocol for Mobile Adhoc Network'. In Wireless Communication and Sensor Networks (WCSN), 978-1-4244- 9731-7 © 2011 IEEE.

[10] Mohd Anuar Jaafar and Zuriati Ahmad Zukarnain , "Performance Comparisons of AODV, Secure AODV and Adaptive Secure AODV Routing Protocols in Free Attack Simulation Environment", In European Journal of Scientific Research,ISSN 1450-216X Vol.32 No.3 (2009), pp.430-443

[11] C. E. Perkins and E. M. Royer. Ad-hoc On-Demand Distance Vector Routing. Proceedings of the Second IEEE Workshop on Mobile Computer Systems and Applications (WMCSA), page 90, 1999.

[12] [Representation of elliptic curve digital signature algorithm keys and signatures] http://www.ietf.org.

❑❑❑

Enhanced Security In Cloud With Multi-Level Intrusion Detection System

M.Kuzhalisai & **G.Gayathri**

Computer Science And Engineering, Sri Sairam Engineering College, Chennai, India
E-mail : kuzhalisai6@gmail.com & gayu.govindaraj@gmail.com
Co-author : Mrs. MANIMALA G M.E

Abstract Cloud computing is a new type of service which provides large scale computing resource to each customer. Cloud Computing Systems can be easily threatened by various cyber attacks, because most of Cloud computing system needs to contain some Intrusion Detection Systems (IDS) for protecting each Virtual Machine (VM) against threats. In this case, there exists a trade-off between the security level of the IDS and the system performance. If the IDS provide stronger security service using more rules or patterns, then it needs much more computing resources in proportion to the strength of security. So the amount of resources allocating for customers decreases. Another problem in Cloud Computing is that, huge amount of logs makes system administrators hard to analyse them. In this paper, we propose a method that enables cloud computing system to achieve both effectiveness of using the system resource and strength of the security service without trade-off between them.

Keywords- *IDS, Cloud Computing, Intrusion Detection, Multi-level IDS, Cooperative IDS.*

I. INTRODUCTION

As Green IT has been issued, many companies have started to find ways to decrease IT cost and overcome economic recession. Cloud Computing Service is a new computing paradigm in which people only need to pay for use of services without cost of purchasing physical hardware. For this reason, Cloud Computing has been rapidly developed along with the trend of IT services. Cloud Computing can be defined as internet-based computing, whereby shared resources, software, and information are provided to companies and other devices on demand (1).

It is efficient and cost economical for consumers to use computing resources as much as they need or use services they want from Cloud Computing provider. Especially, Cloud Computing has been recentlymore spotlighted than other computing services because of its capacity of providing unlimited amount of resources. Moreover, consumers can use the services wherever Internet access is possible, so Cloud Computing is excellent in the aspect of accessibility. Cloud Computing systems have a lot of resources and private information, therefore they are easily threatened by attackers (2). Especially, System administrators potentially can become attackers. Therefore, Cloud Computing providers must protect the systems safely against both insiders and outsiders.

IDSs are one of the most popular devices for protecting Cloud Computing systems from various types of attack. Because an IDS observes the traffic from each VM and generates alert logs, it can manage Cloud Computing globally (3).

In this paper, we propose Multi-level IDS and log management method based on consumer behavior for applying IDS effectively to Cloud Computing system. The rest of the paper is organized as follows. In Chapter II we describe related works which are Cloud Computing and IDS. After that, we describe our proposal method in Chapter III. In Chapter IV, we evaluate our method. Finally, we conclude the paper in chapter in Chapter V.

II. RELATED WORK

A. Cloud Computing

Cloud Computing is a service that assigns virtualized resources picked from a large-scale resource pool, which consists of distributed computing resources in a Cloud Computing infra, to each consumer, Cloud Computing is a fused-type computing paradigm which includes Virtualization, Grid Computing , Utility Computing ,Server Based Computing (SBC) , and Network Computing , rather than a entirely new type of computing technique (3)(4).

Table 1 shows the description of each computing technique. Cloud Computing provider can assign large-scale resources to each consumer using these techniques. Cloud Computing uses hypervisor in order to provide virtual OS for users by using unified resource. Hypervisor is software which enables several OSs to be executed in a host computer at the same time. Hypervisor also can map the virtualized, logical resources onto physical resource. Hypervisor is sometimes called Virtual Machine Monitor (VMM), and several OSs which are operated in a host computer are called the guest Oss. A Hypervisor provides isolated Virtual hardware platform for operating guest Oss. Therefore, guest Oss are operated in each VM environment instead of real hardware. A host OS which provides the image of original OS to guest OS, can assign various type of OS other than the type OS of host itself. Figure I conceptually describes the organization of hypervisor, host OS, and guest OS.

TABLE I. USER RISK LEVEL

Technology	Definition
Virtualization	The creation of a virtual version of something, such as an operating system, a server, a storage device or network resources
Grid Computing	The virtualized combinationof computing power from multiple domain getting high capacity of computing resource(distributed computing architecture)
Utility Computing	Consumers pay for computing resources as much as they use without buying them.
Server Based Computing (SBC)	Any applications and data exist in server. Clients access the server and utilize them using Servers' computing power.
Network Computing	It is similar to SBC, but client loads applications and data from Server and utilizes them using local computing power.

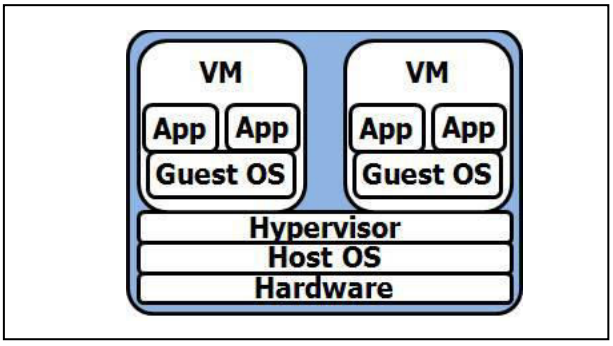


Figure2Proposal Multi-Level IDS Architecture

As figure 1, resource, instruction, and traffic of guest Oss in a hypervisor are mapped to a physical hardware through host OS.

Cloud Computing is a set which consists large amount and various types of computing resource, hypervisor, and data. Therefore Cloud Computing providers should own database centers to maintain their resources and data. Cloud Computing service is very attractive to consumers in the aspects of infinite scalability and payment cost in accordance with the amount of computing resource they used, however there also exists the risk that personal and private data are stored in uncontrolled place themselves (5). So Cloud Computing providers must protect their Cloud Computing system against all users include administrators and intruders (6).

B. IDS

IDS are software or hardware systems that automate the process of monitoring the events occurring in a computer system or network, analyzing them for signs of security problems (7). IDSs are one of widely used security technologies. An IDS alerts to system administrators, generate log about attack when it detects signature of accident according to host or network security policy. An IDS can be installedin a host or a network according to purpose.

An IDS detects attacks based on lots of rules each of which have unique signatures that describes attack patterns. So, the detection power of IDS increases when the number of rule grows. However the existence of more rules means that each incoming packet needs to be compared with more patterns. Thus large scale of rule causes system to become overloaded. In the Cloud Computing service, it isnecessary to allocate resources to users as much as possible. So it is important issue ot manage resources for reducing consumption of resources caused by implementing IDS.

In this paper, we propose the method for maintaining strength of security while minimizing waste of resources

III. MULTI-LEVEL IDS AND LO MANAGEMENT METHOD

We propose the Multi –level IDS method for implementing effective IDS in Cloud Computing system. Multi-level IDS method leads to effective resource usage by applying differentiated level of security strength to users based on the degree of anomaly. It is true that Cloud Computing is easy to be target of attach (9). For this reason, it is possible to judge all users and administrators as potential attacker and apply strong security policy to all traffic, but it is not efficient at all. So we propose the method that binds

users to different security group in accordance with degree of anomaly, called anomaly level in this paper. Our proposal architecture is as shown in figure 2.

AAA is a management module for authentication, authorization, and accounting. When a user tries to access Cloud Computing system, then AAA checks the user's authentication information. If the user is authenticated, then AAA gets the user's anomaly level, which has been most recently generated, by inspecting the user's information in the database. After that, AAA chooses suitable IDS which have the security level correspondent to the user's anomaly level. Then AAA requests the host OS, in which the chosen IDS is installed, to assign guest OS image for the user.

Storage center stores private data of users. All users ' data is logically isolated. So nobody can access the data except owners of the data and users who have been given access right by owner. After a user is assigned a guest OS, the connection between the guest OS and data owned by the user in storage center is then established. Figure 3 shows this relationship.

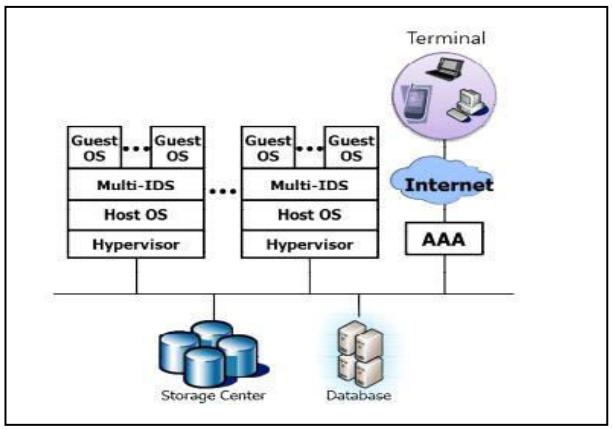


Figure 2. Proposal Multi-level IDS Architecture

In our paper, we divide security level in to three, such as High, Medium, and Low for effective IDS construction. High-level is a group which applies patterns of all known attacks and a portion of anomaly detection method when it needs, for providing strong security services. Medium-level is a group of middle grade which apply patterns of all known attacks to rules for providing comparatively strong security service. Finally, Low-level is a group for flexible resource management which apply patterns of chosen malicious attacks that occur with high frequency and that affect fatally to the system.

In Multi-level IDS scheme, an IDS consumes more resource when providing higher level security, because higher level security apply more rules than lower level. On the other hand, if an IDS provides lower level security policy, then the amount of resource usage is decreased although the detecting power of attacks also drops. The assignment of VM to a user is determined in accordance with security level. The grade of VM is proportional to user criteria of anomaly level. Anomaly levels of users are estimated by their behaviors during the usage of service based on saved user anomalylevel in system. For instance, when a user access Cloud Computing system first time, Multi-level IDS judges anomaly level of user using following matters: the user's IP coverage, vulnerable ports to attack, the number of ID/PW failure, and so on. The most important element for estimating anomaly level is how fatal it is. The rest of judgment criteria are possibility to attack success, possibility to attack occurrence, and OS on (1). Possibility to attack success is an experimental value which indicates the probability of success for an attack. Possibility to attack occurrence is a value based on the frequency of specific attack.

TABLE 2. USER RISK LEVEL

	Likelihood of incident scenario	Very Low	Low	Medium	High	Very High
Business Impact	Very Low	0	1	2	3	4
	Low	1	2	3	4	5
	Medium	2	3	4	5	6
	High	3	4	5	6	7
	Very High	4	5	6	7	8

Multi-level IDS defines the anomaly behaviors by risk level policy such as table-1. The risk levels assign risk points in proportion to risk of anomaly behavior. The criteria of behaviors for judging that some traffic is anomalous are described in table 3(2).

Cloud Computing security system evaluates user anomaly level according to assessment criteria in table 3. Multi-level IDS accumulates risk point to each user when they are against more than one rule in assessment rules. When a user is assigned a VM by the system first time, there is no data for determining which security level of IDS is suitable for the user, so a high-level IDS should be assigned to the user.

Since, first provisioning, the decision of which VM is to be assigned to the user may change according to anomaly level of the user, and a migration may occur. Migratio is a technique to move VM to other VM space (8). Cloud Computing system checks users' behaviors

everyday and decreases 1 risk point if a user uses Cloud Computing service more than one hour and increases less than 3 risk points a day .

Anomalous activity traffic	Risk point
Attempt to administrator account without working time	8
Guest OS attempt to unauthorized memory space	7
The user set Network Interface Card to promiscuous mode	6
Traffic of a guest OS increases up to 500% than usual traffic	6
IP address of user terminal is changed during the usage Cloud service	6
Host OS manager attempts to access some guest OSs	5
An guest OS attempts to other guest OSs	5
Traffic of a guest OS increases up to 300% than usual traffic	4
Administrator access some host OSs without notice	4
Login failure for 5 times	3
Unlicensed IP coverage	3
Known-vulnerable port number	3
Undertaking malicious probes or scans	3
Non-updated Guest OS	3
Between guest OS connect session in the same host OS	2
Abnormal guest OS power-off	2
Traffic of a guest OS increases up to 150% than usual traffic	1

Table 3. ASSESSMENT OF ANOMALOUS

IV. ESTIMATION

In this paper, our method increases resource availability of Cloud Computing system and handle the potential threats by deploying Multi-level IDS and managing user logs per group according to anomaly level. We can suppose that VMs have equal quantity of resource, then host OS can assign less guest OS with IDS, because IDS use much resource.

The criteria of anomaly level for deciding security group with risk point is shown in table 4.

Table 4.CRITERIA FOR ANAMALY LEVEL

IDS group	Standard
High-Level IDS	More then 6
Medium-Level IDS	3-5
Low-Level IDS	0-2

On the other hands, we can assign more guest OS with Multi-level IDS, because the user classified as low-level group are judged that they are normal user. As a result low-level IDSs maintain little rules for managing effective resource, so it can assign more guest OS than high and medium-level. Our method also supports classifying the logs by anomaly level, so it makes the system administrator to analyze logs of the most suspected users first. Therefore our method provides high speed of detecting attacks.

V. CONCLUSION

Cloud Computing technology provides human to the advantages such as economical cost reduction and effective resource management, However, if security accidents occurs, ruinous economic damages are inevitable. The system is very effective for the varied applications. The type of IDS that is needed for the specified purpose can be adapted as per the needs . Also the data traffic in the cloud is minimized and security is enhanced .

ACKNOWLEDGMENT

It is a pleasure to express our heartfelt thanks to Prof. N. NITYANANDAM, Head of the Department, Computer Science and Engineering for his encouragement and valuable guidance. We express our heartfelt gratitude to our project coordinator Mrs.V.HEMA, Senior Lecturer, Computer Science and Engineering, for his guidance to our project .We express our gratitude and sincere thanks to our guide Mrs. MANIMALA G, Senior Lecturer, Computer Science and Engineering, for her invaluable suggestions and constant encouragement for successful completion of this project. Finally we wish to thank all the members of our college, staff, lab coordinators and technicians without whom, this project would not have been successful.

REFERENCES

[1] Wikipedia, http:// en.wikipedia.org/ wiki/ Cloud_computing

[2] Ensia, Cloud Computing Risk Assessment, Nov. 2009

[3] Roberto Di Pietro and Luigi V .Mancini, Intrusion Detection Systems,Springer, Jan 2008.

[4] JaeHyuk Jang, Cisco, Cloud Computing: Drive Business Paradigm Shift, 2010.

[5] Cloud Security Alliance, Security Guidance for Critical Areas Of Focus in Cloud Computing, Dec.2009.

[6] N. Gruschka and M.Jensen, "Attack Surface: A Taxonomy for Attacks on Cloud Services", IEEE 3rd International Conference on Cloud Computing, pp 276-279, 2010.

[7] Rebecca Nace and Peter Mell, NIST Special Publication on Intrusion Detection Systems, 16 Aug.2001

[8] Kento S, Hitoshi. S Satoshi. M, "A Model-based Algorithm for Optimizing I/O Intensive Applications in Cloud using VM-Based Migration", 9th IEEE? ACM International Symposium, Cluster Computing and Grid, 2009.

Optimal Decoding of Linear Block Codes using Ordered Statistic Decoding and Adaptive Belief Propagation

Vishnu.S[1], Rachna Jaymohan Unnithan[2], Anju.C[3] and Devika Subash[4]

Department of ECE, Amrita School of Engineering, Coimbatore
E-mail : [1]svishnu.76@gmail.com, [2]unnithan.rachna@gmail.com
[3]chandran.anju@gmail.com, [4]devika.subash@gmail.com

Abstract - Reliability based decoding is based on the reliability of each bit. This reliability value of bits has been effectively used in various soft decision decoding algorithms of Linear Block Codes. OSD algorithm was used in linear block codes to achieve good error performance. ABP was also used which gave a better error performance but with higher complexity. Here OSD and ABP are combined to achieve a tradeoff between complexity and error performance.To further reduce the complexity the G bound criteria is implemented in OSD.

Keywords *-Linear Block Codes, Ordered Statistic decoding, Adaptive Belief Propagation.*

I. INTRODUCTION

Many Soft decision decoding has been implemented in linear block codes .OSD and BP was the most extensively used soft decision decoding algorithm. In both these methods reliability values of each bits is calculated. These reliability values help to differentiate between most reliable and least reliable bits. For certain block codes BP algorithm may suffer error propagation due the existence of short cycles in graph representations. In [1] an algorithm was proposed which adaptively modifies the parity check matrix into systematic form at each iteration which improved the error performance. But this algorithm suffers performance degradation because of the irremovable errors in the most reliable bits. The OSD [2] is one algorithm capable of correcting errors at the most reliable bit positions. so an algorithm is proposed in which OSD and ABP is combined so that the error performance is improved but with minimal increase in complexity. The soft outputs are exchanged between the OSD and ABP. This helps in improving the error performance.

II. PROPOSED WORK

In this proposed algorithm we fuse OSD and ABP to get better error performance with reduced complexity. First OSD (w) is done and checked for necessary conditions; if the conditions are satisfied then the obtained code word is theoptimum decoded code word. Else, we update the reliability values using ABP algorithm until we get the optimum code word.

III. SOFT DECISION DECODING ALGORITHMS

A. Ordered Statistic Decoding (OSD)

In general, it's known that MLD is achieved at the expense of great computational complexity for long codes but it has an efficient error performance which cannot be ignored. Hence, it is desirable to devise an algorithm which can achieve an optimum error performance as that of MLD along with significant reduction in the decoding complexity and such an algorithm is OSD[3]. This algorithm makes use of MRIP reprocessing algorithm that processes the MRIPs progressively in every stage based on the joint noise statistics after symbol reordering. These statistics are also used to evaluate the error performance after each stage and hence able to achieve the desired level of error performance.

Consider a binary (n, k, d_{min}) linear block code C with generator matrix G and parity check matrix H. Let y be the received sequence which has Gaussian noise with mean zero and variance $N_0/2$.the reliability of each code is calculated by

$$r(0) = \ln\left(\frac{\Pr\left(c_i = 0 / y_i\right)}{\Pr\left(c_i = 1 / y_i\right)}\right) = \frac{4}{N_0} y_i \qquad (1)$$

The $|r(c_i)|$ is sorted in descending order, based on the first kmost reliable independent position bits (MRIP) $I_0, I_1, \ldots\ldots I_k$ in r(ci), G is transformed into a systematic form G_1 by properrow operations such that columns

associated with the MRIP form and k × k permutation matrix. The first k symbols of r(c_i) are the most reliably independent positions; hence their hard decision will contain very few errors. Based on this concept as in [4], the algorithm proceeds.

For the OSD algorithm of order-w, it performs the following steps:

1. The hard-decision vector z is obtained from the r(ci).
2. Perform hard-decision decoding of the first k bits of r(c_i), which forms the information sequence u.
3. Then the code word v = uG_1 is constructed for the information sequence u, and compute the correlation discrepancy λ (r, v) of v.

   $\lambda(r,v)=\sum_{i\in D_1(v)}|r(c_i)|$ (2)

   where,

   $$D_1(v)=\{i: v_i \neq z_i \ \forall\ 0 \leq i < n\} \qquad (3)$$

4. For 1≤ l ≤ w, make all possible changes of l of the k most reliable bits in u. For each change, a new information sequence u is formed along with its corresponding v.
5. Compute the correlation discrepancy λ (v, y) for each generated code word.
6. After the l reprocessing phases, the v_{best} corresponding to the minimum λ is taken as the decoded code word.

The required order for OSD algorithm is $d_{min}/4$.The OSD algorithm of order-w consists of (w+1) reprocessing phases and requires processing of

$$1+\binom{k}{1}+\ldots\ldots+\binom{k}{w}$$

Candidate code words to make a decoding decision. Therefore, the number of code words that needs to be processed in OSD is far less when compared to the MLD which requires processing of 2^kcode words.

Ordered Statistic Decoding with G bound

The G bound is boundary value which tells the minimum allowable discrepancy for a particular code word. The G bound condition is included into OSD, so that itreduces the number of candidate code words that needs to be processed. Hence, the number of iterations and the decoding complexity is reduced. The G bound condition is:

$$G(\boldsymbol{v_{best}}, w_1)=\sum_{j=1}^{l+1}|r_{k-j}|+\sum_{j\in D_0^{(\delta)}(v_{best})}|r_j| \quad 4)$$

where,

$$\delta=\max\{0, d_{min}-|D_1(v_{best})|-(l+1)\}$$

and

$$D_0(v)=\{i: v_i=z_i\ \forall\ 0\leq i<n\}$$

$D_o^{(\partial)}(v_{best})$indicates the first δ elements of D_0(v). Aftereach l, the G bound condition is checked i.e.

$$\lambda(r, v_{best}) < G(v_{best}, w_1) \qquad (5)$$

If the correlation discrepancy is less than the G bound value, then the corresponding code word is the decoded codeword.

Adaptive Belief Propagation (ABP)

Belief propagation is a message passing algorithm which has proved to be a general approved approximate algorithm on general graphs. But for codes of practical block length, the BP decoding does not achieve appropriate approximate error performance as in [5].An algorithm has been developed in [1] where the code is modified adaptively after every iteration so that the bit reliabilities of the BP algorithm can converge more approximately towards the correct codeword. This shows much improvement in word error rate (WER) when compared to other soft decision decoding techniques.

Let y be the received sequence. The reliability values are calculated by

$$R(0)=\ln\left(\frac{\Pr\left(c_i=0/y_i\right)}{\Pr\left(c_i=1/y_i\right)}\right)=\frac{4}{N_0}y_i \qquad (6)$$

Sort the R(c_i) in the ascending order .Sort the parity check matrix corresponding to received sequence so that the first n-k columns forms a systematic matrix each column corresponding to the least reliable bits. If the parity check matrix conditions are satisfied for a particular received sequence, then that sequence is considered to be the desired codeword and we stop the iteration. If the condition is not satisfied the LLR values are updated using of the Sum Product Algorithm which produces external information R_{ext}as in [6]. Thus the updated R values can be obtained by

$$R_{j+1} = R_j + \alpha R_{ext} \tag{7}$$

where j is the iteration number and α is the damping coefficient and 0 < α < 1.This is continued until a predetermined number of iterations or until the parity check conditions are satisfied. We calculate the external LLR value as in [7].

$$R_{ext}^{(l)} = \sum_{j \in \theta_i} 2\tanh^{-1}\{\prod_{m \in \mu_{j,i}} \tanh(\frac{R^{(l)}(c_m)}{2})\} \tag{8}$$

for $0 \leq i < n$, where

$$\theta_i = \{j | 0 \leq n-k, h_{j,i}^{(l)} = 1\}$$

and

$$\mu_{j,i} = \{m | 0 \leq m < n, h_{j,i}^{(l)} = 1\}$$

The desired codeword would be the codeword that satisfies the parity check equations.

OSD-ABP algorithm

The OSD-ABP algorithm aims at developing a soft decision decoding algorithm that gives an optimal decoded output with less complexity. The OSD-ABP algorithm is as follows.

1. First find the LLR values of the received sequencey.
2. Perform ordered statistic decoding of order-w.
3. Check for G-bound condition or the maximum number of iterations N_{max} for the OSD-ABP algorithm.
4. If the conditions are satisfied, then the resultant code word is the decoded code word.
5. Else update the LLR values using ABP and go back to step 2.

IV. SIMULATION RESULTS

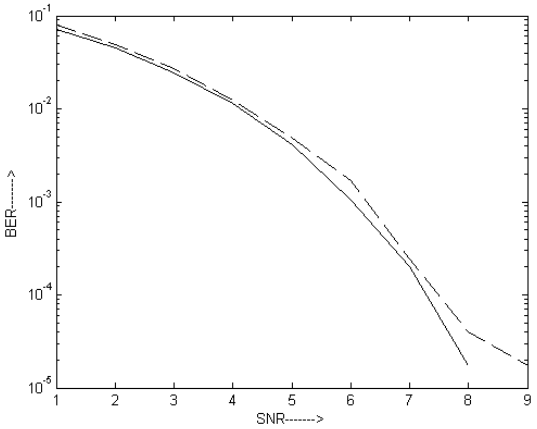


Fig: 1

———— OSD-ABP
— — — OSD

In this section hamming code (7,4,3) are simulated for performance verification. In this bits where transmitted over AWGN channel with BPSK modulation. From fig:1 it is found that OSD-ABP algorithm shows at least 0.1dB, 0.3 dB, and 0.1dB gain for the respective BER values 10^{-2},10^{-3} and 10^{-4} over the OSD algorithm.

S.NO	OSD		OSD-ABP	
	Bit Error	Symbol Error	Bit Error	Symbol Error
1	14039	4328	12610	3902
2	8655	2690	7999	2498
3	4803	1503	4280	1347
4	2183	686	2005	635
5	844	266	725	232
6	293	93	180	58
7	43	14	35	15
8	7	2	3	2
9	3	1	0	0
10	0	0	0	0

Table: 1 shows the symbol error rate for both OSD and OSD-ABP. The alpha value used here is 1 and the maximum number of iteration N_{max} = 10. Since there is bilateral exchange of soft information between OSD and ABP there is faster convergence rate.

V. PROPOSED RESULT

Hamming codes are codes with d_{min}=3.OSD of order 0 is sufficient to effectively decode the received sequence. In order to implement the algorithm with higher orders an alternate channel code such as BCH code can be used.

VI. CONCLUSION

In this study we found that the convergence rate of OSD is high but the error performance is low when compared to ABP. So the OSD algorithm is performed first and then the error performance is improved using ABP. So that there is only minimal increase in complexity when compared to ABP performed alone whereas achieving the same error performance as that of ABP.

REFERENCES

[1] J. Jiang and K. R. Narayanan, "Iterative soft decision decoding of Reed-Solomon codes based on adaptive parity check matrices," in Proc. 2004

IEEE Int. Symp. Inform. Theory, Chicago, IL, June 2004, p. 261

[2] Chung Hsuan Wang, Yu-Min Hsieh, and Hsin-Chuan Kuo, "Bilateral Exchange of Soft-Information for Iterative Reliability-Based Decoding with Adaptive Belief Propagation "IEEE Communication Letters, vol. 13, No. 9, Sept 2009.

[3] M. P. C. Fossorier and S. Lin, "Soft-decision decoding of linear block codes based on order statistics," IEEE Trans. Inform. Theory, vol. 41, pp. 1379-1396, Sept. 1995.

[4] Shu Lin and Daniel J.Costello, "Error Control Coding",Second Edition, Published in 2011, pp. 482-485

[5] J. S. Yedidia, J. Chen, and M. Fossorier, "Generating code representations suitable for belief propagation decoding," Tech. Rep. TR-2002-40, Mitsubishi Electric Research Laboratories, 2002

[6] A. Kothiyal and O. Y. Takeshita, "A comparison of adaptive belief propagation and the best graph algorithm for the decoding of block codes," in Proc. IEEE Int. Symp. on Inform. Theory 2005, pp. 724-728.

[7] J. Hagenauer, E. Offer, and L. Papke, "Iterative decoding of binary block and convolutional codes," IEEE Trans. Inform. Theory, vol. 42, March 1996.

❑❑❑

Particle Swarm Optimization Based Adaptive Traffic Flow Distribution In Computer Network

Anand Tilagul & Prasad A Y

Dept. of ISE S.J.C.I.T, College, Chickaballapura
E-mail : arilanand@gmail.com Mob - +91-9964498402

Abstract - Because of the stochastic nature of traffic requirement matrix, it's very difficult to get the optimal traffic distribution to minimize the delay even with adaptive routing protocol in a fixed connection network where capacity already defined for each link. Hence there is a requirement to define such a method, which could generate the optimal solution very quickly and efficiently. This paper presenting a new concept to provide the adaptive optimal traffic distribution for dynamic condition of traffic matrix using nature based intelligence methods. With the defined load and fixed capacity of links, average delay for packet has minimized with various variations of evolutionary programming and particle swarm optimization. Comparative study has given over their performance in terms of converging speed. Universal approximation capability, the key feature of feed forward neural network has applied to predict the flow distribution on each link to minimize the average delay for a total load available at present on the network. For any variation in the total load, the new flow distribution can be generated by neural network immediately, which could generate minimum delay in the network. With the inclusion of this information, performance of routing protocol will be improved very much.

Index Terms— *flow distribution, computer network, evolutionary programming, particle swarm optimization, artificial neural network.*

I. INTRODUCTION

Particle swarm optimization (PSO) is an optimization technique inspired from the interaction between swarm members that requires no supervision or prior knowledge and is based on primitive instincts. PSO technique has been applied to different layers of the open system interconnection (OSI) multilayer reference model which is designed for standard separation of network functionalities in communication

THE designing of computer network is always a challenging and fascinating task. Because, several domains have been integrated with network, present difficulties are manifold compare to earlier days of network evolution. But characteristics of fundamental problem, determining the most economic way to interconnect nodes while satisfying some reliability and quality of service constraints remain same even today. Two different types of network can be defined: (1) the centralized network: where server distributes transmission and resource access permission to all other nodes to the network. (2) The distributed network: where collectively nodes determine the order in which they can send information, by taking into account the multiplicity of available routes. In the deign of packet switched networks various aspects to be consider to achieve the objectives :(i) the topological configuration that refers to the set of links connecting nodes together, (ii) the traffic that corresponds to the number of packets exchanged per second between each node pair of the network to be designed, (iii) the capacity assignments that consists of determine the maximum number of bits per second (bps) that can be transmitted by each link of a given topological configuration, (iv) the routing scheme that allow selection of the best among the multiple routes connecting each node pair, (v) the flow control procedures, which assure that the quantity of information, sent by the emitter does not overwhelm the receiver.

Quality of network can be defined by several parameters like average delay and reliability of the network. As an index of quality of service, average packet delay in a network can be defined as the mean time taken by a packet to travel from a source to a destination node. The reliability is measured in terms of k-connectivity. Topological design of distributed packet switched networks can be viewed as a search of topologies that minimize communication cost by taking into account delay and reliability constraints. There exist a number of papers, which deal with such approaches has proposed the system called SIDRO using artificial intelligence techniques for the topological design of packet switch networks have proposed a hybrid method integrating both an algorithmic approach and a heuristic

knowledge-based system. Many papers have utilization of simulated annealing. Average transit delay of a packet through the network is one of the most important basic performance criteria. For a given network topology of switching nodes and partially connected by communication links; fixed link capacity and fixed traffic requirement; the packet delay is a function of routes employed in forwarding packets in the network. A congested link would be queued and experience excessive waiting time in queue before it can be served (transmitted). Finding the optimal route and hence optimal flow assignment so as to minimize the packet delay has thus become an important issue in the design of packet-switched communication networks. Multipath routing or spatial traffic dispersion is a load balancing technique in which the total load from a source to a destination is partially distributed over several paths. It is useful for relieving congestion and delivering quality of service guarantees in communication networks.

Optimization techniques developed for real search spaces can be applied on Integer Programming problems and determine the optimum solution by rounding the real optimum values to the nearest integer.

Multipath routing has been found to be an effective method to alleviate the adverse effects of traffic burst. In addition, multipath routing protocols helps to spread out congestion and thus minimize network delays. The key to multipath routing is how to allocate a proper portion of traffic to each participating path so as to satisfy the desired objectives, such as the minimization of the average end-to-end path delay. Most of the existing work considered the traffic arrival rate at every link in the network, and found an optimal routing which directs traffic exclusively on least-cost paths with respect to some link costs that depend on the flows carried by the links. It is computationally expensive to find an optimal flow assignment for such source-destination pair. The solution is generally not scalable in terms of the size of the network considered. Adaptive routing schemes have been proposed to spread packets dynamically over multiple paths according to the network load. These procedures require parameters to determine the load distribution. Yet the calculations of such parameters are either computationally intensive or done in an ad-hoc manner. Thus there is need for new multipath routing schemes that allow a rapid computation of the optimal load distribution parameters.

II. NETWORK DESCRIPTIONS: A MODEL APPROACH

A typical distributed computer network can be viewed as a two level hierarchical structure. First level consists of the communication sub network also called backbone. It is comprised of linked switching nodes and has as its main function the end-to-end transportation of information. The second level consists of terminals, workstations, multiplexers, printer and so on. In this paper design related to first level only focus. Each network link is characterized by a set of attributes, which principally are the flow and capacity. For a given link i, the flow fi is defined as the effective quantity of information transported by this link, while its capacity Ci is a measure of the maximal quantity of information that it can transmit. Flow and capacity are both expressed in bits/s (bps). Capacity options are only available on the market in discrete or modular options. The traffic Yij between a node pair (i,j) represents the average number of packets/s sent from source i to destination j. The flow of each link that composes the topological configuration depends on the traffic matrix. Indeed this matrix is varies according to the time, the day and application used.

III. PROBLEM DEFINITION

Traffic requirements between nodes arise at random times and the size of the requirement is also a random variable. Consequently, queues of packets build up at the channels and the system behaves as a stochastic network of queues. For routing purposes, packets are distinguished only on the basis of their destination, thus messages having a common destination can be considered as forming a class of customers. The packet switch network therefore can be modeled as a network of queues with ‘n’ classes of customers where ‘n’ is the number of different destination.

Average (busy-hour) traffic requirement between nodes can be represented by a requirement matrix R={**r**jk}, where **r**jk is the average transmission rate from Source j to destination k. In some cases we define the requirement matrix as R= ρ k, Where k is a known basic traffic pattern and ρ is a variable scaling factor usually referred to as the traffic level. In general, R (or k) cannot be estimated accurately a priori, because of its dependence upon network parameters (e.g. allocation of resources to computers, demand for resources, etc.), which are difficult to forecast and are subject to changes with time and with network growth. The routing policy and the traffic requirements uniquely determine the vector f (f1,f2 f3….fb) where fi is the average data flow on link i.

Because of the continuous dynamic condition of requirement matrix, even for adaptive routing protocol, it’s very difficult to determine such a flow vector, which could quickly minimize the average delay of packet in the network with present variation.

IV. AVERAGE DELAY MODEL IN NETWORK

4.1 Delay expression

The average packet delay (T) in a network can be defined as mean time taken by a packet to travel from a source node to a destination node. With the following assumptions (i) external Poisson arrivals (ii) exponential packet length distribution (iii) infinite nodal storage (iv) error free channels (v) no node delay (vi) independence between inter-arrival time and transmission time on each channel, expression for T can be defined as

$$T = (1/\gamma) \sum_{i=1}^{N} f_i / (c_i - f_i) \text{ ----------(1)}$$

$$\text{Where } \gamma = \sum_{i=1}^{N} f_i$$

fi denotes the flow in the link i, Ci is the maximum capacity of link i, γ is the total traffic, N is the number of links in the network. More accurate expression for delay can be derived by extending the equation (1), but for most design purpose above equation is accurate.

4.2 Optimization model of delay

Optimization model has formulated as Minimization of delay.

To achieve the optimal minimal value of delay, formulation can be defined as

Given: Topology
Channel capacities {Ci}
Requirement matrix R

Minimize: T

Over the design variable f =(f1, f2, f3…fn)

Subjected to

a) f is a multicommodity flow satisfying the requirement matrix R

b) $f \leq C$

V. OPTIMIZATION USING EC & PSO

Evolutionary computation has experienced a tremendous growth in the last decade in both theoretical analysis and industrial applications. Its scope has evolved beyond its original meaning of biological evolution. Towards a wide variety of nature inspired computational algorithms and techniques, including evolutionary, natural, ecological, social and economical computation etc. in a unified framework, EC is the study of computational system which use ideas and get inspirations from nature evolution and adaption. It is a fast growing interdisciplinary research field in which a variety of techniques and methods are studied for dealing with large complex and dynami problems. The primary aims of EC are to understand the mechanism of such computational systems and to design highly robust, flexible and efficient algorithm for solving real world problems that are generally very difficult for conventional computing methods. EC was originally divided into four groups: evolutionar strategy (ES), evolutionary programming (EP),genetic algorithm (GA) and genetic programming (GP) Nowadays all the approaches used in EC employ population based search engine with perturbation (e.g crossover and mutation) and acceptation (selection an reproduction) to the better solutions compared t conventional optimization methods. The majo advantages of EC approaches include: conceptual an computational simplicity, broad applicability, excellence real world problem solvers, potential to use domain knowledge and hybridize with other methods parallelism, robust to dynamic environments capability for self –optimization, able to solve problems with known solutions etc. there are also some other advantages with EC approaches e.g. no need for analytic expression of the problem, no need for derivatives etc.

The Particle Swarm Optimization (PSO) method is a member of the wide category of Swarm Intelligence methods, for solving optimization problems. PSO can be easily implemented and it I computationally inexpensive, since its memory an CPU speed requirements are low. Moreover, it does no require gradient information of the objective function under consideration, but only its values, and it use only primitive mathematical operators PSO has been proved to be an efficient method for many problem and in some cases it does not suffer the difficulties encountered by other EC techniques.

5.1 Evolutionary programming (EP)

Evolutionary algorithms, such as evolutionary programming (EP), evolution strategies (ES), and genetic algorithms (GA's), operate on a population of candidate solutions and rely on a set of variation operators to generate new offspring. Selection is used to probabilistically promote better solutions to the next generation and eliminate less-fit solutions. Conventional implementations of EP and ES for continuous parameter optimization use Gaussian mutations to generate offspring.

EP has been applied with success to many function and combinational optimization problems.

Optimization by EP can be summarized into two major steps:

(1) Mutate the solutions in the current population,

(2) Select the individuals for the next generation from the mutated and current solutions. These two steps are a population-based version of generate-and-test method, where mutation generates new solutions (offspring) and a selection test that newly generates new solutions should survive to the next generation. Generate –and-test framework can be defined as shown in fig .1. Various models of mutation have been given, the most successful form are (a) Gaussian mutation (b) Cauchy mutation (more generalize form is Levy distribution) (c) mixed mutation including Gaussian and Cauchy mutation. In the Gaussian mutation the search step is sometimes not large enough for the individual to jump out the local optimum hence Cauchy mutation can be taken as solution to solve this problem.

Nevertheless a large search step size may not be beneficial at all if the current search point is already very close to the global optimum. A remedy of above defined problem associated with gaussian and Cauchy mutation, a hybrid approach having facility to generatean offspring from a parent by gaussian and Cauchy mutation separately and among the two offspring, one which will have high value of fitness will accepted as survived offspring for that parent

1.generate the initial solution at random and denote it as the current solution.
2.generate the next solution from the current one by perturbation.
3.test whether the newly generated solution is acceptable
<a> accepted it as the current solution if yes.
<b>keep the current solution unchanged otherwise.
4.Goto steps 2 if the current solution is not satisfactory stop otherwise.

Fig.1.Generate and Test framework

VI. PARTICLE SWARM OPTIMIZATION

6.1 The Particle Swarm Optimization algorithm

A generalized model of PSO is proposed which will be utilized for adaptive resource allocation. In PSO, individual members of swarm are called particles. Each particle keeps track of its coordinates in the problem space which are associated with the best solution (fitness) it has achieved so far.

PSO's precursor was a simulator of social behaviour that was used to visualize the movement of a birds' flock. Several versions of the simulation model were developed, incorporating concepts such as nearest-neighbor velocity matching and acceleration by distance . When it was realized that the simulation could be used as an optimizer, several parameters were omitted, through a trial and error process, resulting in the first simple version of PSO. PSO is similar to EC techniques in that, a population of potential solutions to the problem under consideration is used to probe the search space. However, in PSO, each individual of the population has an *adaptable velocity* (position change), according to which it moves in the search space. Moreover, each individual has a *memory*, remembering the best position of the search space it has ever visited. Thus, its movement is an aggregated acceleration towards its best previously visited position and towards the best individual of a topological neighborhood. Two variants of the PSO algorithm were developed. One with a global neighborhood, and one with a local neighborhood. According to the global variant, each particle moves towards its best previous position and towards the best particle in the whole swarm. On the other hand, according to the local variant, each particle moves towards its best previous position and towards the best particle in its restricted neighborhood. In the following paragraphs, the global variant is exposed (the local variant can be easily derived through minor changes). Suppose that the search space is *D*dimensional, then the *i*-th particle of the swarm can be represented by a *D*-dimensional vector, $Xi = [xi1, xi2, \ldots\ldots xiD]$. The *velocity* (position change) of this particle can be represented by another *D*-dimensional vector $Vi = [vi1, vi2 \ldots viD]$. The best previously visited position of the *i*-th particle is denoted as $Pi = [pi1, pi2, \ldots piD]$. Defining '*g*' as the index of the best particle in the swarm (i.e., the *g*-th particle is the best),'n' is the best seen by that particular particle and let the superscripts denote the iteration number, then the swarm is manipulated according to the following two equations

$$V(n+1)\,id = \chi\,[w\,Vnid + C1\,r1\,(Pnid - Xnid) + C2\,r2\,(Pngd - Xnid)] \ldots\ldots\ldots (2)$$

$$X(n+1)\,id = X\,nid + V(n+1)\,id \ldots\ldots\ldots (3)$$

Where *w* is called *inertia weight*; *c*1, *c*2 are two positive constants, called *cognitive* and *social* parameter respectively; and χ is a *constriction factor*. The role of these parameters is discussed in the next section. In the local variant of PSO, each particle moves towards the best particle of its neighborhood.

Indeed, the swarm in PSO performs space calculations for several time steps. It responds to the quality factors implied by each particle's best position and the best

particle in the swarm, allocating the responses in a way that ensures diversity. Moreover, the swarm alters its behavior (state) only when the best particle in the swarm (or in the neighborhood, in the local variant of PSO) changes, thus, it is both adaptive and stable.

6.2 The parameters of PSO

The role of the *inertia weight w*, in Equation (2), is considered critical for the PSO's convergence behavior. The inertia weight is employed to control the impact of the previous history of velocities on the current one. Accordingly, the parameter *w* regulates the trade-off between the global (wide-ranging) and local (nearby) exploration abilities of the swarm. A large inertia weight facilitates global exploration (searching new areas), while a small one tends to facilitate local exploration, i.e., fine-tuning the current search area. A suitable value for the inertia weight *w* usually provides balance between global and local exploration abilities and consequently results in a reduction of the number of iterations required to locate the optimum solution. the gaussian mutation the search step is sometimes not large enough for the individual to jump out the local optimum hence cauchy mutation can be taken as solution to solve this problem. Initially, the inertia weight was constant. However, experimental results indicated that it is better to initially set the inertia to a large value, in order to promote global exploration of the search space, and gradually decrease it to get more refined solutions. Thus, an initial value around 1.2 and a gradual decline towards 0 can be considered as a good choice for *w*. The parameters $c1$ and $c2$, in Equation (2), are not critical for PSO's convergence. However, proper finetuning may result in faster convergence and alleviation of local minima. An extended study of the acceleration parameter in the first version of PSO is given in (Kennedy, 1998). As default values, $c1 = c2 = 2$ were proposed, but experimental results indicate that $c1 = c2 = 0.5$ might provide even better results. Recent work reports that it might be even better to choose a larger cognitive parameter, $c1$, than a social parameter, $c2$, but with $c1 + c2 \geq 4$ (Carlisle and Dozier, 2001). The parameters $r1$ and $r2$ are used to maintain the diversity of the population, and they are uniformly distributed in the range [0, 1]. The constriction factor χ controls on the magnitude of the velocities, in a way similar to the *Vmax* parameter, result in a variant of PSO, different from the one with the inertia weight.

6.4 Differences between PSO and EC techniques

In EC techniques, three main operators are involved. The *recombination*, the *mutation* and the *selection* operator. PSO does not have a direct recombination operator. However, the stochastic acceleration of a particle towards its previous best position, as well as towards the best particle of the swarm (or towards the best in its neighborhood in the local version), resembles the recombination procedure in EC .In PSO the information exchange takes place only among the particle's own experience and the experience of the best particle in the swarm, instead of being carried from fitness dependent selected "parents" to descendants as in GA's. Moreover, PSO's directional position updating operation resembles mutation of GA, with a kind of memory built in. This mutation-like procedure is multidirectional both in PSO and GA, and it includes control of the mutation's severity, utilizing factors such as the *Vmax* and χ.PSO is actually the only evolutionary algorithm that does not use the "survival of the fittest" concept. It does not utilize a direct selection function. Thus, particles with lower fitness can survive during the optimization and potentially visit any point of the search space.

VII. EXPERIMENTAL SETUP FOR COMPARATIVE ANALYSIS BETWEEN EP AND PSO.

For network shown in fig.7, assuming the current total load in the network is 60%of total capacity. With different variations of EP and PSO as shown in table (2), task has defined for each case as: for what distribution of flow the average delay will be minimum.

7.1 Parameter initialization for experiment

In all cases, initial flow distributions defined randomly with uniform distribution in range [1 50]; Population size 150 for Gaussian and Cauchy mutation methods and 100 for Hybrid method (because each parent generate two offspring) and 300 for all variations of PSO, so that next generation is created by a population of 300.For all variation of EP: $\sigma i = 0.01$, for all i; In PSO, $\chi = 0.75$, w gets changing from 1.2 to 0.1 with iteration wise, C1 and C2 both taken as 0.5.Terminating criteria taken as: when for twenty continuous iteration, if the difference in objective function values having change lese than 0.00000001; For each setup total number of generations taken before termination of execution, total time taken to execute the program and best average delay given at the time of termination by program are consider as final outcomes. The process of execution repeated for ten independent trails and results are shown in table (2). From the results it's very clear that in different variations of EP, gaussian mutation and Cauchy mutation based approach nearly perform equally, while hybrid approach, combination of both gaussian and cauchy, perform better comparatively. This is because longer jump of cauchy mutation helps the algorithm at the early stage and smaller step of gaussian, when near to optimal value. But PSO with constraint factor χ clearly outperforms all other approaches. Performances of this method are shown in

fig.2 and in fig.3. Hence for training and test data generation PSO with χ is selected with same parameters initialization as taken above.

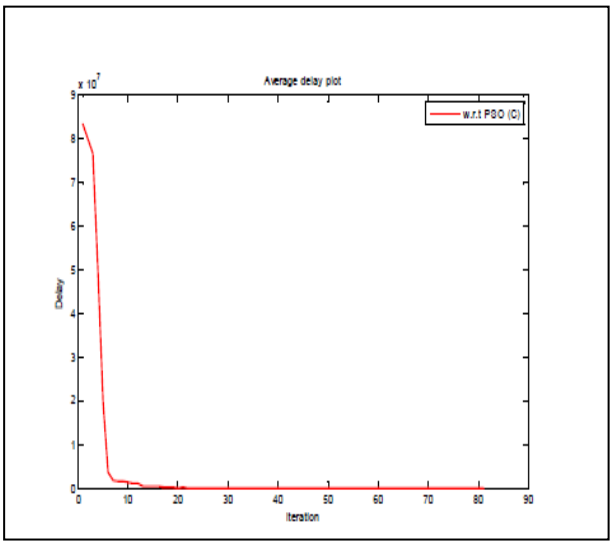


Fig.2.performance on delay minimization

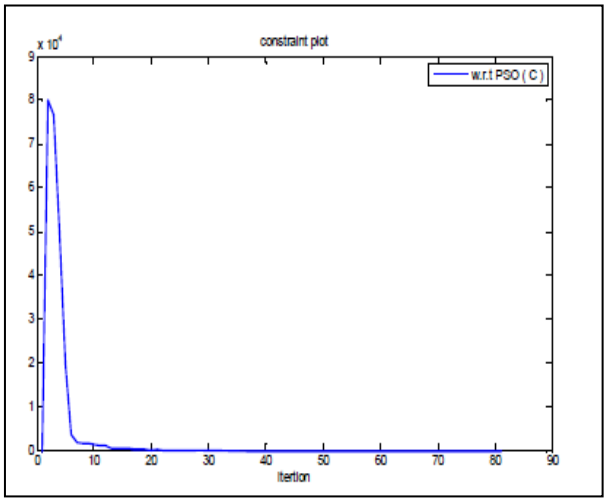


Fig.3.Constrint value performance

VIII.ANN PREDICTIVE MODELFOR FLOW DISTRIBUTION

Steps taken to develop the model that provide the assistance to routing protocol to define the optimal flow on links have given below and its application with routing protocol shown in fig.4.

(1) Generate the various different possible total load (Li, i=1,2…m) for given network in the range of 30%-95% of the maximum capacity of the network.
(2) For each value of Li find the optimal value of flow vector f, using an optimization method.
(3) Create a data set containing number of possible load and its corresponding optimal flow distribution, this is training data set.
(4) Create a data set as in step 3 with remaining information in step 2, this is test data set.
(5) Give training to neural network with training data set, by taking input as the total load and its corresponding optimal flow distribution as target.
(6) Verify the result with test data set.

Fig.4. Steps of predictive model for flow distribution

The role of ANN is to provide the optimal distribution of flow for any present load in the network. This distribution is a very useful information for routing protocol for assigning the flow on each link so that minimum average delay with given load can achieve. Any variation in total load of traffic matrix will sense by neural network and in result immediate optimal distribution. Hence neural network can be use to provide the information of flow distribution for any variation of load that may happen with network, very quickly and precisely. Training data and test data set for various total loads, the optimum distribution, which could generate minimum delay. Along with that, Mean link utilization (M.L.U) and number of generation taken has also given. Training has given over training dataset with the feed forward architecture and a variation of back propagation learning algorithm. Specification of architecture and learning algorithm has given below: Size of architecture: 1 input node, 7 hidden nodes, 13 output nodes; Learning rate =0.9, momentum constant=0.2; Weights are initializing with uniform random distribution in range [-0.5 0.5]; Bias node has applied to all hidden nodes. Total number of allowed iteration =5000; The curve of learning shown in figure (5).

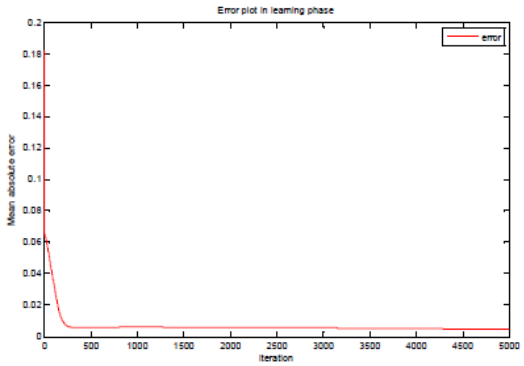


Fig.5.Learning curve of ANN

IX. CONCLUSION

In this paper the challenge to find the optimal flow assignment with dynamic traffic matrix has solved by the application of neural network and particle swarm optimization together. The solution generated by proposed method is very close as it was expected and it's applicable to wide variations of load. To achieve the best performance of system, various variation of evolutionary programming compared with PSO variations. For taken problem, PSO with constriction factor has shown dominancy over other methods. Proposed method is easy to implement and very efficient. It can be integrated with the existing solution with simple engineering to increase the quality of service in terms of minimizing the average delay.

REFERENCES

[1] W.Chang and R.S.Ramakrishna,"A genetic algorithm for shortest path routing problem and the sizing of populations",IEEE Transaction on Evolutionary computation,Vol.6,No.6,December(2002).

[2] X.Lin,Y.Kwok and V.Lau,"A genetic algorithm based approach to route selection and capacity flow assignment", computer communication 26,pp 961-974,(2003).

[3] A.Dutta ans S.Mitra,"Integrating heuristicc knowledge and optimization models for communication-network-design" ,IEEE Trans. knowl. Data Eng., vol5,no.6,pp.999- 1017,1993.

[4] R.H.Jan, F.J.Hwang and S.T.Cheng,"Topological optimization of a communication network subject to a reabilityconstraint."IEEETrans.Rel., vol.42,no.1,pp.63-70,1993.

[5] K.Kamimura and H.Nishino,"An efficient method for determining economical configration of elementary packet–switchednetworks.", IEEE rans.Commun.vol.39,no.2,pp.278- 288,1991.

[6] A.Kershenbaum,P.Kermani,and .A.Grover,"MENTOR:An algorithm for mesh network topological optimization and routing,"IEEE Trans.Commun,vol.39,no.4,pp.503-513,1991.

[7] S.Pierre,M.A.Hyppolite,J.M.Bourjolly and O.Dioume," Topological design of computer communications networks using simulated anneling,"Eng.Applicat Aritf.Intell. vol.8,no1, pp.61-69,1995.

[8] S.Pierre and H.H.Hoang,"An artificial intelligence approach for improving computer communications network topologies." J.Oper.Res.Soc., vol41,no., pp.405 418,1990.

[9] A.Konak and A.E.Smith,"Designing resilient networks using a hybrid genetic algorithm approach,"in GECCO'05: proceeding of 2005 conference on genetic and evolutionary computation,(New York, USA),pp.1279-1285,ACM Press,2005.

[10] H.Kobayashi, M.Munetomo,K.Akama and Y.Ato,"Designing a distributed algorithm for bandwidth allocation with a genetic algotithm".Syst.Comput.Japan,vol.35,no.3,pp.37-45,2004.

[11] Ka-Cheong Leung and Victor O.k.Li,"Flow assignment and packet scheduling for multipath routing", Journal of communications and Networks,vol.5,no.3.September 2003.

[12] Tarek M.Mahmoud," A genetic and simulated annealing based algorithms for solving the flow assifnment problem in computer networks",World academy of Science, Engineeringand Technology 27,2007.

❑❑❑

Modified LSB Watermarking for Image Authentication

R.Aarthi, V. Jaganya, & S.Poonkuntran

Department of Information Technology, Velammal College of Engineering and Technology, Madurai, India
E-Mail - aarthiramasami@gmail.com, jaganyavijayan@gmail.com, s.poonkuntran@gmail.com

Abstract - This paper mainly aims at developing an authentication scheme for digital images. The LSB scheme is chosen as base for o proposed work. Through literature survey it is found that conventional LSB scheme provides low embedding rate, low distortion and irreversible. Because of its irreversibility, the conventional LSB scheme cannot be used for critical applications where reversibility mandatory. Through this literature survey, we learnt that this conventional LSB scheme uses only one bit in every pixel for embeddin Our proposed scheme presents a modified LSB embedding strategy that satisfies the reversibility and improves the embedding rate b using two bits in every pixel for embedding.

Key words*: LSB, reversibility, watermarking, authentication, selection strategy, secret data, PSNR*

I. INTRODUCTION

Digital watermarking [1] is a method of embedding useful information into a digital work (especially, thus, audio,image, or video) for the purpose of copy control, content authentication, broadcast monitoring, etc. The distortion introduced by embedding the watermark is often constrained so that the host and the watermarked work are perceptually equivalent. However, in some applications, especially in the medical, military, and legal domains, even the imperceptible distortion introduced in the watermarking process is unacceptable. This has led to an interest in *reversible* watermarking [2]-[6], where the embedding is done in such a way that the information content of the host is preserved.

This enables the decoder to not only extract the watermark, but also perfectly reconstruct the original host signal from the watermarked work.

II. TRADITIONAL LEAST SIGNIFICANT BIT

The least significant bit (LSB) technique is used to embed information in a cover image. The LSB technique is that inside of a cover image, pixels are changed by bits of the secret message. These changes cannot be perceived by the human visibility system. However, a passive attacker can easily extract the changed bits, since it has performed very simple operation.

For example, Figure 1 shows the 1-bit LSB. In Figure 1, LSB can store 1-bit in each pixel. If the cover image size is 256 x 256 pixel image, it can thus store a total amount of 65,536 bits or 8,192 bytes of embedded data.

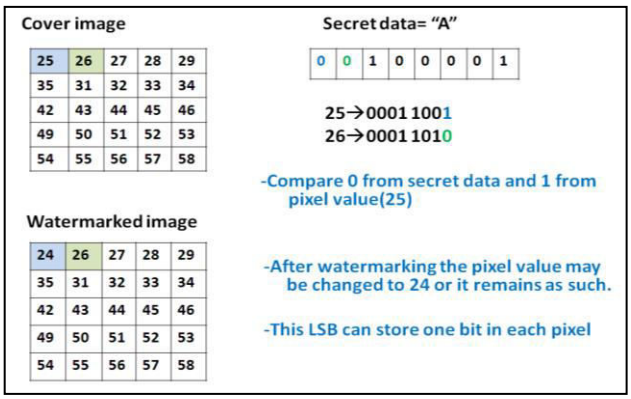


Figure 1 An example of 1 bit LSB.

III. MODIFIED LEAST SIGNIFICANT BIT

A. Reversibility

After the secret data gets embedded or hidden in the cover image, the original cover image will get modification to some extent with respect to the length of the secret data. At the receiving end we are not able to get back the original cover image since our traditional LSB is not providing reversibility. Reversible feature is a process of getting back the cover image from the watermarked or embedded image at the extraction phase. After getting the watermarked image, we need to create a matrix initialized with zeros, whose dimension is equal to the watermarked image. By XOR-ing each and every pixel of both the original and watermarked image, the result will be stored in the corresponding positions in the newly created matrix. This matrix will also be sent to the extraction phase along with

the watermarked image. During extraction the value of the newly created matrix will be checked. If it is 1, then watermarked image's s LSB of each pixel must be changed, else vice versa. Finally we could get back the original cover image.

B. Boosting the capacity of the scheme

Most of researchers have proposed the first LSB scheme but our proposed watermarking algorithm is using the third and fourth LSB for hiding the data. Our algorithm can store 2-bits in each pixel. If the cover image size is 256 x 256 pixels image, it can thus store a total amount of 1, 31,072 bits secret data which is double the number of bits stored by traditional LSB. First, we select the image as shown in figure 2 and then we will convert the data to binary value as shown in the figure 3. Then, we hide the data in the image using the proposed algorithm. Then, we will get the watermarked image as shown in the figure 4. Then, the receiver will retrieve the data back from watermarked image by extraction.

B=

25	26	27	28	29
35	31	32	33	34
42	43	44	45	46
49	50	51	52	53
54	55	56	57	58

Figure 2 An example for cover image matrix.

w=

0	1	0	1	0	0	1	1	(S)
0	1	1	1	0	1	0	0	(t)
0	1	1	0	0	0	0	1	(a)
0	1	1	1	0	0	1	0	(r)
0	1	1	1	0	1	0	0	(t)

Figure 3 An example for secret data matrix

17	18	19	20	21
39	23	32	45	38
46	38	32	37	42
49	54	55	60	49
58	55	60	53	50

Figure 4 An example for watermarked image.

To implement reversibility in our proposed algorithm, we can simply create two matrices, to record the modifications made in the 3rd and 4th LSBs of the cover image. As previously said we need to send these matrices to the extraction phase to get back the original cover image.

C. *Selection Strategy*

After the modification done on the traditional LSB, we could realize the changes in the pixel values in the cover image and the watermarked image by comparing the figure 5 and figure 6 and that may reduce imperceptibility. If all the altered pixels are clustered in a location, it may lead to robustness but in our paper we are providing fragility. To solve the above two problems we are implementing selection strategy. For that we are randomly selecting the pixels and after that we are embedding the secret data in the cover image. Our modified algorithm failed in providing imperceptibility, it is shown in the figure 5. Since reversibility is implemented we could get the extracted image which same as that of cover image as shown in the figure 6.

After applying selection strategy in our modified algorithm imperceptibility is also achieved as shown in the figure 7.

Figure 5 Watermarked image after applying LSB34_rev.

Figure 6 Extracted image after applying LSB34_rev.

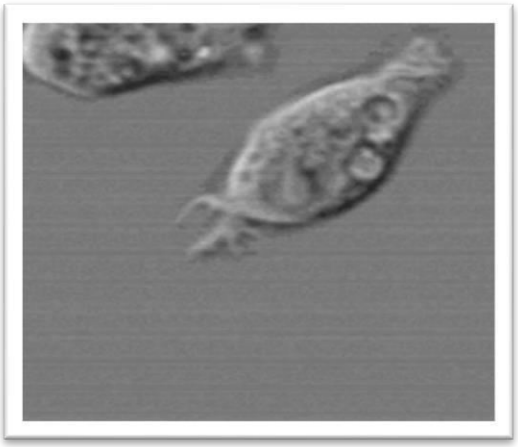


Figure 7 Watermarked image after LSB34_REV_SEL.

IV. QUANTITATIVE ANALYSIS

A. Imperceptibility and Reversibility

The PSNR value was used to evaluate the quality of the watermarked images. It is most easily defined via the Mean Squared Error (MSE) which is for two M x N images I and K where one of the images is considered as a noisy approximation of the other. MSE is defined as the following equation (2) and the PSNR is defined in equation (1).

$$PSNR = 10 \cdot log_{10}\left(\frac{MAX_I^2}{MSE}\right) = 20 \cdot log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right) \quad (1)$$

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j]^2 \quad (2)$$

where I is the original image and K is the watermarked image. Based on equations (1) and (2), we calculate the PSNR for our proposed algorithm to see the quality of the watermarked images.

SCHEME NAME: LEAST SIGNIFICANT BIT

TYPE: PNG File

Table 1 A sample table for LSB algorithm analysis.

SIZE OF WATERMARI	IMPERCEPTIBILIT (PSNR values)	REVERSIBILITY (PSNR values)
50	78.2565	78.2565
100	74.8137	74.8137
500	68.0870	68.0870
1000	64.9475	64.9475
2000	62.0506	62.0506
10000	55.0951	55.0951
100000	Not Applicable	Not Applicable

The above Table 1 is to show the result of the PSNR for two combinations,

1) Original image and embedded image (imperceptibility)
2) Original image and extracted image (reversibility)

Since the PSNR value for both above mentioned combination of input are same, it is understood that embedded and extracted images are also same and the reversibility is not achieved. After applying reversibility we could get the Table 2 as follows,

SCHEME NAME: LEAST SIGNIFICANT BIT WITH REVERSIBILITY

TYPE: TIF File

Table 2 A sample table for LSB with reversibility.

SIZE OF WATERMARI	IMPERCEPTIBILIT (PSNR values)	REVERSIBILITY (PSNR values)
50	73.1359	100
100	70.2103	100
500	63.2421	100
1000	60.2253	100
2000	57.2827	100
10000	Not Applicable	Not Applicable
100000	Not Applicable	Not Applicable

Since the original image and the extracted image are same the PSNR value is 100. Hence the reversibility is now achieved. After boosting up the capacity of the scheme, we got the Table 3 and Table 4 as follows.

By comparing Table 2 and Table 4, we could say that our scheme has boosted the capacity of traditional LSB.

SCHEME NAME: LEAST SIGNIFICANT BIT34

TYPE: PNG File, Table 3 A sample table for LSB34.

SIZE OF WATERMARI	IMPERCEPTIBILIT (PSNR values)	REVERSIBILITY (PSNR values)
50	61.6457	61.6457
100	57.9029	57.9029
500	50.7422	50.7422
1000	47.7507	47.7507
2000	45.1578	45.1578
10000	38.0822	38.0822
100000	Not Applicable	Not Applicable

SCHEME NAME: LEAST SIGNIFICANT BIT34 WITH REVERSIBILITY
TYPE: TIF File

Table 4 A sample table for LSB34 with reversibility.

SIZE OF WATERMARK	IMPERCEPTIBILITY (PSNR values)	REVERSIBILITY (PSNR values)
50	56.6351	100
100	53.5651	100
500	46.6396	100
1000	43.8361	100
2000	40.7374	100
10000	33.9417	100
100000	Not Applicable	Not Applicable

Higher the PSNR values better the quality of the image. Since we embedded the secret data in 3rd and 4th LSB bits of each pixel, we got some changes with the value of the pixels. Because of this, our algorithm's imperceptibility went down as shown in the Figure 8.

By consolidating all the values from 20 tables (i.e. 10 images*2 shemes) we got the following graph for representing imperceptibility.

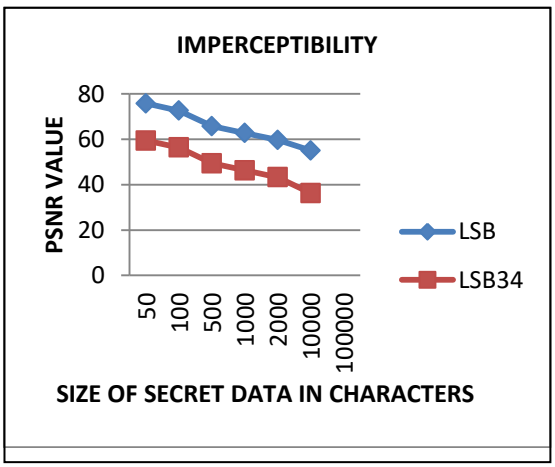


Figure 8 Imperceptibility Analysis.

Since imperceptibility is very important feature in information hiding, we overcame this problem by implementing the pixel selection strategy.

B. Fragility

To check the fragility in our modified LSB algorithm, we are attacking [7] the watermarked image and that must modify our hidden data in it.

SCHEME NAME: LEAST SIGNIFICANT BIT34 (LSB_34)
NAME OF THE ATTACK: JITTER
TYPE: TIF File
Percentage of attack: 70

Table 5 An example to show the attacked percentage.

SIZE OF WATERMARK(bits)	**ATTACKED SECRET DATA (%)**
400	13.25
800	8.12
4000	6.80
8000	11.45
16000	10.31
80000	8.40
800000	Not Applicable

Table 5 is an example to prove that our algorithm is fragile [5] because it shows how much percentage of secret data got attacked. Figure 9 is to represent all the tables in the form of graph.

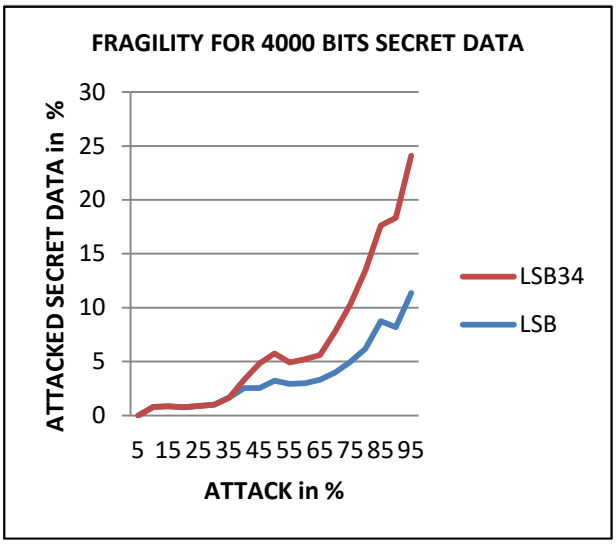


Figure 9 Fragility Analysis.

V. CONCLUSIONS

Thus the result of our quantitative analysis helps us to prove that our proposed algorithm will boost the capacity of the scheme and provide reversibility, fragility for the transmitting secret data.

REFERENCES

[1] Techniques and applications of digital watermarking and content protection by Michael Konrad Arnold, Martin Schmucker, Stephen D. Wolthusen

[2] "Reversible Zero-Bit Watermark Based on Chaotic Encryption "in Wireless Communications Networking and Mobile Computing (WiCOM), 2010 6th International Conference, Sept. 2010.

[3 "Digital watermarking algorithm using LSB" in Computer Applications and Industrial Electronics (ICCAIE), 2010 International Conference, Dec. 2010.

[4] "Block-based digital image watermarking using Genetic Algorithm" in Emerging Technologies (ICET), 2010 6th International Conference, Oct. 2010

[5] "Cheating resistance and reversibility-oriented secret sharing mechanism " in Information Security, IET, June 2011.

[6] "Robust LSB watermarking optimized for local structural similarity" in Electrical Engineering (ICEE), 2011 19th Iranian Conference, May 2011.

[7] "A steganographic scheme for colour image authentication (SSCIA) " in Recent Trends in Information Technology (ICRTIT), 2011 International Conference, June 2011.

[8] "A watermarking e-note technique against geometric attacks" in Mechanical and Electronics Engineering (ICMEE), 2010 2nd International Conference, Aug. 2010.

❑❑❑

Empirical Study on different Multi-scale Transforms with Set Partitioning Embedded Block

S.P. Princess & P. Sundareswaran

Manonmaniam Sundaranar University, Tirunelveli, Tamilnadu, India
E-mail : avemariaprincymary@gmail.com

Abstract - The objective of this paper is to discuss the different types of multi-scale transforms on gray scale images along with SPECK. The transforms involved in this paper are Curvelet, Contourlet and Ridgelet. In the past, a number of texture features have been proposed in literature, including statistic methods and spectral methods. However, most of them are not able to accurately capture the edge information which is the most important texture feature in an image. Recent researches on multi-scale analysis, especially the curvelet research, provide good opportunity to extract more accurate texture feature for image retrieval. Curvelet was originally proposed for image denoising and has shown promising performance. The ridgelet transform was introduced as a sparse expansion for functions on continuous spaces that are smooth away from discontinuities along lines. The contourlet transform was proposed as a directional multiresolution image representation that can efficiently capture and represent singularities along smooth object boundaries in natural images. Its efficient filter bank construction as well as low redundancy make it an attractive computational framework for various image processing applications. However, a major drawback of the original contourlet construction is that its basis images are not localized in the frequency domain.

Keywords— *Multi-scale Transforms, SPECK.*

I. INTRODUCTION

The last two decades have seen tremendous activity in the development of new mathematical and computational tools based on multiscale ideas. Today, multiscale/ multiresolution ideas permeate many fields of contemporary science and technology. In the information sciences and especially signal processing, the development of wavelets and related ideas led to convenient tools to navigate through large datasets, to transmit compressed data rapidly, to remove noise from signals and images, and to identify crucial transient features in such datasets. In the field of scientific computing, wavelets and related multiscale methods sometimes allow for the speeding up of fundamental scientific computations such as in the numerical evaluation of the solution of partial differential equations. By now, multiscale thinking is associated with an impressive and ever increasing list of success stories.

Despite considerable success, intense research in the last few years has shown that classical multiresolution ideas are far from being universally effective. Indeed, just as people recognized that Fourier methods were not good for all purposes—and consequently introduced new systems such as wavelets—researchers have sought alternatives to wavelet analysis. In signal processing for example, one has to deal with the fact that interesting phenomena occur along curves or sheets, e.g., edges in a two-dimensional image. While wavelets are certainly suitable for dealing with objects where the interesting phenomena, e.g., singularities, are associated with exceptional points, they are ill-suited for detecting, organizing, or providing a compact representation of intermediate dimensional structures. Given the significance of such intermediate dimensional phenomena, there has been a vigorous research effort to provide better adapted alternatives by combining ideas from geometry with ideas from traditional multiscale analysis.

Multiscale methods are also deeply related with biological and computer vision. Since, Olshausen and Field's work in Nature, researchers in biological vision have re-iterated the similarity between vision and multiscale image processing. It has been recognized that the receptive fields of simple cells in a mammalian primary visual cortex can be characterized as being spatially localized, oriented and bandpass (selective to structure at different spatial scales). Therefore, they can be well represented by wavelet transforms. One approach to understand the response properties of visual neurons has been to consider their relationship to the statistical structure of natural images in terms of

efficient coding. A directional multi scale sparse coding is desirable in this field. A multi resolution geometric analysis (MGA), named curve let transform, was proposed in order to overcome the drawbacks of conventional two-dimensional discrete wavelet transforms.

Contourlets, as proposed by Do and Vetterli, form a discrete filter bank structure that can deal effectively with piecewise smooth images with smooth contours. This discrete transform can be connected to curvelet-like structures in the continuous domain. Hence, the contourlet transform can be seen as a discrete form of a particular curvelet transform. Curvelet constructions require a rotation operation and correspond to a partition of the 2D frequency plane based on polar coordinates. For contourlets, it is easy to implement the critically sampling. There exists an orthogonal version of contourlet transform that is faster than current discrete curvelet algorithms. The directional Filter bank, as a key component of contourlets, has a convenient tree-structure, where aliasing is allowed to exist and will be canceled by carefully designed filters. Thus, the key difference between contourlets and curvelets is that the contourlet transform is directly defined on digital-friendly discrete rectangular grids. Unfortunately, contourlet functions have less clear directional geometry/features than curvelets (i.e., more oscillations along the needle-like elements) leading to artifacts in denoising and compression.

The rest of the paper is organized as follows. The Curvelet Transform is discussed in Chapter II. The Contourlet transform is presented in Chapter III. The Ridgelet Transform is given in Chapter IV. The SPECK technique is presented in Chapter V. The experimental results are given in Chapter VI. The conclusion is discussed in Chapter VII.

II. CURVELET TRANSFORM

Basically, curvelet transform extends the ridgelet transform to multiple scale analysis. Therefore, let's start from the definition of ridgelet transform. Given an image function $f(x, y)$, the continuous ridgelet transform is given as:

$$\Re_f(a, b, \theta) = \iint \psi_{a,b,\theta}(x,y) f(x,y) dxdy$$

Where $a>0$ is the scale, The ridgelet is defined as:

$$\psi_{a,b,\theta}(x,y) = a^{-\frac{1}{2}} \psi(\frac{x\cos\theta + y\sin\theta - b}{a})$$

Fig. 1 shows a typical ridgelet. It is oriented at an angle θ, and is constant along lines: $x \cdot cos\theta + y \cdot sin\theta = const$. It can be seen that a ridgelet is linear in edge direction and is much sharper than a conventional sinusoid wavelet.

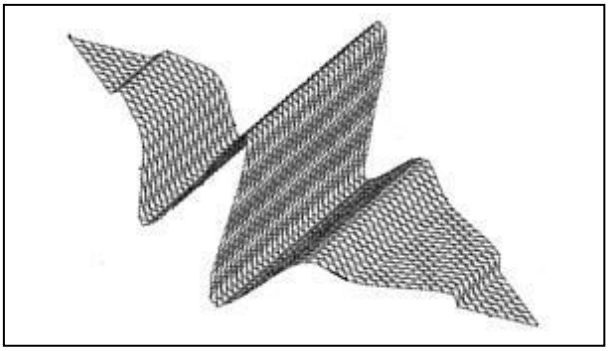


Fig. 1 A Ridgelet Waveform

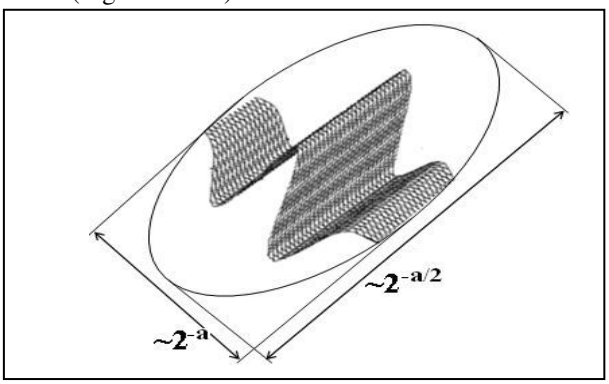
For comparison, the 2-D wavelet is given as:

$$\psi_{a_1,a_2,b_1,b_2}(x,y) = a_1^{-\frac{1}{2}} a_2^{-\frac{1}{2}} \psi(\frac{x-b_1}{a_1}) \psi(\frac{y-b_2}{a_2})$$

As can be seen, the ridgelet is similar to the 2-D wavelet except that the point parameters ($b1$, $b2$) are replaced by the line parameters (b, θ). Fig. 2 shows a single curvelet and the curvelets tuned to two scales and different number of orientations at each scale.

But different from Gabor filters which only cover part of the spectrum in the frequency domain, curvelets have a complete cover of the spectrum in frequency domain. That means, there is no loss of information in curvelet transform in terms of capturing the frequency information from images

Fig. 3 (top image) shows the curvelet tiling and cover of the spectrum of a 512x512 images with 5 scales. The shaded wedge shows the frequency response of a curvelet at orientation 4 and scale 4. It can be seen, the spectrum cover by curvelets is complete. In contrast, there are many holes in the frequency plan of Gabor filters (Fig. 3 bottom).



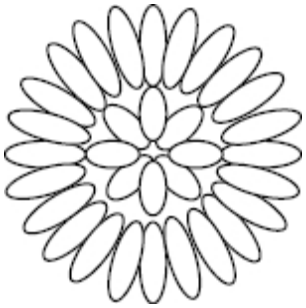


Fig. 2. Left: a single curvelet. Right: curvelets tuned to different scales and orientations

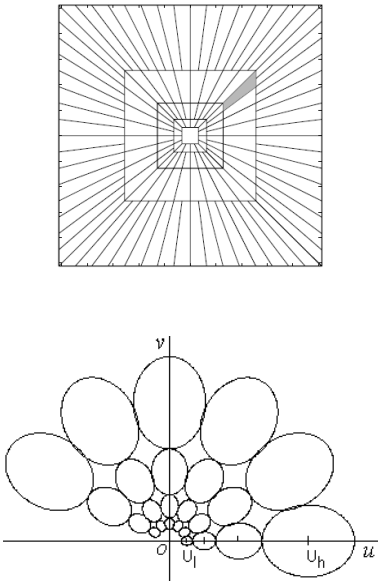


Fig. 3. Top: the tiling of frequency plan by curvelets. Bottom: the tiling of half frequency plan by Gabor filters, the ovals are the covered spectrum.

The digital curvelet transform is implemented using the fast discrete curvelet transform. Basically, it is computed in the spectral domain to employ the advantage of FFT. Given an image, both the image and the curvelet are transformed into Fourier domain, then the convolution of the curvelet with the image in spatial domain becomes the product in Fourier domain. Finally the curvelet coefficients are obtained by applying inverse Fourier transform on the spectral product.

But due to the frequency response of a curvelet is a nonrectangular wedge, the wedge needs to be wrapped into a rectangle to perform the inverse Fourier transform. The wrapping is done by periodic tiling of the spectrum using the wedge, and then collecting the rectangular coefficient area in the centre. Through this periodic tiling, the rectangular region collects the wedge's corresponding portions from the surrounding periodic wedges. The complete feature extraction process using a single curvelet is illustrated in Fig. 4.

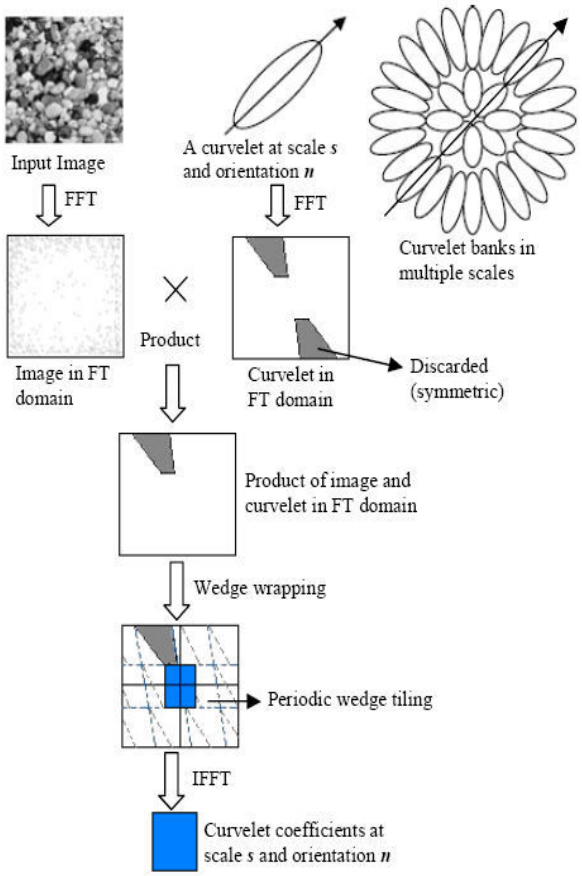


Fig. 4. Fast discrete curvelet transform

III. CONTOURLET TRANSFORM

For image enhancement, one needs to improve the visual quality of an image with minimal image distortion. Wavelet bases present some limitations, because they are not well adapted to the detection of highly anisotropic elements such as alignments in an image. Recently Do and Vetterli proposed an efficient directional multi resolution image representation called the contourlet transform. Contourlet transform has better performance in representing the image salient features such as edges, lines, curves and contours than wavelet transform because of its anisotropy and directionality. It is therefore well-suited for multi- scale edge based color image enhancement. The contourlet transform consists of two steps which is the sub band decomposition and the directional transform. A Laplacian pyramid is first used to capture point discontinuities, then followed by directional filter banks to link point discontinuity into lineal structure. The overall result is an image expansion using basic elements like contour segments, thus the

term contourlet transform being coined. Figure 5 shows a flow diagram of the contourlet transform.

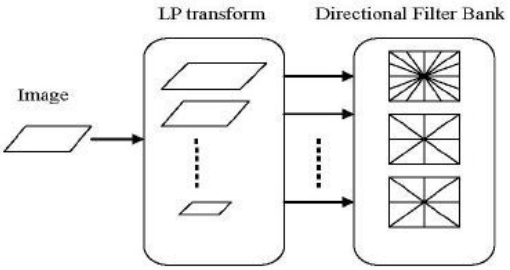


Fig. 5 Contourlet transform framework

Figure 6 below shows the contourlet filter bank. First, multiscale decomposition by the Laplacian pyramid, and then a directional filter bank is applied to each band pass channel.

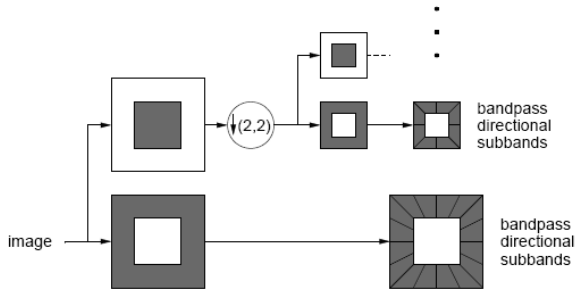


Figure 7 shows a sample contourlet transform coefficients of the test images in case study IV (refer to the results sections). This is level three, with 3, 4, and 8 directions from coarse to fine levels respectively.

Fig. 7 Contourlet transform coefficients of the source images, a) visual imageb) night vision image

IV. RIDGELET TRANSFORM

The ridgelet transform was originally proposed by Candès and Donoho and offers a sparse coding of image with edges. A ridgelet is defined as a wavelet distributed along a ridge of orientation $x\cos\theta + x\sin\theta = b$ within the Cartesian plan (x1,x2):

$$\psi_{a,b,\theta}(x_1,x_2) = a^{-1/2}\psi((x_1\cos\theta + x_2\sin\theta - b)/a), a>0, b\in \mathbf{R}, \theta\in[0,2\pi[$$

The ridgelet coefficients Rid$I$ of an image I are obtained by projection on this base :

$$\mathrm{Rid}_I(a,b,\theta) = \iint \psi_{a,b,\theta}(x_1,x_2) I(x_1,x_2)\,dx_1 dx_2$$

This projection is related to the Radon transform which consists in integrating the image along lines of different Orientations:

$$\mathrm{Rad}_I(\theta,t) = \iint I(x_1,x_2)\delta(x_1\cos\theta + x_2\sin\theta - t)\,dx_1 dx_2$$

Consequently, the ridgelet transform can be seen as 1-D wavelet transform of the Radon transform Rad$I$ along the translation parameter t:

$$\mathrm{Rid}_I(a,b,\theta) = \int \mathrm{Rad}_I(\theta,t)\psi((t-b)/a)\,dt$$

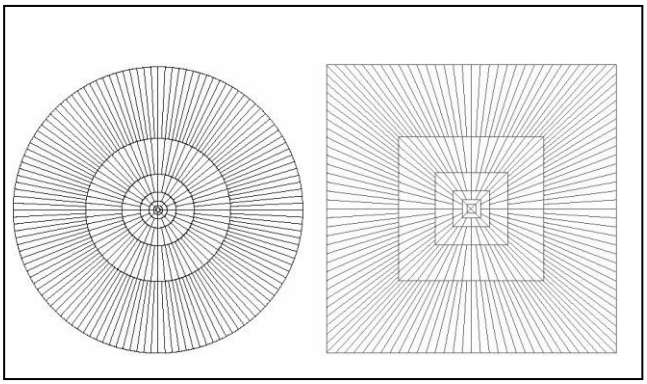
An important property can be exploited, called the projection-slice therorem, which says that the 1-dimensionnal constant-θ slice of the Radon transform and the 1-dimensionnal radial slice of the Fourier transform makes a Fourier transform pair:

$$\hat{I}(\lambda\cos\theta, \lambda\sin\theta) = TF_t\left[\mathrm{Rad}_I(\theta,t)\right] = \int \mathrm{Rad}_I(\theta,t)e^{-\lambda i t}dt$$

Which means that the Radon transform for a given orientation can be derived from the inverse 1-dimensional Fourier transform of the image Fourier transform performed along radial lines. Consequently, Equation can be simply written in the frequency domain:

$$\mathrm{Rid}_I(a,b,\theta) = TF_\lambda^{-1}\left[\hat{I}(\lambda\cos\theta,\lambda\sin\theta)TF_t\left[\psi(t/a)\right]\right]$$

In order to apply equation the frequency domain has to be re-sampled on a polar grid. This task is not easy because radial slices do not always intersect the Cartesian grid. A simple and efficient approximation of the polar grid is the rectopolar grid which consists in concentric square (see Fig. 8). The new frequency samples are distributed along radial lines intersecting the null frequency component of the Fourier spectrum. These new frequency components can be calculated using various interpolation scheme. An example of basically horizontal lines and nearest neighbor interpolation is shown on Fig. 9.



. 8 a) Ridgelet tiling of the frequency domain and b) Digital ridgelet tiling

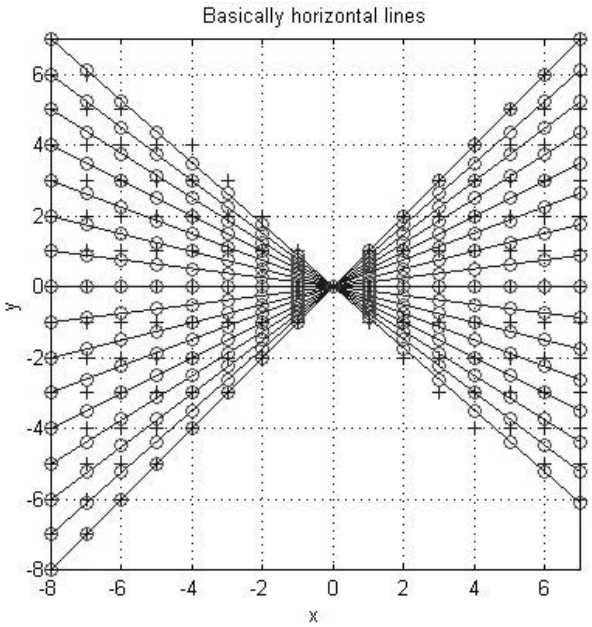


Fig. 9 Cartesian-to-Pseudopolar conversion for the basically horizontal lines for a 16x16 grid, the red circles indicate pseudopolar points and the cross marks indicate nearest neighbor positions on the Cartesian grid

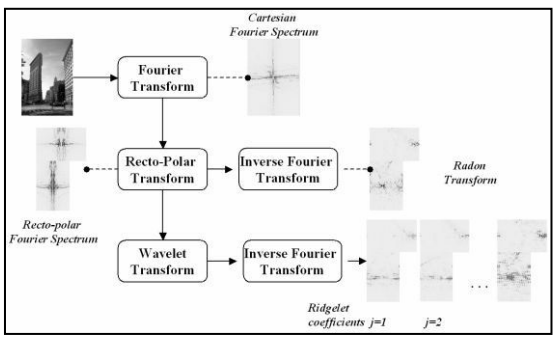


Fig. 10 Block Diagram of Ridgelet Transform

V. SET PARTITIONING EMBEDDED BLOCK (SPECK)

A. *SPECK Process*

SPECK comprises three stages: initialization, sorting, and refinement. In the second stage, information is sorted in two ordered lists: a list of insignificant sets (LIS) and a list of significant pixels (LSP). In the initialization stage, a start threshold which depends on the maximum value in the wavelet coefficients pyramid is defined (chosen as a power of two: $T=2^n$) and the list LSP is initially empty. Then, the image is partitioned into two sections (see Fig. 11): S a set of type which is the root of the pyramid, and Γ a set of type which is the remaining part. From the standpoint of implementation, a block of type S is determined from the coordinates of the pixel in the top-left and the size of this block. First, the set of type S is added to LIS. In the sorting pass, the algorithm sorts each block of type S in LIS by performing a significance test against the current threshold (1 for significant sets or 0 for insignificant sets). A block is said to be significant if it has at least one coefficient whose magnitude is greater than or equal to the threshold value. If a block of S type is significant, it is partitioned into four subsets of the same type (S0, S1, S2 and S3) as shown in Fig. 12.

In LIS, this block is replaced by the subsets S type. In the case where a significant block is of size 1X1 (one pixel), its sign is coded and its coordinate moved to LSP. In the same way, the set of type Γ is examined with respect to the current threshold where its partitioning again produces one subset of type and three subsets of type S S0, S1, S2 and S3) as depicted in Fig. 13. This significance test and partitioning process are carried out for all sets of type S(including the new ones) and the set of type Γ. Depending upon the image content and the target coding bit-rate, a set type Γ might not occur in LIS at some point. In the refinement pass, the nth most significant bit of each entry in LSP, excluding those coefficients which have been added during the last sorting pass, is transmitted. Then, the current threshold is divided by 2 and the sorting and refinement stages are continued until a predefined bit-rate is achieved (lossy case) or all bits of each entry in LSP are transmitted (lossless case).

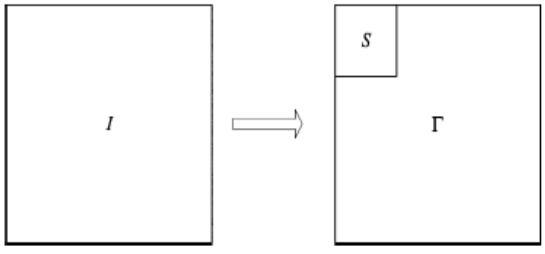


Fig. 11 Partioning of image I into sets S and Γ

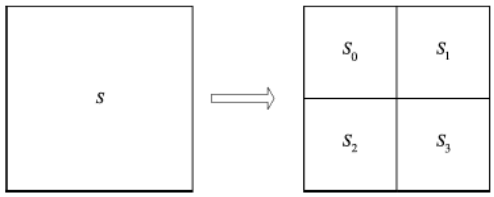


Fig. 12 Partitioning of Set S

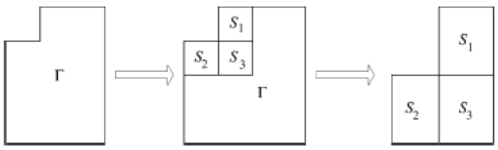


Fig. 13 Partitioning of Set Γ

VI. EXPERIMENTAL RESULTS

The following are the experimental results of the above mentioned multiscale transforms. The results are shown in Fig. 14 – 19.

A. Performance of SPECK with Curvelet Transform

Fig. 14 SPECK Compression with Curvelet

B. *Performance of Multi-scale Transforms*

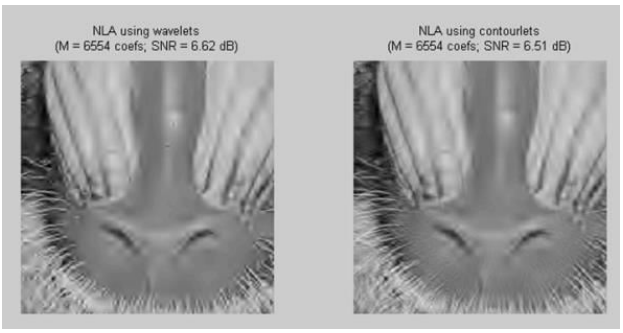


Fig. 15 NLA Using Contourlets and Wavelets

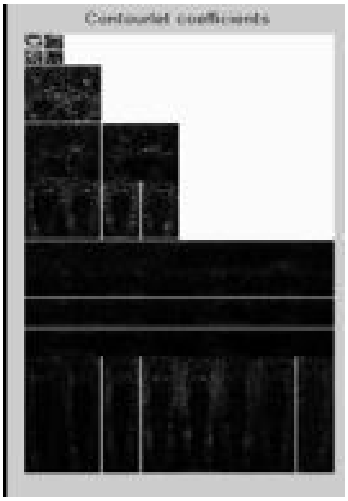


Fig. 16 Contourlet Coefficients

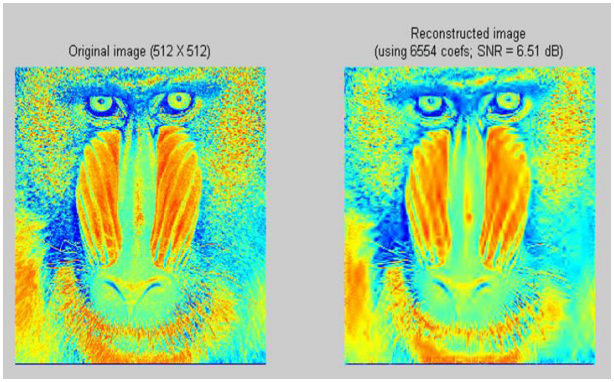


Fig. 17 Contourlet Nonlinear Approximation

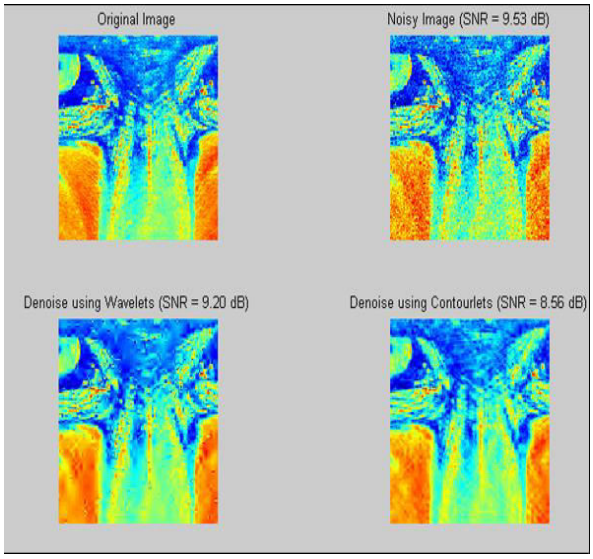


Fig. 17 De-noising by wavelets and by contourlets

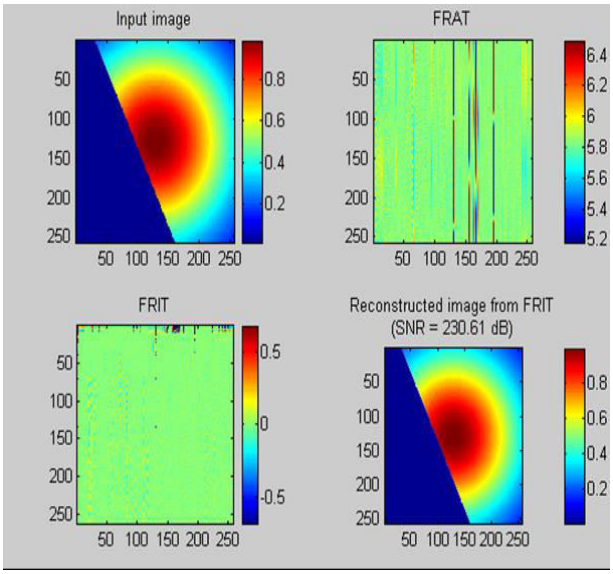


Fig. 18 Ridgelet Transform

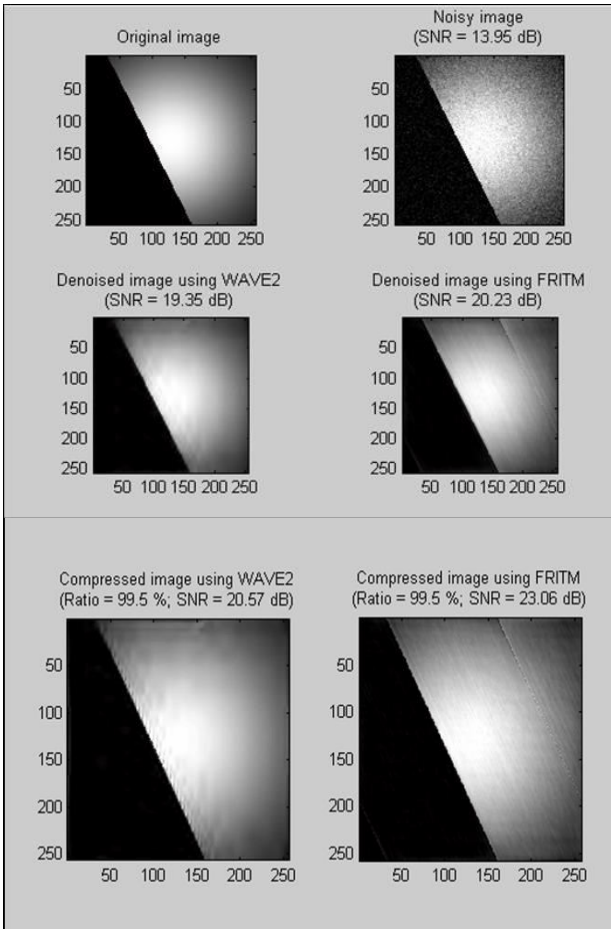


Fig. 19 Comparison of Wavelet and Ridgelet Transform

VII. CONCLUSIONS

In this paper several transforms are described and their interrelationships. In this paper, we have used the ridgelet transform of real world images in order to produce low-levels features. Ridgelet based features seems to capture efficiently man-made elements within the scene. The ridgelet transform is relatively fast compared to the Gabor filters because it does not require a filter response calculation. Further work directions will try to incorporate color information within this framework and study localized ridgelet transform (monoscale ridgelets and curvelets). Higher order moments should also be investigated such as the fourth order moment which is related to the signal kurtosis. However, construction of a representative and exhaustive training set remains a challenge because of the wide varation in scene content. Another challenge is the robustness to variations in the photographic point of view.

Different statistical learning methods have been used, the nonlinear methods produced better classification rate but numerical implementation is still an issue. Linear discriminant methods are less performant but are faster and results interpretation is easier.

In many applications human perception of the fused images is of a fundamental importance and as a result the enhancement results are mostly evaluated by subjective criteria. The experimental results show that the fusion algorithm gives encouraging results for both multi modal and multi focal images. Since the image salient features such as edges lines and contours are well represented using the contourlet transform, the fusion process did not introduce any distortion to the original image.

Directional information introduced by the contourlet transform yields the best description of the all the salient information in the both test images. Thus the composite image is more complete and looks natural and the noise level is minimal. Utilization of the composite image is expected to increase the performance of the subsequent processing tasks. By integrating information, this approach can reduce dimensionality. This results in a more efficient storage and faster interpretation of the output. Using redundant information, the composite image increases the accuracy as well as reliability, and using complementary information, the process also improves interpretation capabilities with respect to subsequent tasks. This leads to more accurate data, increased utility and robust performance.

REFERENCES

[1] Averbuch,A., Coifman,R. R.,Donoho,D. L.,Israeli,M.,andWald en,J.(1999) Rec-to Polar FFTandits Applications. Manuscript.

[2] Candµ es,E.(1999)Harmonic Analysis of Neural Networks, Appl.Comput. Harmon. Anal. 6 (1999),197{218.

[3] Candµ es,E.(1998) Ridgelets: Theoryand Applications. Ph.D.Thesis, Department of Statistics, Stanford University.

[4] Candµ es,E.(1999) Monoscale ridgelets for the representation of images with edges, Technical Report, Statistics, Stanford.

[5] Candµ es,E.(1999)On the Representation of Mutilated Sobolev Functions. Technical Report, Statistics, Stanford.

[6] Candµ es,E.and Donoho,D.(1999)Ridgelets: The key to High-Dimensional Intermittency?.Phil.Trans.R.Soc.Lond.A. 357 (1999),2495-2509

[7] Candµ es,E.andDonoho,D.(1999) Curvelets. Manuscript.

[8] Candµ es,E.andDonoho,D.(1999)Curvelets: a surprisingly effective nonadaptive representation for objects with edges. in Curves and Surfaces IV ed.P.-J.Laurent.

[9] Candµ es,E.andDonoho,D.(1999)Curvelets and Linear Inverse Problems. Manuscript.

[10] J.-L. Starck, E. Candès and D. Donoho, The Curvelet Transform for Image Denoising, IEEE Transactions on Image Processing, Vol. 11, No. 6, pp.670-684, 2002.

[11] E .J.Cand` esandF.Guo(2002).New Multiscale Transforms, Minimum Total Variation Synthesis: Applications to Edge-Preserving Image Reconstruction. Signal Processing 82, 1519–1543.

[12] Cand` es,E.J.;Demanet,L.(2003).Curvelets and Fourier integral operators. C.R. Acad.Sci.Paris,Ser.I 336, 395–398.

[13] M.N.DoandM.Vetterli,"The contourlet transform: an efficient direction almultiresolution image representation," IEEETrans. ImageProc.,vol.14,no.12,December2005.

[14] P.J.BurtandE. H.Adelson," The Laplacian pyramid as a compact image code," IEEETrans.Comm.,vol.COM-31,pp.532–540,April1983.

[15] R.H.Bambergerand M.J.T.Smith," A filter bank for the directional decomposition of images: theory and design," IEEE Trans.SignalProc.,vol.40,no.4,pp.882–893,April1992.

[16] E.J.Cand` es,L.Demanet, D.L. Donoho, and L.Ying," Fast discrete curvelet transforms,"Tech. Rep., Appliedand Computational Mathematics, California Institute of Technology,2005.

[17] T.ChenandP.P.Vaidyanathan,"Consideration sinmulti dimensional filter bank design,"in Proc.IEEEInt. Symp.Circ.and Syst.,Chicago,Illinois,USA,May1993,pp.643–646.

[18] R. Arps and T. Truong. "*Comparison of international standards for lossless still image compression*", *Proceedings of the IEEE,* 82(6):889-899, June 1994.

[19] Alessandro J. S. Dutra, William A. Pearlman,and Eduardo A. B. da Silva. *"Successive Approximation Wavelet Coding of AVIRIS Hyperspectral Images", IEEE Journal of Selected Topics in Signal Processing,* Vol. 5, No. 3, June 2011.

[20] Arian Maleki, Boshra Rajaei, and Hamid Reza Pourreza. *"Rate-Distortion Analysis of Directional Wavelets", IEEE Transactions on Image Processing*, Vol. 21, No. 2, February 2012.

[21] Amar Aggoun. *"Compression of 3D Integral Images Using 3D Wavelet Transform", Journal of Display Technology,* Vol. 7, No. 11, November 2011.

[22] A. Bouridane, F. Khelifi, A. Amira, F. Kurugollu, and S. Boussakta, *"A very low bit-rate embedded color image coding with SPIHT,"* in IEEE Int. Conf. Acoustic, Speech, and Signal Processing, Apr. 2004, vol. 4, pp. 689–692.

[23] Bo Li, Rui Yang, and Hongxu Jiang. *"Remote-Sensing Image Compression Using Two-Dimensional Oriented Wavelet Transform", IEEE Transactions on GeoScience and Remote Sensing,* Vol. 49, No. 1, January 2011.

[24] E. J. Cand`es and D. L. Donoho, *"Curvelets - a surprisingly effective nonadaptive representation for objects with edges,"* in *Curve and Surface Fitting*, A. Cohen, C. Rabut, and L. L. Schumaker, Eds. Saint-Malo: Vanderbilt University Press, 1999.

[25] Ed Chiu, Jacques Vaisey, and M. Stella Atkins. *"Wavelet-Based Space-Frequency Compression of Ultrasound Images", IEEE Transactions on Information Technology in Biomedicine*, Vol. 5, No. 4, December 2001.

[26] O. N. Gerek and A. E. C¸ etin, *"A 2-D orientation adaptive prediction filter in lifting structures for*

image coding," IEEE Trans. Image Processing, vol. 15, no. 1, pp. 106–111, Jan. 2006.

[27] Garima Chopra and A. K. Pal. *"An Improved Image Compression Algorithm Using Binary Space Partition Scheme and Geometric Wavelets", IEEE Transactions on Image Processing,* Vol. 20, No. 1, January 2011.

[28] Hiroaki Myoren, Yun Kimimoto, Kosuke Terui, and Tohru Taino. *"Design of Digital DROSWith SFQ Up/Down Counter for Wide Dynamic Operation Range", IEEE Transactions on Applied Superconductivity,* Vol. 21, No. 3, June 2011.

[29]G. Langdon. Sunset: a hardware algorithm for lossless compression of gray scale images. In *Medical Imaging V: Image Capture, Formatting, and Display,* volume 1444, pages 272-282. SPIE, March 1991.

[30] D. Le Gall and A. Tabatabai. Sub-band coding of digital images using symmetric short kernel filters and arithmetic coding techniques. In International Conference on Acoustics, Speoch and Signal Processing, pages 761-765, New York, 1988. IEEE

[31] A. Munteanu, J. Cornelis, G. Van der Auwera, and P. Cristea, *"Wavelet image compression—The quadtree coding approach,"* IEEE Trans. Inf. Technol. Biomed., vol. 3, no. 3, pp. 176–185, Sep. 1999.

[32] S. Mallat, *A Wavelet Tour of Signal Processing*. San Diego, CA: Academic Press, 1997.

[33] Masashi Nishiyama, Abdenour Hadid, Hidenori Takeshima, Jamie Shotton, Tatsuo Kozakaya, and

Osamu Yamaguchi. *"Facial Deblur Inference Using Subspace Analysis for Recognition of Blurred Faces", IEEE Transactions on Pattern Analysis and Machine Intelligence,* Vol. 33, No. 4, April 2011.

[34] Marijn J. H. Loomans, Cornelis J. Koeleman, and Peter H. N. de With, *"Low-Complexity Wavelet-Based Scalable Image & Video Coding for Home-Use Surveillance",* IEEE 2011.

[35] Michel Barret, Jean-Louis Gutzwiller, and Mohamed Hariti. *"Low-Complexity Hyperspectral Image Coding Using Exogenous Orthogonal Optimal Spectral Transform (OrthOST) and Degree-2 Zerotrees", IEEE Transactions on Geoscience and Remote Sensiong*, Vol. 49, No. 5, May 2011.

[36] W. A. Pearlman, A. Islam, N. Nagaraj, and A. Said, *"Efficient, lowcomplexity image coding with a set-partitioning embedded block coder,"* IEEE Trans. Circuits Syst. Video Technol., vol. 14, no. 11, pp. 1219–1235, Nov. 2004.

[37] Reto Grüter, Oliver Egger, Jean-Marc Vesin, and Murat Kunt, *"Rank-Order Polynomial Subband Decomposition for Medical Image Compression", IEEE Transactions on Medical Imaging*, Vol. 19, No. 10, October 2000.

[38] Sorina Dumitrescu, Geoffrey Rivers, and Shahram Shirani. "Unequal Erasure Protection Technique for Scalable Multistreams*", IEEE Transactions on Image Processing,* Vol. 19, No. 2, February 2010.

[39] A. Said and W. Pearlman. *"Reversible image compression via multiresolution representation and predictive coding".* In *Visual Communications and ImageProcessing,* volume 2094, pages 664-674. SPIE, November 1993.

[40] X. Tang and W. A. Pearlman, *"Progressive resolution coding of hyperspectral images featuring region of interest access,"* in Proc. SPIE Defense and Security, May 2005, vol. 5817, pp. 270–280.

[41] Ulug Bayazit. *"Adaptive Spectral Transform for Wavelet-Based Color Image Compression", IEEE Transactions on Circuits and Systems for Video Technology,* Vol. 21, No. 7, July 2011.

[42] Victor Sanchez*, Rafeef Abugharbieh, and Panos Nasiopoulos, *"3-D Scalable Medical Image Compression with Optimized Volume of Interest Coding", IEEE Transactions on Medical Imaging,* Vol. 29, No. 10, October 2010.

❑❑❑

Reduction of Liars to Improve Trust Level in Mobile Ad hoc Network

G. Abinaya & R. Ramachandran
Computer Science and Engineering, Sri Venkateswara College of Engineering, Chennai, India
E-mail : abi.msg@gmail.com & rramaach@gmail.com

Abstract - Mobile Adhoc Network (MANET) is a self-configuring, infrastructureless network of mobile devices connected by wireless links. Each device in a MANET is free to move independently in any direction. The lack of central co ordination and shared wireless medium in adhoc network makes them more vulnerable to attacks than wired network. So, all the nodes must cooperate with each other in order to route the packets. Co-operating nodes must trust each other by exchanging trust information about nodes within the radio range. Recommendation Exchange Protocol is used to improve the trust level among the group of nodes in MANET. It helps to avoid the effect of colluding attacks composed of liars and also reduces the communication among the malicious nodes. Hence this paper focuses on the importance of improving trust level in Mobile Adhoc Network. The simulation study is performed using Network Simulator NS 2.29.

Keywords- *Adhoc Networks, Attacks, Trust, Security.*

I. INTRODUCTION

Mobile adhoc network is an autonomous system of mobile devices connected by wireless links. The devices are free to move randomly and organize themselves arbitrarily. Mobile Ad-hoc Network is a communication network without a pre-exist network infrastructure. It is built spontaneously as devices get connected. Instead of relying on a base station to co-ordinate the flow of messages to each node in network, the individual network nodes forward packets to and from each other. As a result, nodes play the role of router, compelling them to cooperate for the correct operation of the network. Specific protocol has been proposed for Adhoc networks considering not only its peculiar characteristics, also a perfect co-operation among nodes. In general, it is assumed that all nodes behave according to the application specifications. However, this assumption may be false, due to resource constraint or misbehavior nodes etc .If malicious nodes are present in a MANET, and they may attempt to reduce network connectivity by pretending to be co-operative. These actions may result in defragmented networks, isolated nodes, and drastically reduced network performance. The assumption that nodes behave correctly can lead to unexpected pitfalls, such as resource consumption, and vulnerability to attacks. Moreover, malicious nodes can work together to improve the effectiveness of the attack. For instance, nodes could lie about malicious node to cover its real nature. Therefore, a mechanism that allows a node to infer the trustworthiness of other nodes become necessary. According to the paradigm of autonomic networks, nodes are capable of self-configuring, self-managing, and self-learning by means of collecting local information and exchanging information with its neighbors. Thus it is important to communicate only with trusted neighbor nodes, because the exchange of information with compromised nodes can deteriorate the autonomy of adhoc networks.In general, if the interactions among nodes have been faithful to the protocol, then trust will accumulate between these nodes. Trust has also been defined as the degree of belief level that one node can put on another node for a specific action based on previous direct or indirect observations on behaviours of the node. The nodes in the network evaluate trust for other participating nodes and then form trust relations between them. Nodes study about malicious nodes based on the information exchanged with trustworthy neighbors. Trust is dynamic, not static. Trust is not necessarily transitive; the fact that node A trusts node B and B trusts node C does not imply that A trusts C. Trust is asymmetric and not necessarily reciprocal. The trust information is based on individual experiences and on the recommendations of other nodes in the network.

Recommendation Exchange Protocol (REP) which allows nodes to exchange recommendations about their neighbor nodes. Nodes in the network exchange information with its neighbor nodes. It is difficult to maintain trust information for all nodes, Due to issues like mobility or battery constraints. As a result, nodes do not keep trust information about every node in the network. Nodes use the Recommendation Exchange Protocol (REP) to send and receive recommendations. The effect of liars on the trust evaluation process is analyzed.

The rest of this paper is organized as follows. The related work is discussed in Section II and Section III describes the proposed work. Section IV describes the performance evaluation of our work. Finally, section V presents the conclusion. The simulation study is performed using Network Simulator NS 2.29.

II. RELATED WORK

This section discusses about the literature survey done on various issues like mobility and topology changes, various attacks, co-operation among the selfish nodes and malicious nodes, trust relationship among the group of nodes as well as security in the Mobile Adhoc Networks.

Marti S et al [5] proposed Mitigating routing misbehavioring mobile ad hoc networks, in which two techniques were used to improve throughput in an ad hoc network in the presence of nodes that agree to forward packets. To mitigate this problem, watchdog that identifies misbehaving nodes and a pathrater that helps routing protocols to avoid these misbehaving nodes are used. It could be used to some extent to detect replay attacks. Watchdog's weakness is that, it might not detect a misbehaving node in the presence of ambiguous collisions, receiver collisions, limited transmission power, false misbehavior, collusion, and packet dropping.

Zhong S et al [10] proposed Sprite: a simple, cheat-proof, credit based system for mobile ad-hoc networks, in which Sprite, a simple, cheat-proof, credit based system is used for stimulating co operation among selfish nodes in MANET and provides incentive for mobile nodes to cooperate and report actions honestly. The fundamental operations of Sprite system are to provide incentive to selfish mobile nodes to cooperate. Motivates each node to report its actions honestly, even when a collection of the selfish nodes collude. Sprite system can only handle co operation among selfish nodes. Credit based system provides credit for selfish nodes and reports honestly about each nodes when a collection of the selfish nodes will collude, the cheat proof system is used to ensure the best choice for each nodes. This paper does not deal with the trust management concept.

Yu W et al [9] proposed Attack-resistant cooperation stimulation in autonomous ad hoc networks, in which an Attack-Resilient Cooperation Stimulation (ARCS) system for autonomous ad hoc networks is to stimulate cooperation among selfish nodes and defend against malicious attacks. In the ARCS system, the damage that caused by malicious nodes can be bounded, the cooperation among selfish nodes can be enforced, and the fairness among nodes can also be achieved.

The fundamental operations of ARCS are collusion-resistant. ARCS handle the possible emulating link breakage attacks. The number of route request packets that can be injected by each node is bounded by 1.Another key property of the ARCS system lies in that it is completely self-organizing and fully distributed, it cannot handle well when the malicious nodes have entered the network and this system can only handled co operation among selfish nodes.

Pirzada A.A et al [6] proposed the“Trust establishment in pure ad-hoc networks," in which a trust-based model is used for communication in ad-hoc networks that is based on individual experience rather than on a third party advocating trust levels. The model introduces the notion of belief and provides a dynamic measure of reliability and trustworthiness in pure ad-hoc networks. But the trust mode method also affected by some kind of attacks, such as slander attack in the presence of malicious nodes.

Li R et al [4] proposed the “Future trust management framework for mobile ad hoc networks," which evaluates the trust of participating nodes. The trust management framework is used to force nodes to cooperate in a normal way. Trust is evaluated only by direct observation. The core protocols were used to ensure the co operation among the selfish nodes and isolate misbehaving nodes. However these schemes suffer from some problem and many attacks. Observation by other node provides more vulnerability in the presence of untrusted nodes.

Ishibashi et al [2] proposed Topology and mobility considerations in mobile ad hoc networks, in which a number of statistics were collected from the topologies and mobility patterns of mobile adhoc networks. Connectivity, node degrees, and path lengths were presented, along with link lifetimes and times to route failures. A highly dynamic topology is a distinguishing feature and challenge of a mobile ad hoc network. Links between nodes are created and broken, as the nodes move within the network. This node mobility not only affects the source and/or destination, as in a conventional wireless network, but also intermediate nodes, due to the network's multihop nature. The issues that were surveyed from the existing system are listed below:

a) Existing system is affected by the wrong observations of other nodes in the network.

b) It also affects the network performance in the presence of liars.

c) Some protocol can handle only the co-operation among selfish nodes.

III. PROPOSED WORK

The basic idea of this paper is to build a trust model that provides nodes with a mechanism to evaluate the trust level of its neighbor nodes. A node assigns a trust level for each neighbor, which represents how trustworthy each neighbor nodes in the network. The key concept such as relationship maturity model and Recommendation Exchange Protocol are used to build the trust relationship among group of nodes as well as they send recommendations about the neighboring nodes. Therefore, similar to the concept of human trust, the computation of the trust level of a given neighbor is based on previous experiences and also on the opinion of other neighboring nodes. By previous experiences, a node keeps track of the good and bad actions taken by its neighbors.

The main objective of proposed system is to detect malicious nodes and reduce the communication among the malicious nodes using advanced mechanism. Also increases the performance and trust level among the group of nodes. The proposed system possesses the following advantages. They are

a) Use Recommendation Exchange Protocol.
b) Increase the performance and trust level among the group of nodes.
c) Detect black hole attack in the presence of liars.
d) Reduces the communication among the malicious nodes in the network.

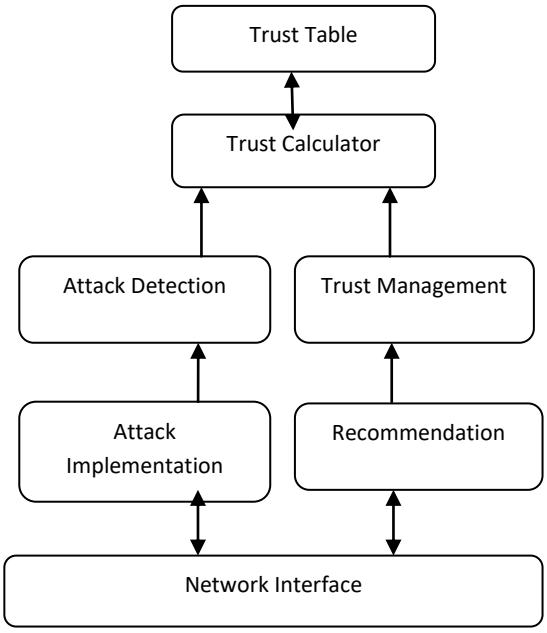


FIGURE 1: Architecture Diagram of Trust Model

The Figure 1 shows the architecture diagram of the trust model. Initially, the Blackhole attack is implemented then the attack is detected in the network. Trust management provides the trust relationship among the group of nodes using Recommendation Exchange Protocol and Relationship Maturity Model. These protocols were used to reduce the number of liars present in the networks. Each node maintains a trust table containing the trust level for each neighbor nodes in the network. The trust level is based on the opinion from neighbor nodes about their common neighbors in the network. Each entry on the trust table is associated with a timeout. Finally, the trust calculator evaluates the trust level based on the trust values received from the individual experiences (Attack implementation and Attack Detection) and the Neighbor recommendations (Trust Management)

A. ATTACK IMPLEMENTATION

This section describes the implementation of blackhole attack. The blackhole attack is implemented using AODV routing protocol. Blackhole attack is a severe attack that can be easily implemented in MANET. A blackhole is a malicious node that falsely replies for any route request without having an active route to a specified destination and if packets were transferred through the affected nodes then it will drop all the receiving packets. AODV routing protocol provides three message controls, they are Route Request, Route Reply and Route Error messages. In Blackhole attack, a malicious node waits for source nodes to send RREQ messages. When the malicious nodes receives RREQ message, without checking its routing table, immediately sends false RREP message giving a route to destination over itself. Therefore requesting nodes assume that route discovery process is completed and ignore other RREP messages and begin to send packets over malicious node. Malicious nodes affect all RREQ messages of their neighbor nodes. Therefore all packets are dropped and never forwarded to proper destination. These malicious nodes work together as a group to damage the entire network.

B. ATTACK DETECTION

In this detection mechanism, malicious nodes were detected by using AODV routing protocol. This technique is mainly used to prevent the malicious nodes in the network. When a source node wants to send packets to the destination node, if any node is affected by blackhole attack then an intermediate node will send the information about the malicious node to the source node. The identity of malicious node is maintained, so that in future, the source nodes can discard any control messages coming from this node. The control messages

from these malicious nodes, too, not forwarded in the network.

C. TRUST MANAGEMENT

The concept of trust is very important when a node communicates with other nodes in the network. The process of evaluating trust level possesses several advantages. First, a node can detect malicious nodes and stops sending packet to the malicious node. Secondly, co-operation is stimulated by selecting the neighbors with higher trust levels. In trust management, a Relationship Maturity model which builds a trust relationship between nodes in an Adhoc networks. The trust is based on the previous experiences and on the recommendation of other nodes. The Recommendation Exchange Protocol (REP) allows nodes to exchange recommendations about their neighbors. Thus, this trust management is mainly used to collect recommendations from neighbor nodes and evaluate the trust level for a given node by using the formula as below,

$$T_a(b) = (1-k)\, F_a + k\, R_a(b) \qquad (1)$$

Where F_a is the value used by node 'a' according to the adopted strategy, R_a (b) is the aggregate recommendation of neighbors about node 'b', and 'k' is the weight factor that allows us to give more relevance to the desired parameter. The source node get accusation message about its immediate neighbor. If it gets more accusation messages for the same nodes then that node will be added to liar's node list and isolated from other nodes. When the node is detected as a liar node, it will not accept any accusation messages from that node. Thus the trust level among the nodes is expected to increase.

IV. PERFORMANCE EVALUATION

The table 1 shows the different simulation parameters used to setup the scenario.

TABLE 1 SIMULATION PARAMETER

Parameter	Value
Simulator	NS-2(version 2.29)
Simulation time	50s
No. of nodes	10-20
Routing Protocol	AODV
Traffic Model	CBR
Terrain area	750m x 750m
Transmission Range	250m
No. of malicious nodes	2
Packet size	512 bytes

The figure 2 shows graph representing the packet delivery ratio in the presence of malicious nodes in Mobile Adhoc Networks without any detection or prevention method. As the number of malicious nodes increases in the network, there is an increase in packet loss.

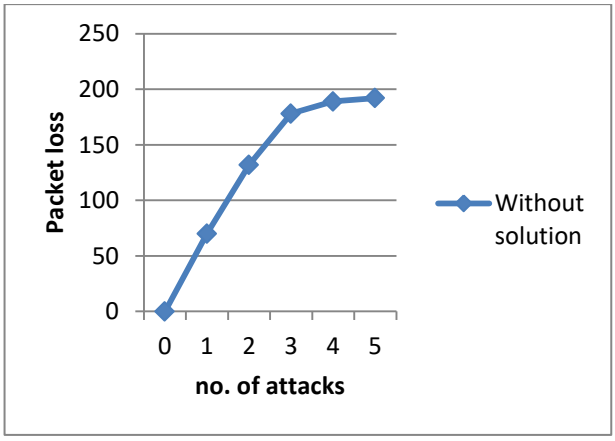


FIGURE 2: Packet Delivery Ratio Under Attack

The figure 3 shows graph representing the packet delivery ratio in the presence of malicious nodes in Mobile Adhoc Networks with detection or prevention method. As the number of malicious nodes increases in the network, there is a decrease in packet loss by using the solution.

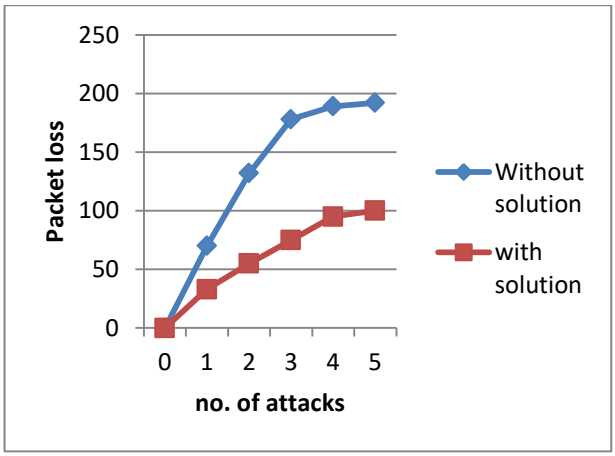


FIGURE 3: Packet Delivery Ratio in the Network

Thus this section discusses about performance evaluation of our work. Thus the number of liars in the network is expected to decrease in order to increase the trust level of the nodes.

V. CONCLUSION

In Mobile Adhoc Networks, all the nodes must cooperate with each other in order to route the packets. Co-operating nodes must trust each other. The lack of base station and shared wired medium provides more vulnerability in the presence of liars. The packet loss will occur due to the malicious nodes and also it will reduce the performance of the networks. For this purpose trust model has been generated. This model can be classified into three different mechanisms, which include attack implementation, attack detection, trust management, and it will be evaluated successfully. Thus the effective trust model is generated to reduce the communication among the malicious nodes and improve the performance of the Mobile Adhoc Networks.

REFERENCES

[1] Buchegger and J.Y.Le Boudes, "The effect of rumor spreading in reputation system for mobile ad-hoc networks", Processing of Modeling and Optimization Mobile Adhoc Wireless Network,vol 7,no.6,pp.963-976,2003

[2] B.Ishibashi, "Topology and Mobility consideration in Mobile Adhoc Networks", Asiam Journal of Adhoc Network vol.3, no.6, pp.362-776, 2005.

[3] R.P.Laufer, G.Pujolle,"Analyzing a human-based trust model for mobile Adhoc networks", Proceedings of IEEE Symposium in Computing Communication, vol.47, no.4, pp.445-487, 2008.

[4] Li and J.Kato, "Future trust management framework for mobile Adhoc networks", International Journal on selected Areas in Communication, vol.46,no.4,pp.108-114,2008

[5] Marti and K.Lai, "Mitigating routing misbehavior in mobile ad hoc networks", Proceedings of International Conference on Mobile Computing a Networking vol.47, no.4, pp.445-487, 2000.

[6] Pirzada and Donald, "Trust establishment in pure Adhoc networks", International Journal in Wireless Personal Communication, vol.37, no.1-2, pp.19-168, 2006.

[7] Pedro.B.Velloso, "Trust management in mobile Adhoc networks using a scalable maturity-based model", IEEE Transaction on network and services management, vol.7, no.3, pp.172-185, 2010.

[8] Velloso, R.P.Laufer,"A trust model robust to slander attack in Adhoc networks", Proceedings of IEEE International Conference in Mobile Adhoc Networks, vol.36, no.8, pp.126-132, 2008.

[9] Yu and K.J.Liu, "Attack-resistant co-operation simulation in autonomous adhoc networks", International Journal on selected areas in communications, vol.23, no.12, pp2260-2271, 2005.

[10] Zhong and Yang, "Sprite: a simple, cheat-proof, credit based system for mobile Adhoc networks", IEEE Transaction on Informatics and communication, vol.2, no.7, pp.2790-2796, 2003.

[11] http://tools.ietf.org/html/draft-ietf-manet-aodv-13.

❑❑❑

Energy-Efficient Multicasting of Scalable Video Streams over WiMAX Networks

Ramesh & P.S.Balamurugan

Department of Computer Science and Engineering, Karpagam University,
Coimbatore, Tamilnadu, India

Abstract Worldwide Inter-operability for Microwave Access, largely known as WiMAX is a telecommunication technology designed to provide effective transmission of data using transmission mode In order to provide effective transmission of data with minimum delay, it is necessary for the WiMAX base station and the subscribers to obtain a clear line-of-sight. Large objects such as buildings and trees can interfere with the signals which would result in packet loss and delay. In order to avoid this unfortunate scenario WiMAX uses mesh mode topology that allows subscriber stations to communicate directly with each other while communicating with the base station. The base station can route the information to that client via another client that has a clear line-of-sight. Furthermore, WiMAX uses a scheduling algorithm for exchange of data meaning the subscriber stations transmit data in their scheduled slots which helps minimize interference within networks. Video content are the information provided by various video applications such as newscasts, sports programs and movies that can be stored and viewed later on or live. Since transmitting video content takes a lot of bits, they are broken into a sequence of frames or images, compressed and sent to subscribers which are viewed at a constant frame rate.Due to compression and decompression methods, frame loss up to a certain extent can go unnoticed to the human eye. However, delays or variations in the playback can greatly decrease the quality of the videovideo streaming can be considered as a loss-tolerant, delay-sensitive mechanism

Keywords*—WIMAX, loss, delay, compressed, video streaming*.

I. INTRODUCTION

Worldwide Inter-operability for Microwave Access, largely known as WiMAX is a telecommunication technology designed to provide effective transmission of data using transmission modes "from point-multipoint links to portable and fully mobile Internet access". The technology is so advanced that it can provide up to 72 Mbps symmetric broadband speed without cables.[1] The traditional cable-based access networks can deliver content only to subscribers at fixed points. This technology appears to be outdated for the modern world where an alarming rate of people use cell phones and other portable electronic devices such as laptops to do their daily work at mobile locations. Therefore, there is an increasing demand for a new technology that can deliver information to mobile users.[4] WiMAX is intended to surpass the current, expensive network transmission technologies such as Asynchronous Digital Subscriber Line (ADSL) and T1 line and provide fast and cheap broadband access especially to rural areas lacking the necessary infrastructure such as optical fiber and copper wires. WiMAX operates in the frequency range of 10GHz - 66GHz as it has less interference and more bandwidth. A lower range of frequency band was later introduced which operates between 2GHz and 11GHz . There are two main types of WiMAX services: mobile and fixed. Mobile WiMAX enables users access Internet while traveling whereas fixed WiMAX stations provide wireless Internet access to clients within a fixed radius. Moreover, WiMAX is capable of delivering high speed wireless services up to a range of approximately 50km which is far longer than that of DSL, cable modem, etc. which has a span of approximately 5.5km. [2]

WiMAX is an evolving set of the commercialization of IEEE 802.16 standard which was initiated at the National Institute of Standards and Technologies in 1998. In June 2004, it was transferred to the IEEE for the purpose of forming a working group 802.16.[5] The WiMAX forum, which was established in 2001comprises of a group of industry leaders such as Intel, AT&T, Samsung, Motorola, Cisco etc who are entitled to support as well as promote the technology by certifying products that conform to the WiMAX standards.

In order to provide effective transmission of data with minimum delay, it is necessary for the WiMAX base station and the subscribers to obtain a clear line-of-sight. Large objects such as buildings and trees can interfere with the signals which would result in packet

loss and delay. In order to avoid this unfortunate scenario WiMAX uses mesh mode topology that allows subscriber stations to communicate directly with each other while communicating with the base station. This way, if the line-of-sight between one client and the base station is interfered, the base station can route the information to that client via another client that has a clear line-of-sight.[1] Furthermore, WiMAX uses a scheduling algorithm for exchange of data meaning the subscriber stations transmit data in their scheduled slots which helps minimize interference within networks.

II. VIDEO STREAMING

Video content are the information provided by various video applications such as newscasts, sports programs and movies that can be stored and viewed later on or live. Since transmitting video content takes a lot of bits, they are broken into a sequence of frames or images, compressed and sent to subscribers which are viewed at a constant frame rate.[3]

Due to compression and decompression methods, frame loss up to a certain extent can go unnoticed to the human eye. However, delays or variations in the playback can greatly decrease the quality of the video which leaves the client unhappy. Therefore, video streaming can be considered as a loss-tolerant, delay-sensitive mechanism which has to be carefully balanced to produce quality video at high Signal-to-Noise Ratio levels (SNR).

Moreover, video content are characterized by the following parameters:

- Video format (the horizontal by vertical pixel resolution)
- Pixel color depth (the number of bits/pixel that describes the color of each pixel)
- Video coding scheme (the mechanism that compresses/decompresses the video)
- Frame inter-arrival rate (the rate at which the frames are received and played back)

Different media uses different video formats and pixel resolutions. A table containing the resolutions and the associated media is shown below

Table 1: Resolution vs. video format

Video format	**Resolution**
Video CD	350×240
Umatic, Betamax, VHS, Video8	330×480
Analog broadcast	440×480
D-VHS, DVD, miniDV, Digital8, Digital Betacam (pro)	720×480
D-VHS, HD DVD, Blu-ray, HDV (miniDV)	1280×720
IMAX, IMAX HD, OMNIMAX	10,000×7000

From the above table, one can see that the number of pixels increases with output quality. Since videos are displayed as a sequence of images, many of these image frames contain spatial (within frame) and temporal (between frames) redundancy. It would cost a lot of memory in order to store all of these frames and thus it appears to be inefficient. As a result, many video coding schemes have been developed to reduce the size video streams by exploiting the redundancies while balancing quality. [6]

The most common video codecs are the H.26x standards and the MPEG-x (Motion Picture Exports Group) standards. In this project, we hope to use an MPEG video codec to compress a video stream.[5] The compression and raw data rates of several MPEG codecs are shown in Table 2 below

Table 2: MPEG-x codec information

Codec	**Raw data rate**	**Compressed rate**
MPEG-1	30Mbps	1.5Mbps
MPEG-2	128Mbps	3-10Mbps
MPEG-4	512Mbps	<1.024Mbps

Video streaming experiences many types of delays while being transmitted from the sender to the receiver. End-to-end delays, propagation delays, processing and queuing delays are the most common types of delays present in video streaming.[6] Later on in this project, we hope to gather statistics of video streaming delays using the Opnet modeler.

III. SYSTEM PERFORMANCE

WiMAX operates similarly to Wi-Fi technology but at higher speeds, over larger distances, and accommodates more wireless users. As illustrated in Figure.1, WiMAX system consists of a WiMAX-enabled base station or tower, and a subscriber station or receiver. WiMAX towers are implemented by service providers and can provide a wireless service footprint as large as 2,500 square miles, similar in concept to cellular communications towers. This capability provides broadband wireless access for users in remote

rural areas, which can be difficult to reach with wires used by traditional telephone and cable companies. Initially, WiMAX receivers and antennas will consist of a small box or Personal Computer Memory Card International Association (PCMCIA) card, and eventually will be developed into portable devices that will be comparable to Wi-Fi-enabled products (e.g., laptops, telephones, PDA) on the market today.[6]

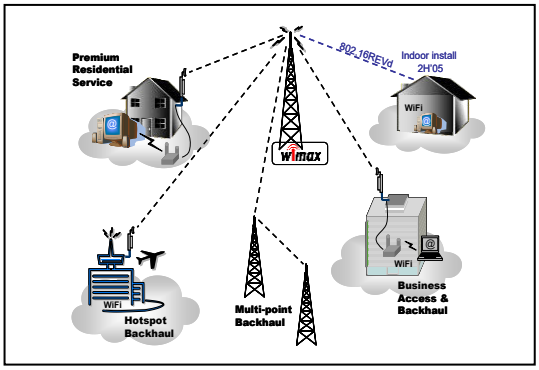


Figure.1. WiMAX System

A. Frequency Reuse

The network topology is basically divided in to clusters of *N* cells. Each cell in the cluster has a different frequency allocations; *S* sectors per cell and *K* different frequency allocations per cell. Thus, the frequency reuse pattern can be represented as $N \times S \times K$. [8] Figure. 2. shows a network topology with reuse pattern $1 \times 3 \times 3$. The colored markings in the center of each cell indicate the sectors and point in the bore sight direction. The red markings correspond to sectors deployment in the same frequency allocation. The blue and green markings indicate the other two frequency allocations for a reuse three network. Networks with universal frequency reuse $1 \times 3 \times 1$ have the same network topology except the same frequency allocation is deployed in all sectors throughout the network. Thus, an operator using, say, 10 MHz channelization would require a total of 10 MHz of spectrum to support a time division duplexing (TDD) system with $1 \times 3 \times 1$ reuse. To reduce interference, a frequency reuse pattern of $1 \times 3 \times 3$ can be implemented by either sharing the available sub channels (say 1/3) in a 10 MHz channel or using 30 MHz of spectrum with 10 MHz in each sector. [8]

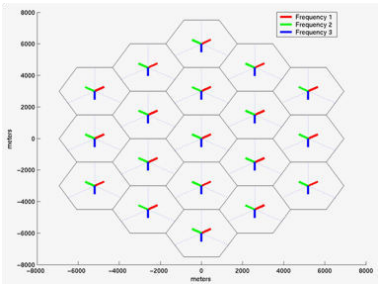


Figure. 2. Network topology for tri-sector (19 cell) configuration with 1×3×3 reuse.

B. Signal level and File Format

An IGMP proxy entity located at the BS or at the AR to report Membership on behalf of its subordinate wireless hosts. No IGMP message is transmitted over wireless channels,. The key idea is to perform the IGMP message conversion at the IGMP proxy based on MAC-layer multicast connection information. This is possible because there is a one-to-one mapping between the MAC-layer multicast connection and the IP-layer multicast stream. When a user joins or leaves an IP multicast group, it triggers the MAC-layer DSA/DSD messages to establish or release a multicast connection, and sends IGMP Join/Leave Message as well. If the MS leaves the regime of a BS without explicitly sending messages to inform BS of its leaving, such as in the case of uncontrolled handover, the BS can detect the condition easily by periodic ranging and in turn update the information of multicast connections related to the MS.[7] Therefore, from the necessary MAC-layer management messages, the BS can actually acquire enough information of its subordinate MSs' interests in a multicast group. IEEE 802.16e allows flexible mapping between multicast connection and IP multicast stream(s). For example, one multicast connection can be specified to serve more than one IP multicast streams. In our proposal, one IP multicast stream is mapped to one multicast connection. The one-to-one mapping approach has the advantage of saving MS's power consumption.

Since a TV channel is one-to-one mapped to a multicast CID, the MS can decode only the selected TV program indentified by the CID and save the power of decoding other unwatched TV programs. Secondly, IEEE802.16 allows static and dynamic provisioning of multicast connections and preserves limited CID space for multicast connections. We choose to use on-demand provisioning of multicast connection because it uses system resources like bandwidth more efficiently than the static provisioning method.[9] The cross-layer multicast management scheme for IGMP proxy located at AR . The host joining a TV program will initiate a DSA request to establish a MAC-layer connection with a CID for traffic transport. BS has information of all active multicast connections and tunnels the information from BS to the AR via R6 reference point. Based on the MAC-layer information, the IGMP proxy directly sends IGMP Report to the upstream multicast router if there is no member in the requested group. When receiving an IGMP Query message, the AR does not forward it to all MSs as in Fig. 2, but instead, replies directly based on the up-to-date multicast connection information of its subordinate hosts.

When the host leaves the multicast group, it initiates a DSD request to release the multicast connection. And the IGMP proxy sends IGMP Leave

message on behalf of the host, if there is no member in the multicast group. Compared with the traditional multicast management scheme in the proposed system totally eliminates the multicast service interruption phenomenon and avoids IGMP's disruption to MS's sleep mode. Besides, the precious radio transmission resources can be saved to an extent, because there is no IGMP traffic in the wireless access network.[8]

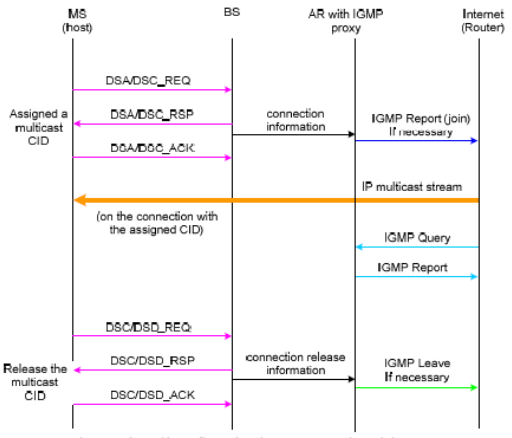


Figure.3. Signaling flow in the proposed architecture

Broadcasting multiple scalable video streams over wireless broadband access networks in real time is a challenging problem, because of the limited channel capacity and variable bit rate of the videos. The difficulty is further increased in the presence of receiver buffer size limitations which may introduce buffer overflow possibilities. The Multicast/Broadcast Service feature of mobile WiMAX network is a promising technology for providing wireless video broadcast services.[9] In this article, we describe a substream selection problem which arises when

Multiple scalable video streams are broadcast based on the Multicast/Broadcast Service feature to a number of buffer size constrained receivers. We first show that the problem is NPComplete and design a polynomial time approximation algorithm based on convex optimization and dynamic programming techniques. We mathematically prove that the solution obtained through our algorithm is always within a constant factor of the optimal solution. Through simulation we show that under real time requirements our algorithm provides solutions which are within 1dB of the optimal solutions.[9]

Video multicasting to mobile devices has emerged as one of the popular services over upcoming next generation wireless networks. Several promising applications like mobile TV, mobile conferencing and mobile multiplayer gaming make use of these services. Technologies from traditional cellular wireless telecommunication networks,[8] terrestrial TV broadcast networks, last mile Internet access networks and other such domains are being proposed for realizing these applications. The IEEE standard 802.16 or WiMAX is a technology which was originally designed for providing last mile wireless broadband access and it is now being considered for providing mobile TV services. For example, Yota Telecom has recently started a TV service with 25 channels over its 10Mbps mobile WiMAX network, and UDCast has announced plans for developing broadcast TV service supporting around 50 channels over mobile WiMAX. Observing this trend we expect to see more deployments of WiMAX based mobile TV services in the near future. Maintaining high quality of service in video delivery is one of the main challenges for these applications. Even though a considerable amount of work has been done to make these deployments a reality, several issues still remain unattended.[10]

Trace packets on individual link Trace file format

event	time	from node	to node	pkt type	pkt size	flags	fid	src addr	dst addr	seq num	pkt id

```
r : receive (at to_node)
+ : enqueue (at queue)              src_addr : node.port (3.0)
- : dequeue (at queue)              dst_addr : node.port (0.0)
d : drop    (at queue)

        r 1.3556 3 2 ack 40 ------- 1 3.0 0.0 15 201
        + 1.3556 2 0 ack 40 ------- 1 3.0 0.0 15 201
        - 1.3556 2 0 ack 40 ------- 1 3.0 0.0 15 201
        r 1.35576 0 2 tcp 1000 ------- 1 0.0 3.0 29 199
        + 1.35576 2 3 tcp 1000 ------- 1 0.0 3.0 29 199
        d 1.35576 2 3 tcp 1000 ------- 1 0.0 3.0 29 199
        + 1.356 1 2 cbr 1000 ------- 2 1.0 3.1 157 207
        - 1.356 1 2 cbr 1000 ------- 2 1.0 3.1 157 207
```

Figure .4. Trace File Format

Video Streaming has address two important problems in multimedia streaming over WiMAX networks: 1) maximizing the video quality and 2) minimizing energy consumption for mobile receivers. In particular, we consider broadcasting multiple scalable video streams to mobile receivers. A scalable video stream is composed of multiple layers, where each layer improves the spatial, temporal, or the visual quality of the rendered video to the user. Because of their flexibility, scalable video streams can efficiently support heterogeneous receivers, adapt to network conditions, and utilize the available wireless bandwidth.[9] We mathematically formulate the problem of selecting the best set of sub streams (or layers) from the scalable video streams in order to maximize the quality for mobile receivers.[10]

IV. CONCLUSION

This project presented a framework for multicasting scalable video streams over mobile WiMAX networks.

We mathematically analyzed the problem of selecting the optimal sub streams of scalable video streams under bandwidth constraints. Solving this problem is important because it enables the network operator to transmit higher quality videos or more number of video streams at the same capacity. The work in this paper can be extended in different directions. For example, we are currently extending our algorithm to consider the probability distribution of hardware profiles of active receivers. The algorithm takes into account the diverse parameters like buffer size, display resolution, and energy consumption profiles such that the produced solution not only optimizes the video quality but also enhances the quality of experience for the majority of mobile subscribers

ACKNOWLEDGMENT

We also express our thanks to our institution, parents, and friends, well wishers for their encouragement and best wishes in the successful completion of this dissertation.

REFERENCES

[1] Mobile Video Services: A Five-Year Global Market Forecast.

[2] Open Mobile Video Coalition website.

[3] Local and Metropolitan Area Networks Part 16: Air Interface for Broadband Wireless Access Systems Broadband Wireless Metropolitan Area Network.

[4] Yota Mobile WiMAX Home Page.

[5] UDCAST WiMAX TV Home Page.

[6] S. Sharangi, R. Krishnamurti, and M. Hefeeda, "Streaming scalable video over WiMAX networks," in Proc. IEEE Workshop Quality of Service (IWQoS'10), Beijing, China, Jun. 2010.

[7] J. Wang, M. Venkatachalam, and Y. Fang, "System architecture and cross-layer optimization of video broadcast over WiMAX," IEEE J. Select. Areas Commun., vol. 25, no. 4, pp. 712–721, May 2007.

[8] R. Cohen, L. Katzir, and R. Rizzi, "On the trade-off between energy and multicast efficiency in 802.16e-like mobile networks," IEEE Trans. Mobile Comput., vol. 7, no. 3, pp. 346–357, Mar. 2008.

[9] P. Hosein, "Broadcasting VBR traffic in a WiMAX network," in Proc. IEEE VTC'08, Calgary, AB, Canada, Sep. 2008, pp. 1–5.

[10] H. Juan, H. Huang, C. Huang, and T. Chiang, "Scalable video streaming over mobile WiMAX," in Proc. Int. Symp. Circuits and Systems, New Orleans, LA, May 2007, pp. 3463–3466.

❑❑❑

Adaptive Rate and Power Control Scheme for CSMA Based Ad hoc Wireless Networks

S. T. Uma & N. M. BalaAmurugan

Computer Science and Engineering, Sri Venkateswara College of Engineering, Chennai, India
E-mail : uma_arunai@yahoo.com & balgan@svce.ac.in

Abstract - Ad hoc wireless networks consists of point to point links distributed randomly in space, carrying out packet transmissions without a centralized control. An SINR based model interference model is considered and if the measured SINR is above a threshold value for the duration of the packet then the packet transmission is successful. CSMA with access control channel which involves the communication of control signals between its own transmitter and receiver improves the performance of conventional CSMA protocol. The proposed work uses the Adaptive Rate and Power Control (ARPC) protocol that bas the ability to control the rate of outgoing traffic from a node and improves the end-to-end throughput. Power Control reduces the energy consumption of nodes and reduces the ene-to-end delay which can improve the performance of CSMA with access control channel.

Keywords*-Ad hoc networks, Adaptive Rate and Power Control, Access Control Channel, CSMA, MAC*

I. INTRODUCTION

An wireless ad hoc network is a network temporarily formed by a collection of mobile stations that does not depend on any established infrastructure. Since mobile stations are battery powered efficient energy management is very critical for wireless ad hoc networks. Mobile units employ omni-directional antennas and each communication channel is shared by closely located mobiles. Sharing the medium and the available resources in a distributed manner are some of the major challenges in the field of wireless communications.

The sharing of channel is controlled by the Medium Access Control (MAC) protocol. Sharing the medium has the adherent problem of interference, which results in erroneous reception of packets. Hence the nodes address the problem of interference through MAC layer design which is an essential source of efficient resource allocation. The networks throughput and efficiency can be determined with the help of this MAC protocol. To further increase the efficiency of networks carrier sense mechanisms can be used requiring the mobile terminal to first sense the channel to determine whether it is idle or busy and then only it attempts its packet transmission. It can also results in collision events when the receiver detects multiple transmissions at power levels and it may not be able to correctly receive them.

Hence the "listen-before-transmit" mechanisms such as CSMA (carrier sense multiple access) does not work well because the channel state might be different at the receiver from what it is estimated at the transmitter. It results in the "Hidden Terminal Problem" where two nodes that do not hear each other transmit packets to common rreceiver ends up with collision at the receiver.

The Distributed Coordination Function (DCF) of IEEE 802.11 is applied in the Medium Access Control (MAC) layer for wireless local area networks.The DCF adopts Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) and retransmission of collided frames are handled with Binary Exponential Backoff (BEB) algorithm. The DCF defines two ways for frame transmiision. The default scheme is a two-way handshaking mechanism called DATA-ACK mechanism. The other is an optional four-way hanshaking mechanism called RTS-CTS-DATA-ACK mechanism which reduces the hidden terminal problem.

A sender-receiver pair exchanges the Request-to-Send and Clear-to-Send (RTS/CTS) signals before frame transmission to reserve the channel. The channel is reserved to avoid the occurence of a collision. After receiving the CTS packet the sender proceeds with frame transmission. The transmission is successful only when it receives the ACK from the receiver. When it does not receive the ACK the sender waits for a random backoff period and again retransmits the packet until it reaches the particular backoff counter value. Otherwise it drops the frame and prepares itself for new transmission.

However IEEE 802.11 has two limitations. First energy used is inefficient because frames are transmitted

with same transmission power without considering the distance between the nodes. Second the spatial reuse of the network is low. When one node is transmitting the other nodes in its physical carrier sensing range is blocked to avoid interference even those transmissions will not interfere with the ongoing transmissions.

II. RELATED WORK

Some of the existing protocols make use of different mechanisms like variable transmission rate and power control protocol with the help of RTS/CTS mechanism Vaidya et al. [2] proposed the Receiver Based Auto Rate (RBAR) protocol where it allows the receiver node to select the rate of transmission. It is done by calculating the SINR of the RTS packet to choose the appropriate transmission rate and communicating that rate to the sender using the CTS packet. This allows much faster Adaptation to the channel conditions compared to Auto Rate Fallback (ARF) but it require changes to the existing IEEE 802.11 standard.

Kanodia et al. [9] proposed the Opportunistic Auto Rate (OAR) protocol which operates using the same receiver based approach. It allows high-rate multi-packet bursts to reduce the overhead at high rates by amortizing the cost of the contention period. OAR changes fairness characteristics from each node by sending an equal number of packets to each node getting an equal allocation of medium time. It results in improved throughput when links of multiple rates operate together in the same space but it require changes the existing IEEE 802.11 standard.

Jia et al. [3] and Ding et al. [1] proposed δ-PCS and DEMAC to improve throughput using a single channel and a single transceiver. These two protocols adjust the transmission power for each packet so that the transmission can be successful and at the same time it will not cause too much interference to other transmissions, but they achieves only limited improvement compared to IEEE 802.11.

Krunz et al. [7] proposed a power controlled dual channel (PCDC) MAC protocol. It indirectly influence the routing decision at the network layer by controlling the power of the broadcasted Route Request (RREQ) packets to produce power efficient routes. It uses the signal strength and the direction of the arrival of the overhead RTS/ CTS packets to build a power efficient topology. PCDC enables simultaneous interference limited transmissions to take place at the receiver by allowing receiver specific computed interference margin.

Muqattash et al. [8] proposed a throughput oriented Medium Access Control with a single channel and single tranceiver called POWMAC. It uses a new decision rule where a node overhears other nodes transmissions and it is allowed its own transmissions as long as it does not interfere with the ongoing transmissions. According to POWMAC several transmissions can happen concurrently but it introduces additional signalling overhead since an ongoing transmissions needs to exchange N (N > 1) more RTS/CTS to enable N concurrent transmissions. Concurrent transmissions may not take place if they are not well synchronized due to propagation delay.

Geng et al. [5] proposed a new adaptive transmission power controlled MAC (ATPMAC) protocol to enhance the network throughput using a single channel and a single transceiver. ATPMAC uses same rule of POWMAC but it does not incur any additional signalling overhead because it needs only one RTS/CTS exchange for N (N > 1) concurrent transmissions. It provides solutions to the synchronization problem so that concurrent data transmissions can happen even though the propagation delay exits. ATPMAC has some limitations like it does not considers nodes mobility and hidden terminal problems still exits.

Li et al. [6] proposed single radio, single channel and multi-rate MAC protocol to improve the spatial reuse of the network. It is enabled by controlling the transmission power so that multiple transmissions can take place without interfering with each other. Hence it is called as Multi-Rate Power Controlled MAC (MRPC-MAC) protocol. It allows new transmissions unless it does not interfere with ongoing transmission. But it has some limitations like it does not address the mobilty issue and does not find an optimal path to maximize end-to-end throughput.

Kaynia et al. [4] proposed a method to improve the performance of wireless ad hoc networks based on the concept of outage probability. When backoffs and retransmissions are not allowed CSMA peforms worse than ALOHA for low densities. This is due to the exposed node problem where the transmitters backoff in situations when their transmissions would not have caused errors for others. By allowing the receiver to sense the channel in CSMA and to inform its transmitter over a separate control channel the peformance is improved. However the performance gain can be improved by increasing the number of backoffs and retransmission attempts.

III. PROPOSED SYSTEM

The proposed work is to evaluate the performance of CSMA protocol with Adaptive Rate and Power Control for CSMA. Conventional CSMA protocol make use of RTS and CTS signals to determine their packet

transmission. Once initiated but received in error at the receiver side then the packet has to be retransmitted. CSMA with access control channel make use control signals to enable the packet transmission. The control signal is a type of packet that is exchanged between its own transmitter and receiver to determine whether or not to initiate the transmission. Adaptive Rate and Power Control protocol based on the signal interference level switches the data rates to mach the channel conditions.

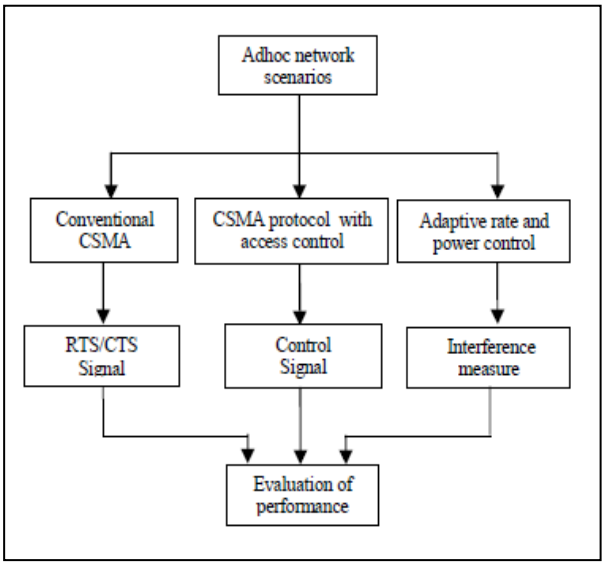


Figure 1. Architecture Diagram

a. Conventional CSMA protocol

The Distributed Coordination Function (DCF) uses the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) mechanism. The RTS and CTS frames contain a Duration field that defines the period of time that the medium is to be reserved to transmit the actual data frame and the returning ACK frame. Thus, collisions occur only on RTS frames and are detected by the absence of a CTS frame.

To control the waiting time before medium access the DCF uses the following parameters called interframe spaces (IFS) namely short interframe space (SIFS), DCF interframe space (DIFS), and extended interframe space (EIFS). The different length of the IFS are defined to provide priority levels for access to the wireless media. SIFS has the shortest waiting time and is given the highest priority for medium access. It is used by short control messages such as ACK and CTS frames. DIFS is a waiting time longer than SIFS and has lower priority for medium access. It is used to transmit data frames by the stations operating DCF. EIFS has the longest waiting time and is used when a transmission failure occurs.

A station that receives an incorrect frame must wait for EIFS before starting its transmission in order to give other stations enough time to acknowledge the frame that the station has received incorrectly. A random backoff process is invoked to reduce the possibility of collision. The random backoff time is calculated as

$$\text{BackoffTime} = \text{random}() \times \text{SlotTime} \quad (1)$$

where random() is a uniformly distributed pseudo-random integer between zero and contention window (CW) and a SlotTime is a PHY-dependent value. Upon receiving a frame the destination station waits for the duration of SIFS and responds with an ACK frame to notify the sender of a successful reception of frames.

b. CSMA protocol with Access Control Channel

CSMA protocol with Access Control Channel make use of control signals to initiate their packet transmission. These control signals are transfered between the own transmitter and receiver. when the channel is idle it transmits the control signal to the receiver that lies within its range. When it receives the response from its own receiver which includes the signal like transmit or not to transmit according to which the transmitter carry out its process. Receiver is the back off decision maker.

Receiver only determines whether or not the packet transmission should be initiated. If the calculated SINR value is above the predefined measured threshold value the packet transmission is initiated otherwise, it is backed off. Each packet is given a maximum number of retransmissions before it is dropped. The communication between the receiver and its transmitter is assumed to occur over a 1 bit control channel.

Hence the delay introduced by the feedback is small compared to packet length.

The main difference between the carrier sense multiple protocol with the access control channel and the popular carrier sense multiple access protocol with collision avoidance used in the IEEE 802.11 and 802.16 standards is that all nodes in the channel that lies within the reception of the transmitter hear the requets-to-send (RTS) and clear-to-send (CTS) signals.

CSMA with access control channel involves the communication of control signals between a receiver and its own transmitter only. Hence the channel usage is efficient and it does not results in wastage of bandwidth which results in improved performance compared to conventional CSMA protocol.

c. Adaptive Rate and Power Control

The importance of spatial reuse in wireless adhoc networks has been long recognized as a key to improving the network capacity. One can increase the

level of spatial reuse by reducing the transmit power. As the transmit power decreases the SINR decreases as a result of the smaller received signal or the increased interference level. Hence the data rate sustained by each transmission may decrease.

The proposed adaptive power and rate control algorithm to enable each node to adjust the transmission power in a way that the frames arrive at receiver guarantees an acceptable signal to interference and noise ratio. The transmit power is so determined that keeps interference effect on the other neighboring concurrent transmissions minimal. Each transmitter finds the maximum signal to interference noise ratio (SINR|max|) that can be achieved at the receiver rx with the transmit power P|tmax|.

If the SINR |max| > SINR|R[i]| then R[i] is the data rate that can be achieved by the transmitter. It sets the transmit power P|t| such that rx can sustain the level of SINR|R[i]|.

$$P|t| = SINR|R[i]| \times I|rx| \times r \quad (2)$$

Where I|rx| is the interference perceived at the receiver and r is the distance between the transmitter and the receiver. Hence the variable tranmission rate can be achieved and performance of wireless networks can be improved.

IV. PERFORMANCE EVALUATION

In this section, we use Network Simulator (NS2) (version2.34) to evaluate the Performance of CSMA protocol. The propagation model used is the two ray ground reflection model. The relationship between transmitted power (Pt) and the received power (Pr) can be represented as

$$Pr = Pt * Gtr \quad (3)$$

Where, Gtr is the gain from the transmitter to the receiver. The table shows the different simulation parameters used to setup the scenario.

Dimension	650m x 650m
Number of nodes	8
Routing Protocol	AODV
Application	CBR
Packet Size	500 bytes
Number of Packets	50
Antenna Model	Omni directional
Medium Access Control	IEEE 802.11

Table 1. Simulation Parameters

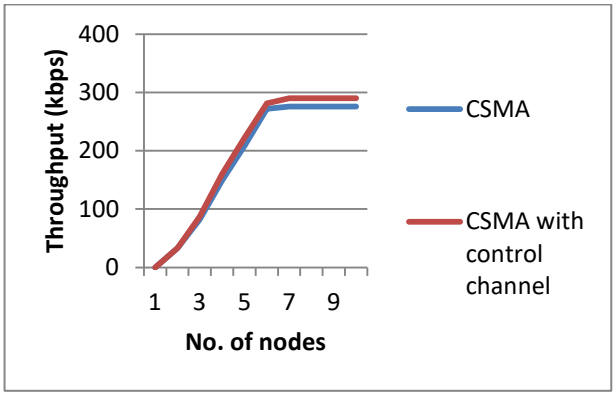


Figure 2. No. Of nodes vs Throughput (kbps)

The figure 2 shows the performance comparison of CSMA protocol with CSMA for access control channel. Here the CSMA protocol with control channel shows the improved throughput when compared to the CSMA protocol.

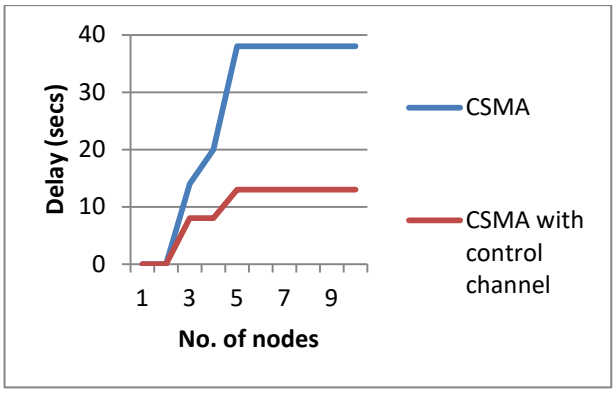


Figure 3. No. Of nodes vs Delay (secs)

The figure 3 shows the Delay introduced by the CSMA with access control channel is very much reduced to the CSMA protocol and hence results in improved performance of wireless networks.

V. CONCLUSION AND FUTURE WORK

Ad hoc wireless networks carry out packet transmissions in the infrastructureless networks. A packet is backed off if the measured or estimated SINR is below the sensing threshold at the beginning of its transmission. CSMA with the access control channel improves the performance of the conventional CSMA protocol. Adaptive Rate and Power Control protocol(ARPC) is proposed which can improve the network performance of CSMA by measuring the interference power. Other possible extensions are to apply different backoff mechanisms to improve the performance of wireless ad hoc networks.

REFERENCES

[1]. P. Ding, J. Holliday, and A. Celik, "Demac: an adaptive power control MAC protocol for ad-hoc networks," IEEE 16th International Symposium on Personal, Indoor and Mobile Radio Communications, vol. 2, pp. 1389-1395, Sept. 2005.

[2]. Gavin Holland, Nitin H. Vaidya, and Paramvir Bahl, "A rate-adaptive MAC protocol for multi-hop wireless networks," International conference on Mobile Computing and Networking, pp. 236-251, 2001.

[3]. L. Jia, X. Liu, G. Noubir, and R. Rajaraman, "Transmission power control for ad hoc wireless networks: throughput, energy and fairness," IEEE Wireless Communications and Networking Conference, vol. 1, pp. 619-625, Mar. 2005.

[4]. M. Kaynia, N. Jindal, and G. Oien, "Improving the performance of wireless ad hoc networks through mac layer design," IEEE Transactions on Wireless Communications, vol. 10, no. 1, pp. 240-252, 2011.

[5]. P. Li, X. Geng, and Y. Fang, "An adaptive power controlled MAC protocol for wireless ad hoc networks," IEEE Transactions on Wireless Communications, vol. 8, no. 1, pp. 226-233, January 2009.

[6]. P. Li, Q. Shen, Y. Fang, and H. Zhang, "Power Controlled Network Protocols for Multi-Rate Ad Hoc Networks," IEEE Transactions on Wireless Communications, vol. 8, no. 4, pp. 2142-2149, April 2009.

[7]. Muqattash and M. Krunz, "Power controlled dual channel (PCDC) medium access protocol for wireless ad hoc networks," IEEE International Conference on Computer and Communication, vol. 1,pp. 470-480, Mar. 2003.

[8]. Muqattash and M. Krunz, "Powmac: a single-channel power-control protocol for throughput enhancement in wireless ad hoc networks," IEEE Journal on Selected Areas in Communications, vol. 23, no. 5, pp. 1067-1084, May 2005.

[9]. Sadeghi, V. Kanodia, A. Sabharwal, and E. Knightly, "Opportunistic media access for multirate ad hoc networks," International conference on Mobile computing and Networking, pp. 24-35, September 2002.

❑❑❑

Traffic Scheduling For Clusters Using Weighted Round Robin Scheduling Scheme in Wireless Networks

P. Priyadarshini & R. Ramachandran
Computer Science and Engineering Sri Venkateswara College of Engineering Chennai, India
E-Mail : priyadarshinip.cse @gmail.com

Abstract - Scheduling of traffic plays a key role in wireless networks. Scheduling defines how the channel is shared between users in the network. By selecting proper scheduling scheme the network throughput can be improved and resource is allocated without any starvation. The main objective of this paper is to find an efficient strategy to improve channel throughput and allocate resource in an efficient manner for the cluster of systems. The use of clusters reduces the network traffic by minimizing the number of message exchanges. Recent scheduling schemes use OFDMA for resource allocation. It provides multiple user access. In this paper we used an algorithm called Weighted Round Robin Scheduling algorithm (WRR) for scheduling. The algorithm computes the weights based on the movement of packets between the nodes. The performance of the algorithm is compared when applied to the individual Mobile Stations and for the cluster.

Keywords*-Resource Allocation,orthogonal frequency division multiple access(OFDMA).*

I. INTRODUCTION

New inventions of broadband wireless access standards, such as IEEE802.16, deploy orthogonal frequency division multiple access (OFDMA) mechanism to improve quality of service provisioning and to overcome fading channel impairments. Resource scheduling in OFDMA networks employs different quality of service (Qos) provisioning, efficient utilization of limited resources available at the Base Station (BS), and maintaining fairness among users. OFDMA is multiple user version of OFDM, provides multiple user access. Orthogonal Frequency Division Multiplexing (OFDM) is a technique for transmitting large amounts of digital data over a radio wave. The technology functions by splitting up the radio signal into multiple smaller sub-signals and are transmitted simultaneously at different frequencies to the receiver. OFDM minimizes the amount of crosstalk in signal transmissions.

For wire line systems, the physical medium is in general regarded as stable and robust. Thus the packet error rate (PER) is usually ignored and can be simply considered as a constant with unit bits/sec. This kind of model is usually referred as error free channel. On the other hands, for wireless systems, the situation can become much more complicate. Whether in wireless networks with short transmission range (about tens of meters) such as WLAN and femto cell or that with long transmission range (about hundreds of meters or even several kilometers) such as the macro cell environments based on WCDMA, WiMAX and LTE, the packet transmission in wireless medium suffers location-dependent path loss, shadowing, and fading. These impairment make the PER be no longer ignorable and the link capacity *C* may also become varying. This kind of model is usually referred as error-prone channel.

Wireless Networks have unique characteristics, and demand specially designed scheduling schemes. The wireless resource is limited, and the mobile users experience time-varying channel conditions. Wireless networks have distinguishing characteristics when compared to wire line networks like topology dependence, interference, time –varying channels and limited resources. This results in demand for designing highly efficient resource utilization for wireless networks. Good scheduling schemes should exploit channel conditions to achieve higher network performance.

The IEEE 802.16 architecture consists of single Base Station (BS) and one or more Mobile Station (MS). Base Station acts as a central component and transfer all the data in a PMP (Point to Multipoint) mode from MSs. Uplink Channel is shared between all MSs and the Downlink Channel is only used by the BS. The standard defines both Time Division Duplexing (TDD) and Frequency Division Multiplexing (FDD) for channel allocation. The standard supports five flow classes for QoS and the MAC supports a request-grant mechanism for data transmission in uplink transmission. The advantages of this technique are small inter-symbol

interference (ISI), better capacity than older Time Division Multiple Access (TDMA) and Code Division Multiple Access (CDMA).

The main objective of the scheduling algorithm is to reduce the computation time at the same time to maximize the utilization of the network resource and thus improving the system throughput. While considering a single flow a MS request the BS for bandwidth, for uplink. BS grants the total bandwidth for all connections, belonging to that MS. The MS then redistributes the sum-total of the grant among its users according to the service class of the user's connections and its QoS requirements. Allocation need to be done in a manner so that each user can get access to the required resource.

II. RELATED WORK

Many scheduling algorithms exist in order to manage the resource availability and allocate without causing starvation.

Knightly.E, et.al [3] proposed Opportunistic Fair Scheduling over Multiple Wireless Channels. Using a realistic channel model, any subset of users can be selected for data transmission at any time, with different throughput requirements and system resource requirements. The best users and rates have been selected from a complex general optimization problem, and is transformed into a decoupled and tractable formulation: a multiuser scheduling problem that maximizes total system throughput and a control update problem that ensures long term deterministic or probabilistic fairness constraints. However, minimizing the average job delay and developing on-line algorithms that approximate the optimal solution with bounded error are not applicable because the multi-channel wireless scheduling problem has a unique formulation such as constraints of fairness among users.

Chong, et.al [4] proposed a Framework for Opportunistic scheduling in Wireless Networks presents a method, called opportunistic scheduling, for exploiting the time-varying nature of radio environment to increase the overall performance of the system under certain Qos/fairness requirements of users. Improve wireless resource efficiently by exploiting time-varying channel conditions while at the same time controlling the level of QoS among users. But the paper does not handle other requirements, such as short-term and delay requirements.

Cheng, et.al [1] proposed an Optimization Framework for Balancing Throughput and Fairness in Wireless Networks with QoS support. In general ith limited radio resources, increasing system throughput and maintaining fairness are conflicting performance metrics, leading to a natural tradeoff between these two measures. Balancing system throughput and fairness is desired. Interference-limited wireless network is considered and generic optimization framework is derived to obtain an optimal relationship of system throughput and fairness with QoS support and efficient resource utilization, by introducing the bargaining floor. In addition, the framework facilitates call admission control to effectively guarantee QoS of multimedia traffic. Different degrees of performance tradeoff between system throughput and fairness can be achieved, by suitably adjusting the value of the bargaining floor. QoS support is assured.

Cioffi, et.al [5] proposed Optimal Resource Allocation for OFDMA downlink systems. Efficient rate and power allocation algorithms for OFDMA downlink systems where each tone is taken by maximum of one user. Weighted sum rate maximization (WSRmax) and Weighted sum power minimization (WSPmin) problems are considered. The paper employs the Lagrange dual decomposition method to efficiently solve both optimization problems. These are originally non-convex problems with exponential complexity; the duality gap has been shown to vanish when the number of tones increases. Lagrange dual decomposition method is employed to efficiently solve both problems.

Dianiti, et.al [2] proposed Cooperative Fair Scheduling for the Downlink of CDMA Cellular Networks. The paper deals with the cooperation among the adjacent Base Stations (BSs) for downlink scheduling in code division multiple access cellular networks have been studied. Cooperative utility fair scheduling has been proposed to increase multiuser diversity gain and reduce interference among BSs. The scheduler maintains fairness and smooth service delivery by balancing the long-term average throughput of users. Cooperative fair scheduling is proposed with an opportunistic service discipline as the core for the downlink of CDMA cellular networks. In order to maintain long-term fairness and smooth service delivery a fairness enforcement mechanism is also integrated.

Optimal power allocation among the SAs also reduces interference from the adjacent BSs, thus improving the total system throughput. Performance improvement is remarkable for the users located near the cell boundaries where the interference among the adjacent BSs is high.

Chong, et.al [8] proposed Opportunistic Scheduling for OFDM systems with Fairness Constraints. Opportunistic scheduling exploits the time-varying, location-dependent channel conditions to achieve multiuser diversity. Multiuser OFDM allows multiple users to transmit simultaneously over multiple channels. A rigorous framework is developed to study opportunistic scheduling in multiuser OFDM system.

Optimal opportunistic scheduling policies has been derived under three Qos /fairness constraints for multiuser OFDM systems- temporal fairness, utilitarian fairness, and minimum performance guarantees. The scheduler not only decides which time slot, but also which subcarrier to allocate to each user.

Qiu, et al [7] proposed Subcarrier allocation algorithm for utility proportional fairness in OFDM systems. The paper focuses the problem of subcarrier allocation to multiple users, downlink OFDM access system was considered. So allocation schemes that provide varying degrees of tradeoff between has been studied (i) achieving throughput fairness among users, (ii) meeting tolerable latency requirements specified by the user applications, and (iii) achieving higher system capacity.

The implantation works do not consider the multiple antenna systems.

III. PROBLEM FORMULATION

The main problem addressed in this paper is formulated as follows: The proposed scheduling algorithm allocates the required data for the cluster of system. Given a network, numbers of users are grouped together to form a cluster in order to reduce the number of transmissions and also the energy needed for the communication. The performance of the algorithm between the individual systems and the clusters are compared.

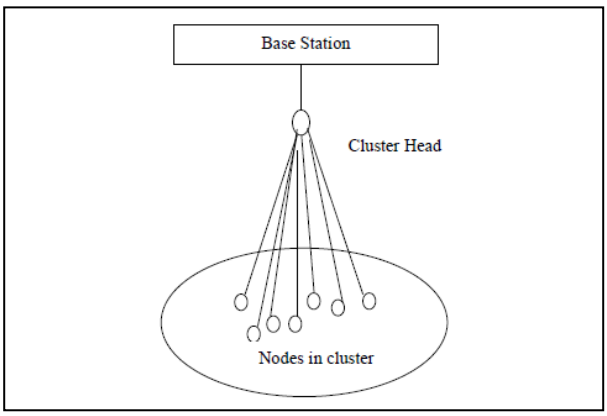
IV. PROPOSED SYSTEM

Wireless networks have unique characteristic like time varying channel conditions, interference and mobility of nodes and thus require some specially designed scheduling schemes.

Scheduling plays an important role in wireless systems and has been used in High Data Rate technology. Scheduling is the allocation and management of resource according to demand from the users. Performance improvement can be achieved by allocating the resource to the cluster of systems. In a network number of nodes can be grouped together to form the cluster.

A. *Resource Allocation*

In OFDMA, users share subcarriers and the time slots, this provides increased multiuser diversity, and the users are allowed to do allocation in an efficient manner. OFDMA is a combination of FDMA and TDMA: in different time slots (TDMA) users are dynamically assigned subcarriers (FDMA).



OFDMA provides the same advantage of robust multipath suppression and frequency diversity as single user OFDM and in addition it gives flexible multiple access, can accommodate many users with wide variety of applications, data rates and QoS requirements. Multiple accesses is performed in the digital domain so the bandwidth can be allocated dynamically and efficiently. Hence sophisticated time and frequency domain scheduling algorithms can be integrated in order to best serve the user population. OFDMA allows the same data rate to be sent over a longer period of time using same total power.

The users request for a resource whether it can be multimedia data or text data, Base Station should provide the requested information to the requested nodes without making them to wait. In order to process the request and to allocate, scheduling needs to be done. Scheduling determines which user can be allocated first and which users can be allotted next. Network throughput can be maximized by means of scheduling and channel utilization can be achieved.

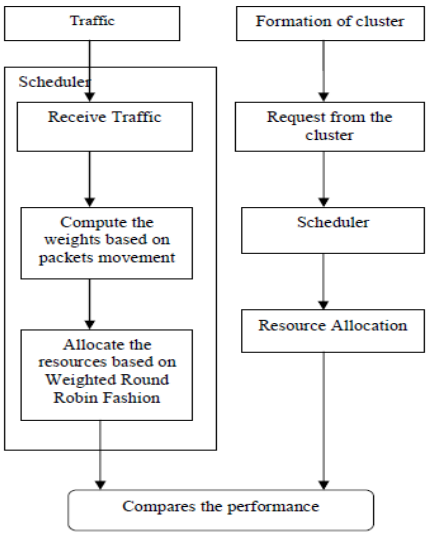


Figure 2.Architecture of Proposed Work

B. *Scheduling*

In a network number of Mobile Stations exist and communicates with the Base Station. It is responsible for all kinds of services and provides the requested data. The request sent by the user is processed by the Access Point. The Mobile Station cannot be able to communicate directly with the Base Station. Hence Access Point acts as interface and receives the request from Mobile Station and process the request and forwards the request to the server. The Base Station then allocates the required data and the Access Point.

The weights can be computed based on the link weights between the nodes. It is calculated based on the number of packets transmitted between two nodes. If there exists nodes with huge number of packet transmitted among them then the link between them has the higher priority and allocated first after that the next higher link weight nodes can be allocated in a round robin fashion. Since it is handled in round robin fashion each node have equal chance of resource allocation and starvation can be avoided. OFDMA defines five types of service flows: Best Effort (BE), Unsolicited Grant Services (UGS), Real Time Polling services (rtps), Non Real Time Polling Services (nrtps), Extended Real Time Polling services (ertps).

The Table 1 gives the simulation parameters used to set up the network scenario:

TABLE 1. SIMULATION PARAMETERS

Parameter	***Value***
Simulator	NS-2(version2.31)
Simulation Time	30s
No. of nodes	9
Traffic model	CBR
Packet Size	500 bytes
Routing Protocol	AODV

The graph given below gives the throughput for different traffic services in Weighted Round Robin Scheduler.

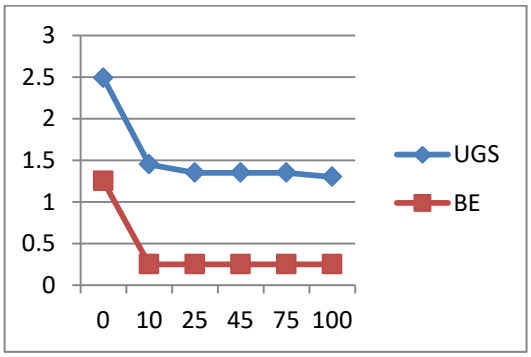


Figure3. Throughput of WRR Scheduler under UGS and BE flow of service

C. *Clustering*

The use of clusters reduces the communication overhead and also reduces the number of packets transmitted during the transmission. The cluster head can be chosen and the entire request for the resource can be sent through that head to the Base Station. Since cluster head alone taking part in transmission in place of its member nodes the number of transmissions are reduced. Hence energy consumed may get reduced. Clusters are formed based on the distance. The node which at one hop distance from the Base Station acts as cluster head and the nodes that is reached from the cluster head become the member of that cluster. Minimum two nodes is required to form cluster and maximum five nodes can be allowed in a cluster. The number of clusters depends on the network size.

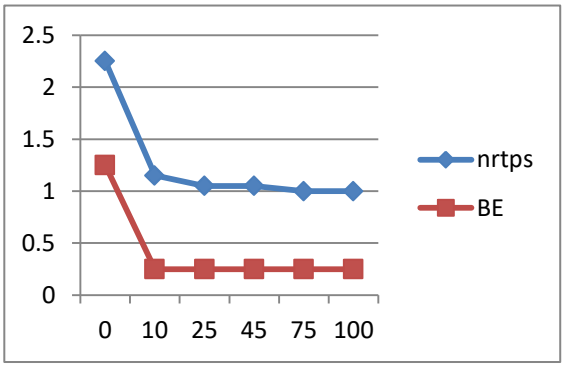


Figure4.Throughput of WRR Scheduler under nrtps and BE flow of service

Clustering reduces the number of nodes taking part in the transmission, the cluster head communicates with the Station and allocates to nodes within the cluster. The cluster head can also communicate with each other. When nodes move out from the coverage area or come inside the coverage area, and if the network size increases the topology information get updated in cluster head. As the rate of network topology changes increases, the exchange of routing tables between neighboring nodes must be more frequent to keep routing information up to date. The energy consumed by the nodes is minimized.

V. CONCLUSION AND FUTURE WORK

Scheduling schemes in wireless networks are used for allocating resources and to manage the traffic movement in the network. This action improves the network utilization and the throughput can be increased. When individual Mobile Stations communicate with Base Station then the network traffic will be high. Number of stations can be grouped together to form the

cluster. Cluster head alone takes part in the transmission instead of all its nodes. The future work involves finding an algorithm that considers the channel status and allocates channel to the cluster of systems without making them to wait for a long period of time.

REFERENCES

[1] Cheng.H.T and Zhuang.W, "An optimization framework for balancing throughput and fairness in wireless networks with QoS support," in Proc.3rd International Conf. Quality Service Heterogeneous Wired/Wireless Netw. (QShini'06), Waterloo, Ontario, Canada, 2006.

[2] Dianiti.M, Shen.X and Naik.K, "Cooperative fair scheduling for the downlink of CDMA cellular networks" IEEE Trans. Veh. Technol., vol. 56, no. 4, pp. 1749-1760, 2007.

[3] Liu.Y and knightly.E, "Opportunistic fair scheduling over multiple wireless channels", in Proc. IEEE International Conf. Comput. Commun. (INFOCOM'03), San Francisco, USA, Apr.2003.

[4] Liu.X, Chong, and Shroff.N.B, "A framework for opportunistic scheduling in wireless networks", 2003.

[5] Seong.K, Mohseni.M, and Cioffi, "Optimal resource allocation for OFDMA downlink systems", in Proc. IEEE International Symp. Inf. Theory (ISIT'06), Seattle, USA, July 2006.

[6] Xuemin, Mehri Mehrjoo, "Design of Fair weights for Heterogeneous Traffic Scheduling in Multichannel Wireless Networks", IEEE transactions on communications, vol.58, no.10, October 2010.

[7] Zhang.T, Zeng.Z, and Qiu, "A subcarrier allocation algorithm for utility proportional fairness in OFDM systems", in Proc. IEEE veh. Technol. Conf. (VTC'8), 2008, pp. 1901-1905.

[8] Zhang.Z, He.Z, "Opportunistic scheduling for OFDM systems with fairness constraints", EURASIP J. Wireless Commun. Netw. Vol.8, no.3, pp.275-277, 2008.

[9] D. M. Chiu and A. S. Tam, "Fairness of traffic controls for inelastic flows in the Internet," *Comput. Netw.*, vol. 51, no. 11, pp. 2938-2957,2007

❑❑❑

Power Adaption Routing Protocol For Realtime Applications In Wireless Sensor Networks Using Robust Nodes

R. Prema & R.Rangarajan

Department of Electronics, Karpagam University, Coimbatore, India &
VSB Engineering College, Coimbatore, India
E-Mail : prema_sibi@yahoo.com, profrr@gmail.com

Abstract : One of the most important and challenging issues in real-time applications of resource-constrained wireless sensor networks (WSNs) is providing end-to-end delay requirement. Many wireless sensor network (WSN) applications require real-time communication. In order to address this challenge, we propose the Power Aware Routing Protocol, which attains application-specified communication delays at low energy cost by dynamically adapting transmission power and routing decisions. Extensive simulation results prove that the proposed Protocol attains better QoS and reduced power consumption.

Keywords*: WSN, Robust nodes, link Quality.*

I. INTRODUCTION

Smart environments represent the next evolutionary development step in building, utilities, industrial, home, shipboard, and transportation systems automation. Like any sentient organism, the smart environment relies first and foremost on sensory data from the real world.Sensory data comes from multiple sensors of different modalities in distributed locations. The smart environment needs information about its surroundings as well as about its internal workings; this is captured in biological systems by the distinction between exteroceptors and proprioceptors.

Wireless sensor networks (WSN) represent a new generation of embedded systems for routing sensory data from the originator sensor node to the control station [1]. Recent technological advances have enabled the development of tiny battery-operated sensors [2]. Although energy efficiency is usually the primary concern in WSNs, the requirement of low latency communication is getting more and more important in new applications. For example, a surveillance system needs to alert authorities of an intruder within a few seconds of detection. Supporting real-time communication in WSNs is very challenging. First, WSNs have lossy links that are greatly affected by environmental factors [3] [4]. As a result, communication delays are highly unpredictable. Second, many WSN applications (e.g., border surveillance) must operate for months without wired power supplies. Therefore, WSNs must meet the delay requirements at minimum energy cost. Third, different packets may have different delay requirements.

II. PROPOSED WORK

Among all the sensor nodes in the network, there are some robust nodes. These robust nodes serve as the backbone for the routing in wireless sensor networks. The remaining sensor nodes are common sensor nodes. Each robust node maintains a table of sensor node power at other robust nodes. So in the route, each robust node will compute the end-to-end power from itself to any other robust nodes. The sensor node power is estimated and updated periodically by each robust node. The robust node which is nearest to the source node finds the robust nodes which are along the route towards destination sensor node. Then packets will be forwarded through these robust nodes to the destination node. Since robust nodes have better communication capability than common nodes, most of the time the power is less than the maximum power. This protocol is compared with AODV protocol. This protocol shows better power adaption than AODV protocol.

A. Estimation of Link Quality

The communication in mobile ad-hoc network is based on electronic signals. In mobile ad-hoc networks it is possible that a communication path (route) will break. This will happen primarily because of the nodes present in the network are moving around the region. The fig.1, depicts the scenario when the link is active. In the fig.1, three nodes are present namely a, b and c. The node-b is within the range of the node-a and node-c. But, the node-a is not within the range of node-c and

node-c is not within the range of node-a. Hence for transmission of data from node-a to node-c, the node-b acts as an intermediate node. After certain duration, due to the mobility of sensor nodes, the link gets break and the data communication between the nodes becomes unreliable.

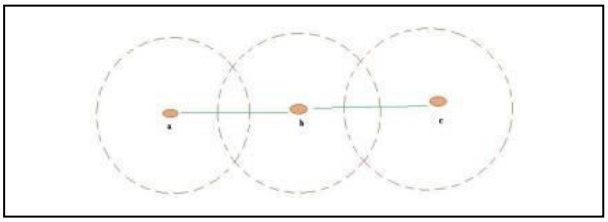


Fig.1 Before the link breaks

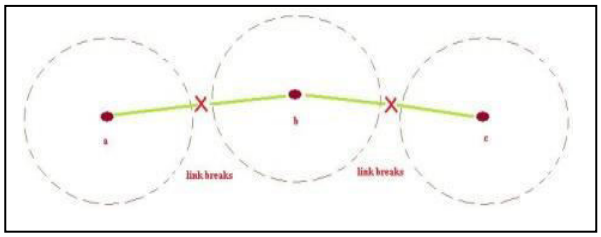


Fig.2 After the link breaks

Due to the mobility of nodes present in wireless sensor network it becomes mandatory to consider the quality of the link.

To be able to see that when a node in the wireless sensor network is moving and hence a route is about to break. So that factor, it is probable to measure the quality of the signal and based upon that presumption, when the link is going to break. This information which is identified by the physical layer is send to the upper layer when packets are received from a node, and then indicate that node is in pre-emptive zone. Pre-emptive zone is the region where the signal strength is weaker which leads to the link failure. Pre-emptive zone uses the pre-emptive threshold value to fix the pr-emptive zone's location. Thus, using the received signal strength from physical layer, the quality of the link is predicted and then the links which are having low signal strength will be discarded from the route selection.

When a sending node broadcasts RTS packet, it piggybacks its transmission power. While receiving the RTS packet, the projected node quantifies the strength of the signal received.

$$L_q = P_R$$

Where,

P_R refers Power of the Receiving node,

P_T stands for Power of the Transmitting node,

λ stands for wavelength carrier,

d is the distance between the sending and the receiving node,

UG_R stands for unity gain of receiving omni-directional antenna

UG_T stands for unity gain of transmitting omni-directional antenna.

$$T_{POW} = \max (L_q \& R_{POW})$$

Where,

CV = Cost Value,

L_q = Link quality

R_{POW} = Residual Power of the sensor node

B. Election of Robust node

At the start, one robust node is set in each grid. We need an election mechanism to produce new Robust nodes because robust nodes also move around. When a Robust node leaves its current grid or due to any other reason there is no robust node in the grid. Suppose, there are more Robust nodes in the current grid of the network, then, the next node with maximum weighted value from the sorted list will be chosen as the new Robust node for the grid. In the proposed routing algorithm, we need to compute the minimum delay between two robust nodes, and find the path with the minimum delay.

For each valid path Pi,

For every node nk in Pi

t_power = t_power + power (nL, nk) + power (nk)

If t_power >= max_power, delete this path, break.

If t_power >= min_power, delete this path, break.

If nk is the destination D, and t_power < min_power,

min_power = t_power;

best_path = Pi + {nk};

Else add node nk to the end of the path,

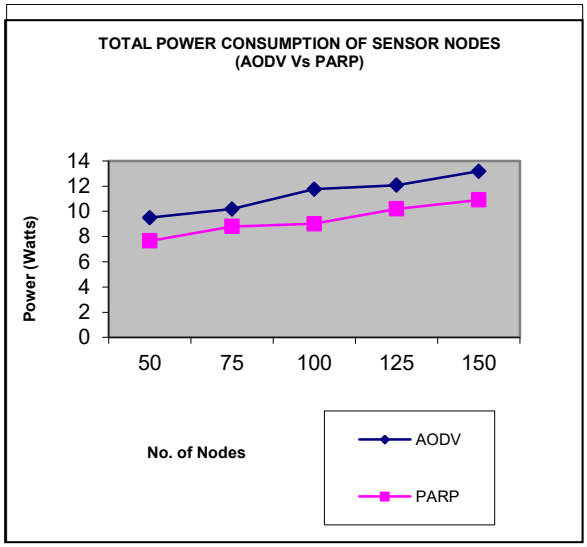
End For

End For

Pseudo code for Robust Sensor node election

C. Simulation Settings & Graphs

No. of Nodes	50, 75, 100, 125 and 150
Area Size	1000 X 1000
Mac	802.11
Radio Range	250m
Simulation Time	50 sec
Traffic Source	CBR
Packet Size	512 KB
Mobility Model	Random Way Point
Speed	5 m/s
Pause time	100 Seconds



Pausetime Vs Power Consumption

III. CONCLUSION

This paper addresses the issue of power adaption and QoS effective routing by design and development of Power Adaption Routing Protocol (PARP). Also, scalability issue is kept in mind when the number of nodes in the network is increased from the range of 50 to 150 nodes. The total power consumption, delivery ratio and delay are taken as the performance metrics and the simulation results proved PARP is better than AODV protocol.

REFERENCES

[1] I.F. Akyildiz et al., "Wireless Sensor Networks: A Survey", Journal of Computer Networks, 38 (2002), 393-422, March 2002.

[2] D. Estrin, et al., "Next Century Challenges: Scalable Coordination in Sensor Networks," Proc. of the 5th Annual Conference on Mobile Computing and Networks (MobiCOM'99), Seattle, WA, August 1999.

[3] J. Zhao and R. Govindan "Understanding packet delivery performance in dense wireless sensor networks," in SenSys 03, 2003, pp. 1–13.

[4] A. Cerpa, J. Wong, L. Kuang, M. Potkonjak, and D. Estrin, "Statistical model of lossy links in wireless sensor networks," in IPSN '05, 2005

❑❑❑

Web Intrusion And Anomaly Detection Based On Data Clustering And ADAM

K. Indumathi, R Sylviya & M.Vanitha

Department of Networking, Sri manakula vinayagar engineering college, Puducherry, India
E-mail : indumathy2610@gmail.com , sylviya1618@gmail.com, vanithavani14@yahoo.com

Abstract - The internet services has increased so drastically now a days that it has become almost impossible to work without it . Web is one of the internet service used round the globe .As a result of which the web servers and web based applications have become the targets of the attacker. So the web based security cannot be ignored where there is drastic increase in web based economy. These protection of such servers has become mandatory. We have proposed two phases for detection of intrusion and anomalies from the HTTP request and defending them. The intrusions and the anomalies are found with the mechanism of clustering and the feature matrix . The first approach has two phases. The first phase has web layer log file matching and the second phase is based on value of packet arrival factor (af) of HTTP request followed by clustering. The defending of the HTTP attack is necessary because the spammers tend to flood the HTTP request at port 80 or port 443 and cause denial of service at web server. The anomaly detection is done by either small scale or artificially generated attacks data. The log files are taken into account and the security analysis is applied on it. This promotes careful, balanced and coordinated scrutiny of several aspects of data in a featured matrix. To assist this, an interactive and easy to use tool named ADAM is used. This is followed by the visualization of the intrusions and blocking of it.

Keywords - *web intrusions, web layer log files, HTTP requests, data clustering, attack labeling, ADAM*

I. INTRODUCTION

The servers that are accessed now a days at such a higher rate are unfortunately visited by the intruders and hackers to fulfill their illegal desire to exploit the confidentiality of websites and the databases. They try to attack the infrastructure of the internet inorder to disturb its functionality by taking the advantage of the internet services and protocols. The attacks that they make are denial of service attacks(DOS),SQL injection attack, e-mail spams and web services are the top threat that are to be recognized. These attacks cannot be underestimated as the web servers and the applications are to be preserved safely with high reliability, efficiency and confidentiality. In our proposed approach the intrusions and anomalies are detected using two phases. The first phase has web host based intrusion detection by matching the input features of web layer log file. The access logs and the error logs are taken into account from web server and they are matched with input features. The second phase has packet arrival factor. In the next approach suspected requests are automated and visualized using ADAM. This enables clear and easy study. Rest of the paper is organized as follows: In section 2, the related work and observations is given. In section 3, the background of our proposed scheme is given. In section 4, the proposed approach of ellipse fitting mechanism is given. In section 5, we have concluded with future work. Rest of paper is organized as follows. In section2, we have presented related work and observations. In section3, we have given background of our proposed scheme. In section 4, algorithm and the technique has been produced. In section 5, we concluded with future work.

II. RELATED WORKS

Once an attack is being detected, based on supervised clustering technique, the system administrator is informed and can take the corrective measure[7]. Authors developed anomaly-based system that learns the profiles of the normal database access performed by web-based applications[3]using number of different models. In [1] a detection system correlates the server-side programs referenced by client queries with the parameters contained in these queries. The system analyzes HTTP requests and builds data model based on the attribute length of requests, attribute character distribution, structural inference and attribute order. In [5] logs of web server are analyzed to look for security violations. However the specific available information has been taken into account which is not portable. Based on our limited survey, following observations have been made:

- Detection of SQL injection attack and HTTP buffer overflow attacks are challenging issues
- Possibility of attack due to poor and careless web application coding by programmers

There have been several attempts to detect anomalous and suspicious activities in web requests. Snot [9],widely used open-source tool, has more than 1,300 signatures on known attacks stored in more than 50 rule sets. However, not all the rules remain effective in typical web server configurations. When applied to IIS web servers, for example, only about 11% of the rules are applicable. More importantly, unless web attacks are analyzed and attack patterns coded as rules, Snort is essentially useless in defecting servers from the threat of unknown attacks.

Kruegel[2] investigated how anomaly detection technique can be applied on web logs. For example, Kruegel developed anomaly detection models based on features such as attribute length, character distribution, or absence of attribute variables and their sequences. While various features can be assigned different weights to optimize performance, it is difficult to determine the "right" parameter values. As operation heavily relies on heuriatics, simple computation (eg., average of anomaly scores) may not detect sophisticated attacks.

Session anomaly detection(SAD), developed by Cho et al.[8],divides a sequence of web requests into sessions. Session characteristics(eq., page sequences) are compared against those of previous sessions intiated by the same IP, and anomaly score is computed based on assumption sessions would exhibit similar patterns. While probably true in static IP environment, such assumption may not hold in environments such as Web Proxy or Network Address Translation(NAT) is used. In addition, accurate identification of web sessions may prove difficult in some environments.

III. PROPOSED APPROACH

According to a study the most frequently attacked web site in the world is united state's department of defense and the second most frequently attacked server is Microsoft 's web server. In such a condition the security to prevent such attacks is mandatory and hence we have generated some web layer logs and these are examined by producing clusters for representative samples of anomalies logs. The clusters are matched with the standardized features of the anomalies and intrusion. It is then represented in the feature matrix and automated using ADAM (anomaly feature matrix). The attacks may be HTTP attacks and SQL injection. The HTTP attacks uses HTTP port 80 or HTTP communication port 443 to perform attacks. It is activated by spammers with flooding HTTP request at particular ports which cause denial of service at server. The SQL injection attack is conducted by spammer for unauthorized web service access breaking the authentication seal and violating integrity of the data storage. It mostly happens in a poor quality code written in PHP.

We have proposed two techniques for such intrusion and anomaly detection. The first technique has two phases. The first phase is based on web layer log file matching and the second phase has value of packet arrival factor (af) of the requests that are clustered and labeled if they are normal or abnormal. The matching of the web layer log files is done by analyzing the characteristics of each and every request so as to produce the intrusion and anomalies in the log and blocking it. The analysis is automated using ADAM.

IV. ALGORITHM AND TECHNIQUES

The concept of intrusion and anomaly detection has been organized into two approaches where the mechanism such as matching the data logs then formation of data clusters and representation of it in the features matrix has been done.

The matching algorithm is as follows.

Let input rows of string values P and web layer's log text file T be embedded with some alphabet § and let P Є§m×m′, T€§n×n′, where m and n are number of rows and columns respectively and n ≥ m and m′ = n′. A two-dimensional character matching problem is yo locate input rows of P as a sub-set of rows of P in T is said to be exact, if relation P is included in relation T as a sub-relation such as P U T → T, and is defined as approximate, if for some tuples X of relation T, the 2D-dist(P,X) id minimal or 2D-dist(P,X) ≤ k. (2D-dist(P,X) ≤ k. (2D-dist [3] is a function defining a two-dimensional distance between two relations.)

2D approximate string matching using 2D edit distance k, k Є N0 means to find all attribute value occurrences of P in T with equal or less than K errors. Let rowi(a) denotes the ith -row of relation a and col i (a) denotes the ith –columns of a. Given two rows of string values with same number of attributes,their KS 2D-distance[3] is the sum of the edit distances of the corresponding rows or columns. The KS edit distance is being computed using columns between P and T can be described by the formula given below:

$$H(T,P)=\{H(T1,P1,)+H(T2,P2)+\ldots+H(Tn,Pn)\}$$
$$n'$$

$$H(Ti,Pi)= edL(coli(T),coli(P))$$

In case of web layer log file matching if it has been found that the approximate edit distance of input P is more than the input threshold K then attack is being

detected. In such type of attack, a temporary role has been generate to restrict the user in updating the database. In case of attack detection based on value of af, the formation of clusters and labeling the attack clusters has been done. Corresponding packets with respect to the attack clusters has been blocked in such case.

Algorithm for attack detection on web log file matching:

INPUT: Web layer log text T; input feature text P;

OUTPUT: Unmatched text M(Φ),u_match_count;

a .[i] Let T be expressed as T={T1,T2,…Tn}, where {T1,T2,…Tn} are the set of rows and each Ti={s1,s2,…sn},where each si is a string of characters.;

[ii]Let the input P be expressed as P={P1,P2,…Pn}, where each row Pi={s'1,s' 2,…s' n},;

[iii] Initialize: matched_row,M(Π)= ϕ;
Matched_ count=0;
Unmatched_row,M(ϕ);
u_match_count=0;

b. for i=1 to m do{ /*m←number of rows inP*/

c. for j=1 to n do{ /*n←number of rows in T*/

d. if(Pi==Tj)then{
match_count=match_count+I;
M(Π)=M(Π)+Tj;}}

e. if(match_count==0)then
M(ϕ)=M(ϕ)+Pi;
u_match_count= u_match_count +1;

f. match_count=0;}

Approximate matching:

INPUT: M(ϕ),T,u_match_count,€

OUTPUT: aprox_match_count,attack_alarm

a. For i=1 to u_match_count do{
b. For i'=1 to n do { /*for all rows in T do */
c. For j=1 to n' do {
d. Len=str_len(s'k); /* s'k ←kth string of **i**th unmatched rows of M(ϕ)*/
e. Um[]=ϕ;
f. For q=1 to len do {
g. c =getchar(sk),c'=getchar(s'1);
h. if(c≠c') then {
[i] c = c'; /* s'k ←kth string of **i**th row of M(ϕ)*/
[j] Um[j]←Um[j]+1;}}}
i. HeD[i']←MIN(Um[j])/*HeD[i']←edit distance of **i**th row of M(ϕ)*/
j. if((HeD[i']) ≤ €)then aprox_match_count←approx_match_count+1;
k. if(aprox_match_count<u_match_count)then generic attack alarm;

Attack detection:

INPUT: Threshold δ ;

OUTPUT: Attack alarm;

[a] compare the value of arrival factor(af) of incoming http service request for some instances I=(I1,I2,……In).

[b] Generate attack alarm if value of af> δ .

[c] Stop.

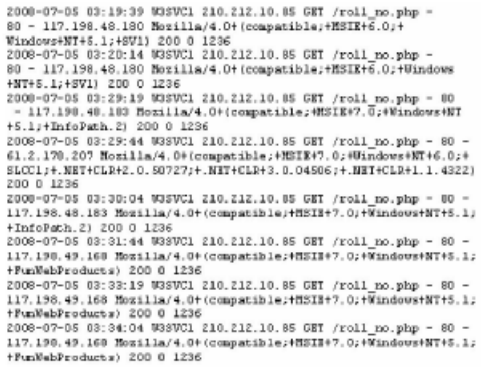
The detection of alarm is done on the base of the threshold value of the arrival factor. The instances of the input requests are analyzed and if the arrival factor is greater than the threshold value then attack is generated.

The mechanism for the intrusion and detection rate of the incoming requests would be represented as follows

TABLE I: DETECTION RATE OF SECOND PHASE

Sample dataset	Value of Volume rank	Attack clusters detection out of total dataset	Normal clusters detection out of total dataset
1	0.5 to 0.6	1%	99%
	0.1 to 0.3	99%	1%
2	0.5 to 0.7	2%	98%
	0.1 to 0.4	98%	2%
3	0.5 to 0.7	0%	100%
	0.1 to 0.4	100%	0%

The sample shot of the log files of the incoming request is shown



Fields / Characteristics	User Attributes			Request Attributes				
	IP	Time	User Agent	Page	Query	Status	Time Taken	Byte
Degree of concentration		▲	▲	▲		▲	□	□
Frequency	▲			▲				
Interval		▲						
Validity	○		○	○	○			

Figure 1. Anomaly Feature Matrix (: user-based, content-based and page based analysis.

Elements included in the feature matrix allow investigation from diverse (eg: ,user -,content- and page based) analysis .For example ,when analyzing frequency of IP or interval between the successive requests ,each IP (eg: user)must be reviewed in isolation when analyzing validity of user agent or query ,conclusions can be derived based on the content itself without having to compare against past requests. Likewise , some security analysis must be applied on each HTML page. For example anomaly on time taken to serve requests and number of bytes transferred is meaningful only when values are analyzed int the context average value associated with the page.

Effectiveness of AFM as a general framework to characterize web attacks becomes apparent only when several anomaly feature elements are combined as shown in the figure 1 .

The figure:2 shows the total working involved .Firstly the HTTP request is taken as input from the web layer log file . The requested input has login attempt to access the database . Before allowing the login rights the client that are requesting for the further access is analyzed properly by extracting its features .The features are all the characteristic properties of the requests which are predefined and are concerned standardized. These features are then matched with the web log signatures which are already stored as default for the only purpose of security. These features are extracted from the web servers and the databases. If they match each other then these requests are granted and if it does not match then they generate alarms and the characterization of the anomalies is done and visualization using ADAM is done . These kind of requests are blocked and access is not allowed to the databases.

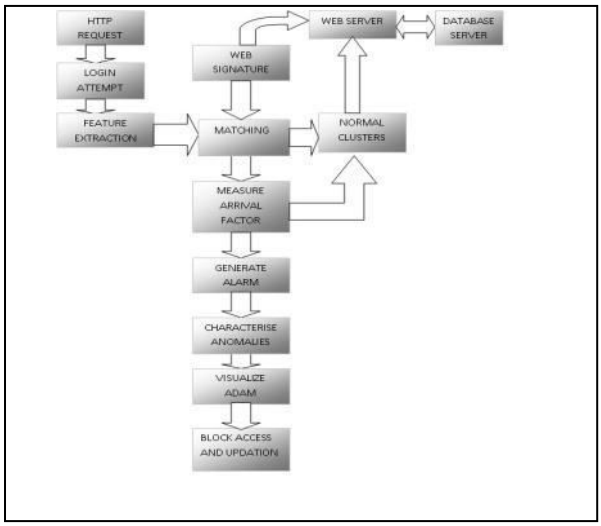


Figure 1 Flow diagram explaining the working

V. CONCLUSION AND FUTURE WORK

Thus we conclude that we have presented an intrusion detection mechanism in which web layer log files are generated and clusters are formed and then labeled data is set either “normal” or “anomalies”. The attacks such as denial of services, SOL injection, directory traversed attack are found out by matching the features of anomalies and intrusive requests that are predefined. Then we have visualized the analysis because it is essential in effectively combating sheer complexity and volume of the logs .ADAM is a useful tool to automate AFM-based anomaly analysis, and it provides powerful visual display capability.This is followed by blocking techniques where the anomalies and the intrusions are traced and the request which originated it is stopped from accessing the database.

In the near future,our attempt would be analyzing and detecting the newly emerging attacks which are not familiar and complicated to the user. We may also try to find the exact location from where the anomalous request has been obtained.

REFERENCES

1) C. Kruegel, G. Vigna, "Anomaly Detection of Web-based Attacks", Proceedings of the 10th ACM Conference on Computer and Communication Security (CCS'03),2003, pp.251-261

2) C. Kruegel, G. Virgna, W. Robertson, A multi-model approach to the detection of web-based attacks, Computer Networks: vol. 48, no. 5, pp. 717-738, 2005

3) F. Valeur, D. Mutz, G. Vigna, "A Learning-Based Approach to the Detection of SQL Attacks", Proceedings of the Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA), Austria, 2005

4) K. Krithivasan and R. Sitalakshmi, "Efficient Two imensional Pattern Matching in the Presence of Errors", Information Sciences, Vol. 43,1987, pp. 169-184.

5) M. Almgren, H. Debar, M. Dacier, "A lightweight tool for detecting web server attacks",In Proceedings of the ISOC Symposium on Network and Distributed Systems Security,2000

6) Qiang and Vasileios Megalooikonomou, A Clustering Algorithm for Intrusion Detection.DEnLab, Temple University

7) Rebecca Bace, Peter Mell, NIST Special publication on Intrusion Detection Systesm, 16th August 2001

8) Sanghyun Cho, Sungdeok Cha, SAD : Web Session anomaly detection based on parameter estimation, Computer & Security.

9) Snort,http://www.snort.org/

10) Stefan Axelsson. Combining a bayesian classifier with visualisation:Understanding the IDS, Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security, pages 99-108, 2004

11) IIS W3C Extended log format, http:// www.loganalyzer.net/ log-nalyzer/w3c-extended.html

❑❑❑

An On-demand Interference-Aware Distance Vector Routing for MANET

G. Nishanthi, & N. M. Balamurugan

Computer Science and Engineering, Sri Venkateswara College of Engineering, Chennai, India
E-mail : nishanthi.2009@gmail.com & balgan@svce.ac.in

Abstract - A fundamental issue impacting the performance of mobile ad hoc networks is the wireless interference among neighboring nodes. In routing protocol, incorporating interference awareness while routing can significantly improve the overall performance of the network. Existing systems measure the interference by actively probing the link. The active probing measurements create additional data overhead and misrepresentation of the link. To overcome this, an analytical model is designed for the effect of interference on data reception probability based on the information which is locally available at that node. In the proposed work, the interference is modeled using interference graph method. The interference graph represents the interference between two communication link or terminals. Based on this graph, no interference path or less interference path is selected for routing. Then calculate the average shortest path length to provide effective transmission between nodes. This proposed method improves the performance of DSR routing protocol.

Keywords*-Interference, Interference graph, Routing protocol*

I. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) are wireless networks that offer multi-hop connectivity between self configuring mobile hosts. Routing in MANET is challenging due to the constraints existing on the transmission bandwidth, battery power and CPU time and the requirement to cope with the frequent topological changes resulting from the mobility of the nodes. In MANET, routing protocols are divided into two categories:

Proactive (table driven) protocols maintain the global topology information in the form o tables at every node. These tables are updated frequently in order to maintain consistent and accurate network state information. DSDV, WRP are some examples o proactive protocols.

Unlike the table driven protocols, on-demand routing protocols execute the path finding process and exchange routing information only when a path is required by a node to communicate with a destination. Some o the on-demand routing protocols are DSR, AODV.

Interference in the mobile ad hoc networks (MANET) influences performance of the network badly. Sometime the terminals which are using the same channel can cause interference when they transmit simultaneously. Interference causes data loss, conflict, and retransmission and so on. The interference model is needed in ad hoc network because of its lack of central co-ordination and distributed nature of network functions. The interference model has the combination of following components: propagation model, interferer's spatial distribution model, network operation model and traffic model. The interference model is classified into three categories:

First one is statistical interference models, which are the statistical characterization of the aggregate interference. The wireless communication requires the knowledge of the statistical characteristics of interference to carry out the performance analysis of the reception technique in a statistical basis.

The second method is modeling the effects of interference. This modeling focuses on the performance of the network which is affected by interference. This model further classified into protocol interference model and physical interference model. Both models establish conditions for correct reception in the presence of interference.

The third method is graph based interference model. Graph also used to model the interference in an ad hoc network, which is called as interference graph. The interference graph is denoted as GI= (VI, EI), and it contains two forms: (1) graphs that model interference between terminals (2) graphs that model interference between links.

These three methods have one common point called radio capture phenomenon, a transmission from a given terminal can be successfully received by another terminal even in the presence of interfering signals at the receiver.

Reducing interference on the path is a critical problem in order to increase the network performance. In the proposed work, interference is modeled using interference graph method. Based on the interference model, less interference path or no interference path is selected for routing. Then calculate the average shortest path to provide the effective transmission between nodes. The average shortest path length is a minimum number of nodes needed to travel between two vertices. This graph based interference model is used to improve the performance of on-demand routing protocols.

II. RELATED WORK

A number of interference metrics have been proposed for estimating the effects of interference in mobile ad hoc network. De Couto et al. in [1] proposed a new metric called Expected Transmission Count (ETX) metric. ETX metric finds expected number of transmissions needed for successful transmission of packets. In this method, the best path is selected by sending data to ten paths one at time, and then selects the path with highest throughput. For implementation purpose they use DSDV and DSR routing protocols. ETX metric improves the performance of DSDV routing protocol compared to find the shortest path.

Jain et al. in [5] proposed the use of conflict graph method used to compute upper and lower bounds for the optimal network throughput under ideal interference-aware routing. Conflict graphs are extracted either based on the protocol interference model or physical interference model. This method improves the performance of multi hop wireless network by selecting optimal routes with less interference than the default shortest path routes. In our work, interference graph method is used to model the interference, based on this interference model, less interference path is selected for routing.

Riadh et al. in [6] proposed a new interference aware routing metric called Estimated Balanced Capacity (EBC). In this work, they propose a 2-hop interference estimation algorithm based on the measurement of received signal strength. The received signal strength is used to calculate the signal to interference plus noise ratio (SINR). The packet error rate is calculated using the SINR value, based on the PER the capacity of a given node is estimated. They propose a new interference aware routing metric based on the capacity estimation analysis. This metric improves the network capacity in wireless multi-hop networks.

Maaly et at in [8] proposed a new topology construction algorithm called interference-aware connected dominating set (IACDS). The IACDS algorithm is an energy-efficient and interference-aware topology construction mechanism used to identify a CDS to turn off the unnecessary nodes while keeping the network connected. This proposed algorithm provides complete communication coverage with minimum interference.

Li et al. in [7] proposed a novel interference aware routing metric called Network Allocation Vector Count (NAVC). In this work, each node will calculate its NAVC value by collecting the Network Allocation Vector (NAV) value from the MAC layer. This NAVC metric is generic and it can be used in all routing protocols. Here, they use NAVC as a routing metric for AODV. The modified AODV routing protocol contains route discovery module and transmit power control module. This metric improves the network throughput and lifetime.

Zhang et al. in [12] proposed a new interference aware routing protocol. In this work, first they compute node-interference, link-interference and path-interference. Based on this information an interference-aware routing protocol with minimum average link interference was proposed. The average link interference-aware routing protocol was implemented on dynamic source routing (DSR). This new routing protocol gives better performance than DSR.

Xian et al. in [4] proposed a new scheme called the critical Neighbor (CN) scheme to reduce the interference in the network. This scheme reduce the level of interference by adaptively change the transmission power of nodes .The critical neighbor scheme (CN) reduces the collisions and it provides the higher throughput and lower delay. This CN scheme implemented on AODV-LR achieves better performance than AODV-LR.

Qiong et al. in [2] proposed a new mechanism called interference aware probability forwarding (IPF) to reduce the interference. The IPF is used to adjust the carrier sensing threshold and then forward the probability to every node in the network. The probability is related with the real time interference and the maximal interference in the network. Finally the IPF mechanism avoids nodes or area with high interference and reduces the total interference.

In summary, there are many interference-aware metrics, schemes and topology control algorithms are proposed to reduce the interference. The main goal of

our work is to model the interference using interference graph method.

III. PROBLEM FORMULATION

The main problem addressed in this paper is formulated as follows: The goal is to model the interference in mobile ad hoc network by using interference graph method.

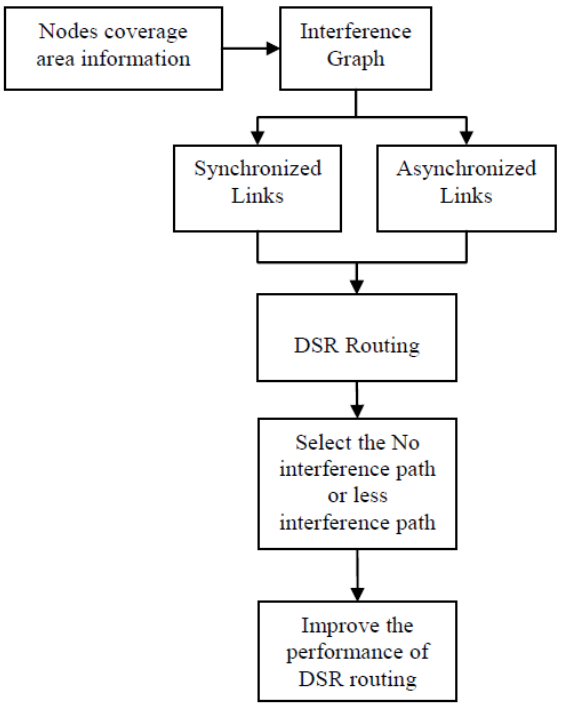


Fig 1. Outline of the proposed work

IV. PROPOSED SYSTEM

The main goal of our work is to reduce the interference level in the path using graph based interference model. The outline of proposed method is illustrated in Figure. 1. The interference graph is constructed based on the node coverage area information such as distance between nodes, whether all nodes are transmitting at the same power and etc. This interference graph is used to model the interference among links. Based on the interference graph the links are scheduled for interference-free transmissions. Then use this interference graph method in dynamic source routing (DSR) and evaluate the performance of DSR routing protocol.

A. Interference Graph

Model the interference using graph is called as interference graph. The interference graph is denoted as GI= (VI, EI), and it contains two forms: (1) graphs that model interference between terminals (2) graphs that model interference between links. In our proposed system, the second method is used for construct the interference graph. In a network a transmitter receiver pair (a, b), with distance r is associated with an interference disk of radius ri (b) = r $\beta 1/\eta$ centered at b, inside which no active transmitter can be located, in order to guarantee successful reception of the signal from v. The interference disk is link specific and it can be used to construct the interference graph that model interference among links. The Figure 2 shows the connectivity graph, in that all terminals are transmit at the same power. In this Figure the link lcd interferers with link lab because transmitter c falls inside the range of b.

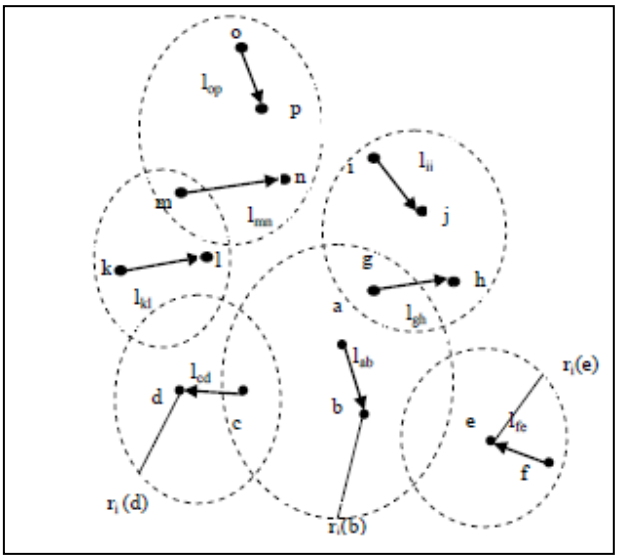


Fig 2. Connectivity graph G= (V, E)

An example of interference graph is shown in Figure 3. The interference graphs are directed, because the link l_{cd}

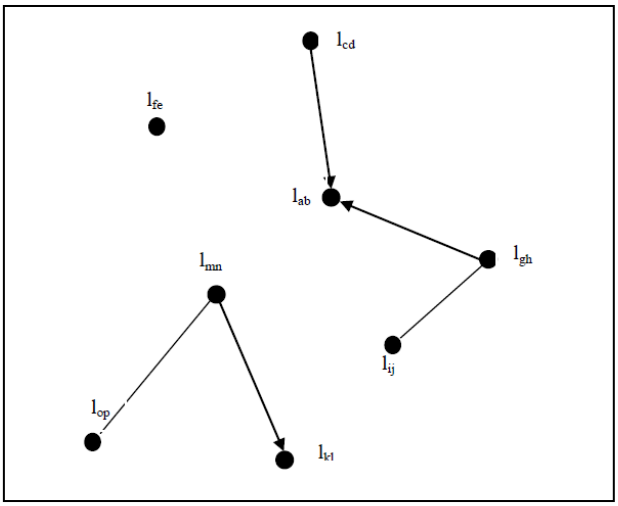


Fig 3. Interference graph GI= (VI, EI)

interferers with link l_{ab}, but not vice versa. The link l_{fe} neither interferers or interfered by other two links. The interference free transmission is provided by scheduling of links. In the above example, the links l_{cd} and l_{ab} cannot be scheduled to be active simultaneously, but link l_{fe} can be simultaneously active with either l_{cd} and l_{ab}.
The less interference path is selected by scheduling the links based on the interference graph. Table 1 shows the scheduled links based on the above interference graph.

TABLE I

Scheduling of links	
Synchronized links	Asynchronized links
l_{ab}, l_{fe}	l_{ab}, l_{cd}
l_{ij}, l_{ab}	l_{ab}, l_{gh}
l_{fe}, l_{cd}	l_{gh}, l_{ij}
l_{op}, l_{ij}	l_{kl}, l_{mn}
l_{ij}, l_{mn}	l_{mn}, l_{op}
l_{fe}, l_{mn}	
l_{kl}, l_{gh}	
l_{kl}, l_{ab}	
l_{kl}, l_{cd}	
l_{gh}, l_{cd}	

In the proposed work, the interference graph method is applied to DSR routing protocol. The DSR protocol is an on-demand protocol and the source node only carries out the path finding process. After the path finding process, the selected paths are tested based on the interference graph method and then the less interference path is selected for routing. Then select the average path length to provide effective transmission between nodes. The average path length l_G is calculated by using the following formula,

$$l_G = \frac{1}{n*(n-1)*\sum_{ij} d(v_i, v_j)}$$

Here, $d(v_i, v_j)$ is distance between vertice v_i to vertice v_j. Lower the value better would be the network transmission. This method can improve the performance of the DSR routing protocol.

V. SIMULATION RESULTS

The performance analysis of interference aware DSR (IA-DSR) routing protocol is focused on the packet loss and packet-delivery fraction in terms of simulation time in seconds. The various simulation parameters are shown in below table.

TABLE II

Simulation Parameters	
Parameters	Values
Data	CBR Traffic
Routing Protocol	DSR
Simulation Time	900 Seconds
Packet Size	512 Bytes

The simulation results show that the packet loss of DSR routing protocol is higher than the IA-DSR. This simulation takes 0 to 900 seconds pause time. The Figure 4 and Figure 5 show the comparison between DSR and IA-DSR routing protocol under 50 nodes and 100 nodes configuration. The packet loss increases when the number of nodes is increased, interference level is directly proportional to the node density. So it will cause more packet loss.

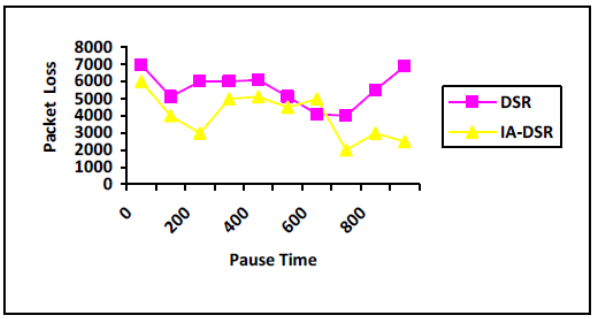


Fig 4. Packet Loss vs. Time (50 nodes)

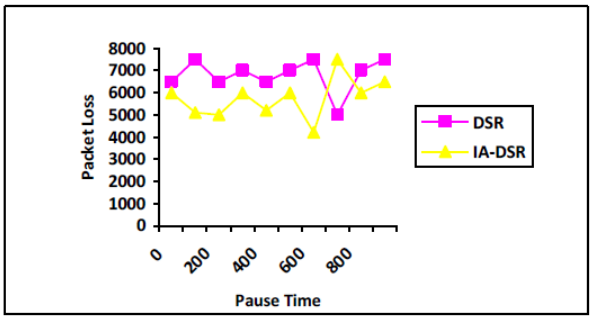


Fig 5. Packet Loss Vs Time (100 nodes)

VI. CONCLUSION

Interference in ad hoc wireless networks is the objective of the work. Here the interference graph method is used to model the interference among links in ad hoc wireless network. The results of interference graph method are applied to DSR routing protocol. The performance evaluation by means of simulations shows

that this proposed method can decrease the packet loss, compared to the existing DSR protocol. The future work is to investigate the benefits of interference aware routing under more complex scenarios like sensor network will be extended.

REFERENCES

[1] Couto D.S.J.D., Aguayo D., Bicket J., and Morris R. "A High Throughput Path Metric for Multi-hop Wireless Networking," Proc. ACM Mobicom, vol. 11, pp.419-434, July 2005.

[2] De Rango. F, Fazio. P, Marano. S, "Impact of interference aware metrics over UWB based MANET," Wireless Telecommunication Symposium, pp.298-303, June 2008.

[3] Georgios Parissidis, Merkourios Karaliopoulos and Bernhard Plattner. " Intererence-Aware Routing in Wireless Multi-hop Networks," IEEE Transaction on mobile computing, vol. 11, No. 5, May 2011.

[4] Hwee Xian TAN, Winston K.G. SEAH, "Dynamic Topology Control to Reduce Interference in MANETs,".

[5] Jain K., Padhye J., Padmanabhan V., and Qiu L. " The impact of interference on Multi-Hop Wireless Network Performance, "Proc. ACM Mobicom, pp.66-80, Sep. 2003.

[6] Kortebi R.M., Gourhant Y., and Agoulmine N., "On the use of SINR for interference-aware routing in Wireless Multi-hop Networks," IEEE Transactions on Wireless Communication and Networking, Oct.2007.

[7] Liran Ma, Qian Zhang, Yongqiang Xiong, and Wenwu Zhu, "Interference-aware Metric for Dense Multi-hop Wireless Networks," IEEE Transactions on Communications, vol.2, pp.1261-1265, Aug.2005.

[8] Maaly A. Hassan, Ibrahim S. Abuhaiba, "Interference Reduction in Mobile Ad hoc and Sensor Networks,"Journal of Engg. And Computer innovations, vol.2(7), pp. 138-154, Sep.2011.

[9] Nor Surayati Mohamad Usop, Azizol Abdullah, Ahmad Faisal Amri Abidin, "Performance evaluation of AODV, DSDV and DSR routing protocol in Grid Environment, "IJCSNS, vol.9, No.7, July 2009.

[10] Paulo Cardieri, "Modeling Interferenve in wireless Ad Hoc Networks, "IEEE Communications surveys& Tutorials, vol.12, No.4, 2010.

[11] Qiong Liu, Ximming Zhang, Yongzhen Liu, Dong Shi, Enbo Wang, "Interference-aware Probability Forwarding Mechanism for Mobile Ad Hoc Networks," ncm,vol. 1, pp.474-479, 2008.

❑❑❑

Graphical Authentication Using Region Based Graphical Password

G. Niranjana & Kunal Dawn

Dept of computer science and engg, SRM University. Chennai, India
E-mail : niranjana.g@ktr.srmuniv.ac.in & kunal.dawn@gmail.com

Abstract - Password authentication is failing as an authentication since it increases the user burden to remember the passwords. Graphical authentication is proposed as a alternative for textual passwords since it may be easy for users to remember.In this paper we propose a new image region selection based graphical password scheme. We are going to present a new technique for authentication which is based on the tracking of mouse motions on an image called mouse gestures for selecting regions in the image. In general, a gesture is a sequence of interactions with the application, which represents one of the Specified symbols. A mouse gesture is a continuous, directed sequence of the mouse cursor movements with the clearly distinguished start and end. A set of gestures may be stored in a database called gesture classes for each user. Users are allowed to select a set of random images and a gesture for each image. Some tolerance level is also given for each gesture. When logging in if the user draws the correct gesture using mouse the user will be treated as an authenticated user. Mouse gestures are captured through bounding box and corner detection algorithms. This method provides more security than cued click points where the user is allowed to click on a particular point called pass point for authentication which is more vulnerable to hackers.

Keywords*-mouse gesture, gesture class, cued click points, authentication.*

I. INTRODUCTION

Passwords are expected to comply with two fundamentally conflicting requirements:

1. *Passwords should be easy to remember,*
2. *Passwords should be secure*

Satisfying these requirements is virtually impossible for users[5]. Various graphical password schemes have been proposed as alternatives to text-based passwords. Research and experience have shown that text-based pass-words are fraught with both usability and security problems that make them less than desirable solutions[5]. Psychology studies have revealed that the human brain is better at recognizing and recalling images than text[3]; graphical pass-words are intended to capitalize on this human characteristic in hopes that by reducing the memory burden on users, coupled with a larger full password space offered by images, more secure passwords can be produced and users will not resort to unsafe practices in order to cope.

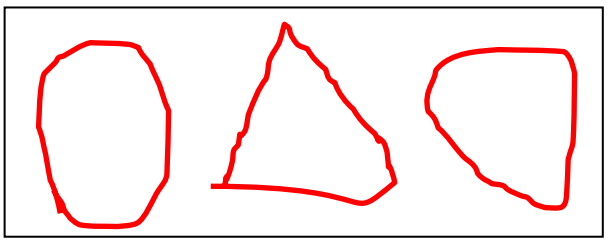
Initially Cued Click Points (CCP) was used for authentication where the users are allowed to select a set of images and in each image one particular point is selected. This particular point is called the passpoint through which the user is authenticated [1]. A password consists of one click-point per image for a sequence of images. The next image displayed is based on the previous click point. Graphical authentication using CCP method has the drawback that the user has to remember the particular pass point in the given set of images and it should have high tolerance level. In this paper, we propose a new image region selection based graphical password scheme. It can be viewed as a combination of Pass Points and Cued Click Point (CCP). A password consists of one region selection per image for a sequence of images. The next image displayed is based on the previous selected region so users receive immediate implicit feedback as to whether they are on the correct path when logging in. This scheme offers both improved usability and security. In the proposed method the user can just remember the region and its shape. No burden to human brains and also a security level may also be given for it.

The rest of the paper is 69rganized in such a way that section 2 contains introduction to mouse gesture. Section 3 carries the region detection algorithm which includes registration process of an user using bound box algorithm for capturing the gesture, Authentication procedure is detailed with corner detection method and region pixel count method to calculate the virtual grid pixels in the region. Section 4 is explained with

experimental results and analysis. Conclusion and future work are described in section 6.

II. MOUSE GESTURE

A mouse gesture is a continuous, directed sequence of the mouse cursor movements with the clearly distinguished start and end points. In our work, gestures are marked by pressing the right button. The usability of the assumednotion of gesture was assessed during experiments described in Hofman [2],For high usability of gestures-based interface, three basic features must be preserved: accuracy, efficiency (of recognition), and adaptability to the possibilitiesand needs of the individual user[4]. Accuracy is understood as the percentage of properly recognised gestures in relation to the intention of the user performing them. Efficiency should be enough for the use on an average computer. Adaptabilitymeans easy registration of the own classes of gestures of the given user. Some of the simple gestures are



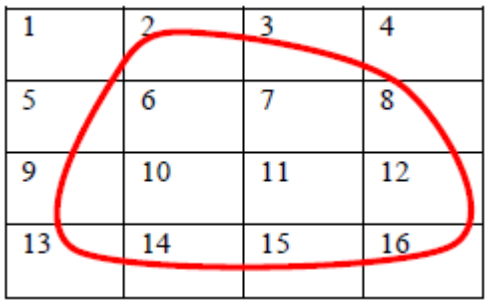
III. REGION DETECTION ALGORITHM:

To detect the user selected region in a very efficient manner we have used three methods that represent the region in a numerical way so that it can be stored in the database in an efficient way and also reduce the network transmission of data.

A. Bounding box method

The first method we will discuss is the bounding box method. This involves drawing a box around the gesture and dividing it up into a grid. The gesture is then defined by the areas that it passes through. The grid would be set up as follows.

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16



The gesture on the right would then be parsed as 13,9,5,1,2,3,4,8,12,16 if you had drawn it from left to right. There are many advantages to this method. The first is that it's very easy to code. The design is simple and creating and defining gestures is very easy. It would also be pretty accurate when actually interpreting the gestures. It would deal with erratic mouse behavior well because human errors are of no consequence as long as it stays in the area. For this same reason, it handles curved gestures as well as straight ones.

In this method we determine the rectangle that bounds the user selected region. A virtual grid is presented on top of the image. When user draws the region on top of an interested image object the pixels are plotted on top of the grid pixels. The grid pixels are set to value of 1 where the user gave drawn the region and elsewhere is set to 0. The bounding box can be detected easily by calculating the maxima and minima of the user inputted pixels in the grid.

$$g(x,y) = \begin{cases} 1 \; if \; its \; a \; gesture \; point \\ 0 \; else \; where \end{cases}$$

Registration algorithm

registration(user_id)

- Sequrnce_number:=1;
- While sequence_number is less than 4 do
  - Generate a random number between 1 to 203 (total number of images in the database), let it be the image_number;
  - Retrieve the random image with image_number from the data base and show it to the user;
  - Draw a virtual grid over the image;
  - Wait for the user to select the region;
  - Calculate the parameters top_x, top_y,$bottom_x$, $bottom_y$;
  - Store the parameters with sequence_number image_number and user_id in the database;

- Sequence_number:=sequence_number+1;

B. Corner detection method

Another method is corner detection. At first this may seem similar to the change in direction method, but is actually quite different. This involves figuring out which points are the corners, and then looking at the relationship between those corners. The advantage of this is that it would be very accurate, provided the algorithm detects the corners properly. This method also takes into account the proportions of each part of the gesture.

In this method we determine the top left and bottom right corners of the bounding box. We use this method because it uniquely represents every user selected regions in that image, that is, no two different regions on the image will have the same Corner value. This can be done easily by the following set of equations.

$$top_x = \min_{x,y}\{\, x \mid g(x,y) = 1 \,\} \quad (1)$$

$$top_y = \min_{x,y}\{\, y \mid g(x,y) = 1 \,\} \quad (2)$$

$$bottom_x = \max_{x,y}\{\, x \mid g(x,y) = 1 \,\} \quad (3)$$

$$bottom_y = \max_{x,y}\{\, y \mid g(x,y) = 1 \,\} \quad (4)$$

The algorithm is defined as follows

Corner detection algorithm

login(user_id)

set sequence_number:=1;

set login_stat:=1;

While sequence_number is less than 4 do

If login_stat=1 then do

- Fetch the parameters from the database with current sequence_number and user_id;
- Retrieve the image from the database with fetched image_number and show it to the user;
- Draw a virtual grid over the image.
- Wait for the user to select the region;
- Calculate the new parameters top_x, top_y,$bottom_x$,$bottom_y$;
- Calculate the difference $d_{tx}, d_{ty}, d_{bx}, d_{by} d_{gp}$;
- If the calculated differences are within CT and GPT range then

a. sequence_number:=sequence_number+1;

b. login_status:=1;

else

a. sequence_number:=sequence_number+1;

b. login_stat:=0;

else do

- Generate a random number between 1 to 203 (total number of images in the database), let image_number;
- Retrieve the image with image_number from the data base and show it to the user;
- Draw a virtual grid on top of the image;
- Wait for the user to select the region;
- sequence_number:=sequence_number+1;

End

End

iflogin_stat=1 then do

successful login;

else

login fail;

End

The differences$d_{tx}, d_{ty}, d_{bx}, d_{by} d_{gp}$are calculated using the following equations.

$$d_{tx} = |n_{topx} - o_{topx}| \quad (5)$$

$$d_{ty} = |n_{topy} - o_{topy}| \quad (6)$$

$$d_{bx} = |n_{bottomx} - o_{bottomx}| \quad (7)$$

$$d_{by} = |n_{bottomy} - o_{bottomy}| \quad (8)$$

$$d_{gp} = |n_{gesturepixel} - o_{gesturepixels}| \quad (9)$$

Here $d_{tx}, d_{ty}, d_{bx}, d_{by}$ are the displacement values and d_{gp} is the pixel difference value that are calculated from the new and old saved parameters as described above.

B. Region Pixel Count Method:

In this method we determine how many virtual grid pixels the user had used to select the region. This method is required because two different user may select the same region in the same image but there selection cannot be the same hence they defer on the number of the virtual pixels and also it distinguish the same region selection with different shape because different shape will have different pixel count

$$gesture_{pixel} = \sum_{i=1,j=1}^{x,y} g(i,j) \quad (10)$$

Where $g(x,y)$is defined as

$$g(x,y) = \{^{1\ if\ its\ a\ gesture\ point}_{0\ elsewhere} \quad (11)$$

These three methods together creates the required parameters that can represent the data as a set of numeric values which are very much convent to store and retrieve and also encryption on this data can be done while transferring over network.

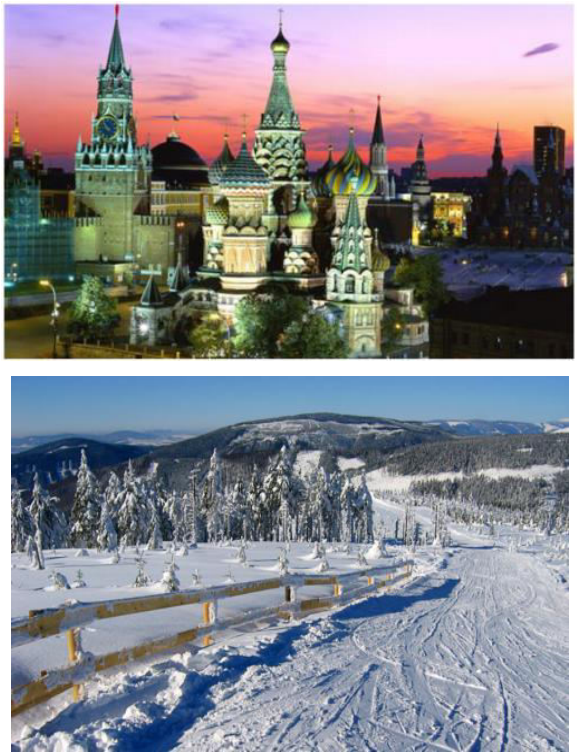
IV. EXPERIMENTAL RESULTS AND ANALYSIS

At the time of registration the user selects a specific region onthe given image of his interest which he can remember easily. A set ofrandom and unique images are fetched from the database forregistration. For the set of images given to the user, user selectsregions in every image and remembers its position and size in that sequence and this information is stored in the database for futurelogin purpose. At the time of login the sequence of images given tothe user one by one which was saved at the time of the registration.Now the user selects the region with the gesture that was used at the time of registration. For every image, our algorithm calculates theparameter's and matches with the previously stored parameter's forthat image with some tolerance value. If the match is a success thennext image is fetched from the database and the process is repeated and if the match is unsuccessful then the user is not notified untilthe end and at the next sequence a random image is given to the userand login fail flag is activated. This approach increases the totalsearch space of the attacker and also smart users can select complex regions.

In our work, we have used 203 images for selecting random images. The parameters are calculated using the equations (1) – (11). Some tests are carried out based on the following parameters.

Number Of Images	203
Size Of Image	500x312
Size Of Grid	125x78
Size Of Grid Cells	4x4
Number Of Images for Authentication	4
Total Attempts per test	20

Users are allowed to register to the system by creating their own passwords. Then we record the number of Successful Login per 20 attempts to login correctly. It is also possible that the user may fail to login although he or she has entered correct data. This occurs because of the tolerance value we have used for the test. Here we vary the CT and GPT parameters and check how they affect the Success per Correct Attempt.



(a)

Figure 1. Registration process

Figure 1. shows sample outputs (a) original images (b) user selected gestures (c) bounding box for gestures.

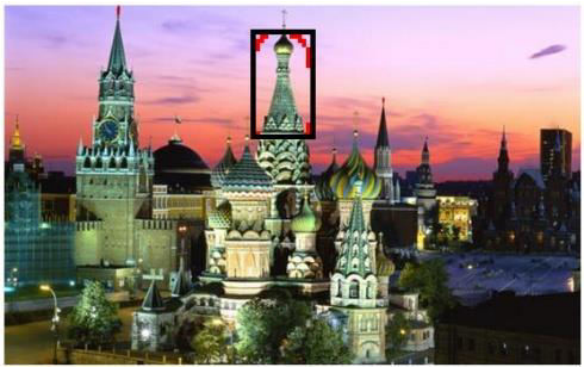
Table 1 shows the actual gesture calculated values of top_x, top_y,$bottom_x$,$bottom_y$using the equations (1) – (4).

Table2 shows the calculated values of top_x, top_y,$bottom_x$, $bottom_y$along with the tolerance when the user logs in.

Img Id	Seq No	Top X	Top Y	Bottom X	Bottom Y	Grid Pixel Count
84	1	59	3	73	30	71
165	2	85	15	115	59	135
169	3	12	46	79	78	151

Imgid	SeqNo	Top X	Top Y	Bottom X	Bottom Y	Grid Pixel Count
84	1	59	6	73	31	74
165	2	86	18	118	60	121
169	3	11	43	81	73	179

(b)



(c)

Table 3 shows the various test cases results by calculating difference between the stored data and login data using the equations (5) – (10). Table 4 shows the results of various tolerance level by calculating coordinate tolerance and grid pixel tolerance using the equations (11) and (12).

Fig 4 shows the graph o the success rate for the proposed method. Users are authenticated by allowing them to select their own gestures so that they can easily remember it. Also hackers are diverted in such a way that they could not identiy where they went wrong.

Table 1. Actual data stored for user
Table 2. Data collected at the time of login

Result : Successful Login With

Coordinate Tolerance (C.T): 10

Grid Pixel Tolerance (G.P.T): 30

Table 3. Test Cases:

Calculated Difference among the Stored Data & Login Data

Seqence Number	Top X Difference	Top Y Difference	Bottom X Difference	Bottom Y Difference	Grid Pixel Count Difference	Result
Login Attempt 1 / Authenticated / Tolerance [C.T=10] , [G.P.T=50]						
1	0	3	0	1	3	Pass
2	1	3	3	1	14	Pass
3	1	3	3	1	28	Pass
Login Attempt 2 / Login Fail / Tolerance [C.T=5] , [G.P.T=50]						
1	2	1	2	3	4	Pass
2	6	2	1	0	12	Fail
3	-	-	-	-	-	Fail
Login Attempt 3 / Login Fail / Tolerance [C.T=10] , [G.P.T=10]						
1	2	1	2	3	4	Pass
2	6	2	1	0	12	Fail
3	-	-	-	-	-	Fail
Login Attempt 4 / Success / Tolerance [C.T=8] , [G.P.T=20]						
1	2	1	2	3	4	pass
2	6	2	1	0	12	pass
3	1	7	3	8	18	pass

Table 4. Test Cases result on different tolerance level

No	C.T	G.P.T	Success/Correct Data	Total Attempt	Success Rate
1	2	2	**2**	20	10%
2	2	4	**1**	20	5%
3	2	8	**2**	20	10%
4	2	12	**3**	20	15%
5	2	16	**5**	20	25%
6	4	2	**9**	20	45%
7	4	4	**11**	20	55%
8	4	8	**10**	20	50%
9	4	12	**13**	20	65%

10	4	16	**13**	20	65%
11	8	2	**1**	20	10%
12	8	4	**3**	20	15%
13	8	8	**17**	20	85%
14	8	12	**17**	20	85%
15	8	16	**18**	20	90%
16	12	2	**3**	20	15%
17	12	4	**7**	20	35%
18	12	8	**15**	20	75%
19	12	12	**19**	20	95%
20	12	16	**20**	20	100%
21	16	2	**4**	20	20%
22	16	4	**6**	20	30%
23	16	8	**15**	20	75%
24	16	12	**18**	20	90%
25	16	16	**20**	20	100%

Our study shows that CT and GPT parameters have greater effect on the security of the system. The low value of the CT and GPT means it will accept more accurate login data only where if we increase the tolerance value then the system will allow more user errors. In case of low value of CT and GPT the user require more attempts to login but it also increases the security to great extent where with high value of CT and GPT the user may login at his first attempt with near correct data only which also decreases the security of the system.

V. CONCLUSION AND FUTURE WORK

The data in the table depends on the parameters we have selected and the capability of the users while we testing the system. Different implementation with different parameters may produce different data. To generalize this approach we define a new parameter called Security level which is based on different requirements of the secure system. A system with low security level allow users to login to their system with maximum error in the login attempt hence it makes easy for the user to login but it also decreases the search space of the attacker per image. Where a system with high security level allow users to login to their system with near accurate data in login attempt hence it makes more difficult for the user to login but also increases the security to maximum level.

The security level parameters have maximum value of 5 which indicated maximum security of the system and minimum value of 1 which indicate minimum security of the system. Some examples of the different systems with different security levels are:

1. Security Level 1 – System with very less security that only requires user authentication but not great security. Examples of this kind of systems may be simple Forum and Blog sites.
2. Security Level 2 – System with less security. Examples of this kind of systems may be Individuals sites with very less valuable contents.
3. Security Level 3 – System with medium security. Examples of this kind of systems may be Social Networking sites.
4. Security Level 4 – System with high security. Examples of this kind of systems may be Private Business sites or corporate login systems.
5. Security Level 5 – System with very high security. Examples of this kind of systems may be Online Banking Transaction gateway sites.

Depending upon this 5 Security levels we categorize our CT and GPT values. With CT and GPT values of 0 means that no tolerance is accepted and the user is required to enter the exact data that was used at the time of registration which is near impossible to remember. Our experiments shows that with CT, GPT value greater than 2 the users are able to login to the system and CT, GPT value greater than 16 gives very less security because it accepts login data with great error hence every approximate attempt is a successful login.

Our experiments proved that our method provides a good way of authentication using gestures in graphical passwords. Also our authentication method decreases the rate of probability of getting hacked as the options space for authentication is more. Also the hacker is not informed about the error at the instant thereby avoiding unnecessary attempts. Our future work includes capturing the color and texture information of the gesture and using it for authentication.

REERENCES

[1] Sonia Chiasson, P.C. van Oorschot1, and Robert Biddle “Graphical Password Authentication Using Cued Click Points”

[2] Hofman, P.: Selected Issues of Artificial Intelligence in the Construction of User Interface to a CASE System. MSc Thesis, Wroclaw Uniwersity of Technology, (2005).

[3] Nelson, D.L., U.S. Reed, and J.R. Walling. Picture Superiority Effect. Journal of Experimental Psychology: Human Learning and Memory 3, 485-497, 1977

[4] Pawe l HOFMAN1Maciej PIASECKI1 “Efficient Recognition of Mouse-based Gestures “

[5] Blonder, G.E. “Graphical Passwords”. United States Patent 5,559,961, 1996.

[6] Chiasson, S., R. Biddle, R., and P.C. van Oorschot." A Second Look at the Usability of Click-based Graphical Passwords". ACM SOUPS, 2007.

[7] Cranor, L.F., S. Garfinkel. "Security and Usability". O'Reilly Media, 2005.

[8] Davis, D., F. Monrose, and M.K. Reiter. "On User Choice in Graphical Password Schemes". 13th USENIX Security Symposium, 2004.

[9] Dirik, A.E., N. Menon, and J.C Birget." Modeling user choice in the PassPoints graphical password scheme". ACM SOUPS, 2007.Article in a conference proceedings:

[10] H.Goto, Y. Hasegawa, and M. Tanaka, "Efficient Scheduling Focusing on the Duality of MPL Representatives," Proc. IEEE Symp. Computational Intelligence in Scheduling (SCIS 07), IEEE Press, Dec. 2007, pp. 57-64, doi:10.1109/ SCIS.2007.357670.

❑❑❑

An Ant Colony Optimization For Job Scheduling To Minimize Makespan Time

V. Selvi & **R. Umarani**

Associate Professor in M.C.A Dept., M.A.M College of Engineering Siruganur,Trichy .Tamilnadu &
Associate Professor, Sri Saradha college for Women, Salem. Tamilnadu. India
E-mail : Selvigiri.s@gmail.com & umainweb@gmail.com

Abstract *:* This paper deals with the makespan minimization for Job Scheduling . Research on optimization techniques of the Job Scheduling Problem (JSP) is one of the most significant and promising areas of an optimization. Instead of the traditional optimization method, this paper presents an investigation into the use of an Ant Colony optimization (ACO) to optimize the JSP. The numerical experiments of ACO were implemented in a small JSP. In the natural environment, the ants have a tremendous ability to team up to find an optimal path to food resources. An ant algorithm stimulates the behavior of ants. The main objective of this paper is to minimize the makespan time of a given set of jobs and achieved optimal results are encroached.

Key words*: Job Scheduling Problem (JSP), Ant Colony Optimization (ACO), Makespantime.*

I. INTRODUCTION

This paper examines an application of the recently proposed adaptive metaheuristic Ant Colony Optimization (ACO) for the Job Scheduling problem (JSP). In the static JSP, a finite number of jobs are to be processed by a finite number of machines. Each job consists of a predetermined sequence of task operations, each of which needs to be processed without interruption for a given period of time on a given machine. Tasks of the same job cannot be processed concurrently and each job must visit each machine exactly once. A feasible schedule is an assignment of operations to time slots on a machine without violation of the job constraints.(1). A makespan is defined as the maximum completion time of the jobs. The objective of the JSP is to find a schedule that minimizes the makespan.

Ant colony optimization (ACO) is a popular optimization technique, it is a population-based metaheuristic that can be used to find approximate solutions to difficult optimization problems.

In the ACO, each ant constructively builds a solution by several stepwise probabilistic decisions until a solution is reached. The ACO metaheuristic has been applied to various hard combinatorial optimization problems. For example, in the scheduling field, ACO has effectively been applied to the Flow-shop scheduling problem, Resource Constraint project Scheduling problem, etc.,

This paper is organized as follows: Section 2. gives the description of the non-preemption Job Scheduling. Brief introduction of Ant Colony optimization in section 3, Section 4. Implementation of the experimental study and last section 5 Concludes this paper.

II. JOB SCHEDULING

The optimal solution to the Job Scheduling problem involving n jobs and m machines determines the sequence of jobs on each machine in order to complete all the jobs on all the machines in the minimum total time (i.e. with minimum makespan) where each job is processed on machines 1, 2, 3, …, m, in that order.

All jobs have the same processing operation order when passing through the machines. There are no precedence constraints among operations of different jobs. Operations cannot be interrupted and each machine can process only one operation at a time. The problem is to find the job sequences on the machines which minimise the makespan, i.e. the maximum of the completion times of all operations(6). The Job Scheduling problem is usually solved by approximation or heuristic methods.

III. ANT COLONY OPTIMIZATION

A. Ant Colony Algorithm

The ant colony algorithm is an algorithm for finding optimal paths that is based on the behavior of ants searching for food.

At first, the ants wander randomly. When an ant finds a source of food, it walks back to the colony leaving "markers" (pheromones) that show the path has food. When other ants come across the markers, they are likely to follow the path with a certain probability. If they do, they then populate the path with their own markers as they bring the food back. As more ants find the path, it gets stronger until there are a couple streams of ants traveling to various food sources near the colony.

Because the ants drop pheromones every time they bring food, shorter paths are more likely to be stronger, hence optimizing the "solution." In the meantime, some ants are still randomly scouting for closer food sources. A similar approach can be used find near-optimal solution to the traveling salesman problem.

Ant Colony optimization can also be used to solve variety of combinatorial optimization problems, particularly suitable for the multipoint and non-deterministic search in the solution space of discrete optimization problems and job scheduling problem etc. Scheduling problem is typical kind combinatorial optimization problem. Suppose that there are m machines and n jobs .

IV . EXPERIMENTAL STUDY

Step1 :Generating the Ants

The number of ants depending on the number of jobs are taken initially and the search is started. Each ant starts searching an optimal sequence beginning with the job number as its number .

First ants always search for sequence starting with job number 1, the second ant always search for a sequence with job number 2 like as the first job. Similarly ant always give a sequence with job number n as the first in it.

Let number of jobs n=4.

Let number of machine m=4.

Machine

Machines / jobs	M1	M2	M3	M4	T_{ij}
J1	4	6	8	10	**28**
J2	7	9	11	5	**32**
J3	3	2	6	4	**15**
J4	8	9	1	3	**21**

Table 1:Process Time

$$\tau_{ij} \leftarrow (1-\rho).\tau_{ij} + \Delta \tau_{ij}^{best} \quad \text{--- 1}$$

Step 2: Initialization of pheromone matrix

Next the pheromone matrix has to be initialized. It is referred to the problem as 'τ' matrix. This 'τ' matrix is square matrix of order nxn where 'n' is number of jobs as given in the problem. The pheromone matrix is one which gives the numerical value of the intensity of the pheromone trail remaining in the path i-j. This pheromone matrix helps the ants in deciding which path it has to construct while searching for the optimal solution. All the diagonal element are assigned with 0 since an ant can't go from i^{th} position to i^{th} position. All other elements are assigned to some arbitrary constant.

	P1	P2	P 3	P4
J1	0	0.6815	0.7797	1.0000
J2	0.6587	0	0.7033	0.24
J3	0.2475	0.4012	0	0.5867
J4	0.1223	0.082	0.7957	0

Table 2: Pheromone matrix for 4x4 flow shop scheduling

Step3: Sequence generation by all ants

After the initialization of the pheromone matrix, the ants start constructing the sequence. To decide which job to put first and which job will taken into next, the probability of the selection is done by the following equation(2).

$$\rho_{ij} = (\tau_{ij})^{\alpha}(\eta_{ij})^{\beta} / \sum(\tau_{ik})^{\alpha}(\eta_{ik})^{\beta} \text{ -------(2)}$$

Where, 'i' stands for the job that is already fixed by the ant, 'j' stands for not yet scheduled jobs.

'τ_{ij}' Value is taken from the pheromone matrix , η_{ij} is the reciprocal of the total time taken by j_{th} job through all machines

'k' ant number, Let α, β are constants. In our problem α=2, β=3.

The ACO algorithm always find the local optimal but rarely find the global optimal. The optimal sequence produced by 4 ants are and makespan for each sequence

Ant - No	Optimal Sequence Jobs				Makespantime
1	1	3	4	2	48
2	2	3	4	1	52
3	3	4	1	2	51
4	4	3	1	2	50

Table 3: Different sequences from Ant system

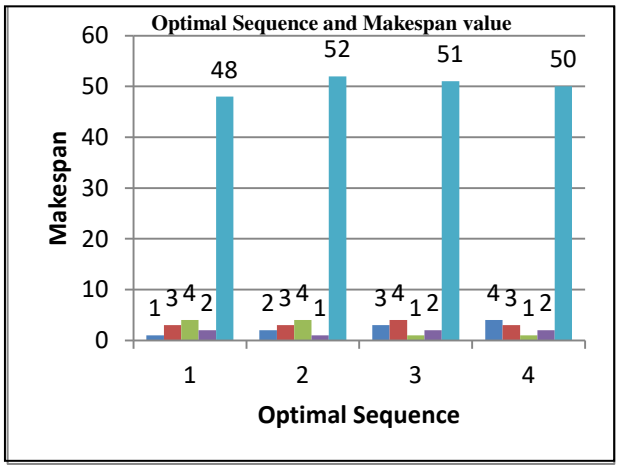


Figure 1 graphical representation of Makespantime. From this above figure, the optimal sequence of 4x4 matrix is 1,3,4,2.

Step4 Calculation of Δτ matrix

Next step is formulation of Δτ matrix. For each ant, a Δτ matrix has to be constructed. The Δτ matrix is a matrix that is used for updating pheromone matrix. This Δτ matrix is constructed for each ant.

Step 5:Updating of pheromone matrix :

The pheromone update equation takes the following form:

The more number of iterations ,give the efficiency of the results obtained and all the optimal sequences are listed out whose output is given as for the low level heuristics.

V. CONCLUSION:

In this paper, an ACO based heuristic to solve the JSP for minimum makespan time criterion is proposed and therefore capable of finding the optimal or near-optimal solutions. ACO can be easily adapted to generate schedules for any scheduling objective of JSP. A future research issue would be to develop hybrid heuristics by incorporating local search techniques, such as PSO and genetic algorithm and tabu search.

REFERENCES:

1. D. Martens, M. De Backer, R. Haesen, J. Vanthienen, M. Snoeck, B. Baesens, Classification with Ant Colony Optimization, IEEE Transactions on Evolutionary Computation, volume 11, number 5, pages 651—665, 2007.
2. Dorigo, M. and St¨utzle, T. (2004). Ant colony optimization. The MIT Press, Massa-chusetts, Cambridge, MA.
3. Xing, L., Chen, Y., and Yang, K. (2009). Multi-objective flexible job shop schedule: design and evaluation by simulation modeling. Applied Soft Computing, 9(1):362–376.
4. Varadharajan, T. and Rajendran, C. (2006). A multiobjective simulated-annealing algorithm for scheduling in flowshops to minimize the makespan and total flowtime of jobs. European Journal of Operational Research, 167(3):772– 795.
5. Chunhui Piao, Xufang Han, Yalan Wu (2010). Improved Ant colony algorithm for solving Assignment problem. International Confernce on Computer Application and System Modeling.V15-476-480.
6. Elnaz Baghal Azardoost, Nrges Imanipour , Proceedings of the 2011 International A Hybrid Algorithm for Multi Objective Flexible Job Shop Scheduling Problem Conference on Industrial Engineering and Operations Management Kuala Lumpur, Malaysia, January 22 – 24, 2011.

❑❑❑

Blur Detection in Digital Images-A Survey

Prasad D.Pulekar[1], J.W.Bakal[2] & Manish Bhelande[3]
[1]Konkan Gyanpeeth College of Engg.,Karjat, Mumbai University,
[2]S.J.Jondhale College Of Enggg.,Dombivali,Mumbai University,
[3]K.C. College of Engg.,Thane, Mumbai University
E-Mail : [1]pprasad1717@gmail.com, [2]bakaljw@gmail.com, [3]manishbhelande@gmail.com

Abstract - This paper describes an overview of blur detection in digital images. Digital cameras are designed with auto-focusing and motion compensation functions. There are several other factors including limited contrast, inappropriate exposure time and improper device handling which can still lead to blurriness i.e. unsatisfactory image quality. So there may be multiple blurry images in anyone's picture collections. Also it causes a wastage of storage space. There are many more methods to detect the blur from from the blurry images some of which requires transforms like DCT or Wavelet and some doesn't require transform

Keywords— *Blur , DCT, Wavelet, SIFT.*

I. INTRODUCTION

In any collection of digital images captured with a low-cost digital camera, the most noticeable artifact is blurring. Typical causes of blurriness include loss of focus, camera jitter, moving objects, limited contrast and inappropriate exposure. Blur stands for smooth, lack of detail and sharpness. This in turn is equivalent to lack of high-frequency components in an image. when highfrequency components are removed from a picture,the result is a blurred picture. Blurriness is unsatisfactory image quality. There are already some existing methods for blur detection or image quality estimation for digital images However, most of them are time-consuming, computation intensive, need different kinds of transformations (e.g. DCT or DWT) or the detection ratio is not very high Also there is one proposed algorithm for automatic real time detection of blurry images The algorithm is based on computing variance values of the local key points that are extracted from the given images through implementing Scale Invariant Feature Transform (SIFT) algorithm in a scale space . No transforms (DCT or DWT) are required to be applied to the images, and no edge locations need to be identified in the proposed method, which are the main techniques used in most of the existing methods. Only pixel values of the given images are directly employed in the algorithm.

II. BLUR IN DIGITAL IMAGES :

By the definition, blur is a form of bandwidth reduction of an ideal image owing to the imperfect image formation process. It can be caused by relative motion between the camera and the original scene, or by an optical system that is out of focus.

Blur stands for smooth, lack of detail and sharpness. This in turn is equivalent to lack of high-frequency components in an image. Blurriness is unsatisfactory image quality. The four main causes of blurry photos are:

a. Out Of Focus

b. The subject moves while the shutter is open

c. The camera moves while the shutter is open

d. Depth Of Field is too shallow

Blur is one of the conventional image quality degradation which is caused by various factors. The blurred images are further classified into either locally or globally blurred images. For globally blurred images, we estimate their point spread functions and classify them into camera shake or out of focus images. For locally blurred images, we find the blurred regions using a segmentation method, and the point spread function estimation on the blurred region can sort out the images with depth of field or moving object. The blur detection and classification processes are fully automatic and can help users to filter out blurred images before importing the photos into their digital photo albums.

Types of Blur in Digital Images:

In digital image there are 3 common types of Blur effects:

1) *Average Blur*

The Average blur is one of several tools you can use to remove noise and specks in an image. Use it when noise is present over the entire image.

This type of blurring can be distribution in horizontal and vertical direction and can be circular averaging by radius R which is evaluated by the formula:

$R = \sqrt{g2 + f2}$

Where: g is the horizontal size blurring direction and f is vertical blurring size direction and R is the radius size of the circular average blurring.

2) Gaussian Blur

The Gaussian Blur effect is a filter that blends a specific number of pixels incrementally, following a bell-shaped curve. The blurring is dense in the center and feathers at the edge. Apply Gaussian Blur to an image when you want more control over the Blur effect.

3) Motion Blur

The Motion Blur effect is a filter that makes the image appear to be moving by adding a blur in a specific direction. The motion can be controlled by angle or direction (0 to 360 degrees or –90 to +90) and/or by distance or intensity in pixels (0 to 999), based on the software used. Three blur features can be utilized to separate blurred and unblurred areas of a distorted image (here we mean both motion blur and out-of-focus blur):

1. Blurred areas unlike corresponding unblurred areas loose some high frequency components in their colour frequency domain.

2. Blurred areas unlike corresponding unblurred areas have smaller gradient magnitude due to removing of sharp edges of objects inherent to natural images.

3. Blurred areas unlike corresponding unblurred areas have smaller colour saturation, what is seen from colour histograms of blurred and unblurred images of the same region.

III. EXISTING BLUR DETECTION TECHNIQUES:

There are following existing techniques for blur detection.

1) Blur detection for Digital images using DCT**:**

This technique uses a new solution to aim at exploiting the available DCT information in MPEG or JPEG compressed video or images while involving a minimal computational load. , this technique is based on histograms of non-zero DCT occurrences, computed directly from MPEG or JPEG compressed images. For MPEG compressed video, the system is suitable for all types of pictures: I-frames, P-frames or B-frames.

The objective of blur detection in this method is to provide a percentage indicating the global image quality in terms of blur: 0% would mean that the frame is totally blurred while 100% would mean that no blur at all is present in that particular frame. This blur indicator characterizes the global image blur caused by camera motion or out of focus. Since we focus analyzing MPEG compressed video data, it is desirable that the blur indicator can be directly derived from the DCT layer of an MPEG video bitstream. To achieve this objective, one should be aware that: The DCT coefficients used within MPEG are intended for compression and are deeply related to the image content. Basically, they reflect the frequency distribution of an image block.

In a MPEG stream, DCT coefficients are directly applied on the pixels of I-frames. On the contrary, coefficients of P- and B-frames describe the residual image that remains after motion compensation. It is therefore important to select a blur indicator which is as independent as possible from the particular content of an image as well as from the type of MPEG frames (I, P or B). Blur is the opposite of edge sharpness. DC coefficients render this sharpness via the high values of some **AC** coefficients. In this method blur measure therefore looks for the absence of such edges into the image, which is considered to prove a blurred image. The blurr measure is obtained as follows

1. In order to characterize the global blur, it is proposed to establish a measure that takes into account the DCT information of the entire image as a whole. It is likely that any type of edge will cross some 8 x 8 blocks at least once in the image. Globalization among all DCT blocks would therefore enable to have an idea about the general edge sharpness, i.e. the global (camera or motion) blur.

2. In order to be as independent as possible of the content of the image, coefficients should not be considered directly since their values are closely related to the type of image they depict. One rather proposes to look at the distribution of null coefficients instead of the values themselves: blurred images are likely to have all of their high frequency coefficients set to zero, whatever their content is.

3. In order to remove the dependency to the image size, the number of blocks in the image should divide the number of times a coefficient is not zero. This would limit histogram values to 1. However, coefficients are often zeros in P- and B-frames. In order to homogenize the look of the histogram for all types of pictures, the number of non-zero occurrences of a coefficient is divided by the number of non-zero occurrences of the DC

coefficient. 2)Blur Detection for Digital Images Using Wavelet Transform :

This technique uses Harr wavelet transform, which belongs to direct methods. It can not only judge whether or not **a** given image is blurred, which is based on edge type analysis, but also determine to what extent the given image **is** blurred, which **is** based on edge sharpness analysis. This technique recovers sharpness from the blurred version . It is effective for both Out-of-focus blur and Linear-motion blur. In this technique of blurr detection , Different edges are generally classified into three types: namely, Dirac-Structure, Step-Structure and Roof-Structure **.** Step-Structure is classified into Astep-Structure and Gstep- Structure according to whether the change of intensity is gradual or not Note that for Gstep-Structure and Roof- Structure edge, there is a parameter $\boldsymbol{a}$ $(0 < \boldsymbol{a} < \boldsymbol{n/2})$ indicating the sharpness of the edge: the larger $\boldsymbol{a}$ is, the sharper the edge is. The basic idea is : In general, most natural images contain all types of edges more or less, and most Gstep-Structure and Roof- Structure are sharp enough. When blur occurs, no matter whether it is caused by Out-of-focus or Linear motion, both Dirac-Structure and Astep-Structure will disappear. both Gstep-Structure and Roof-Structure tend to lose their sharpness. This technique technique judges whether a given image is blurred according to whether it has Dirac- Structure or Astep-Structure, and uses the percentage of Gstep- Structure and Roof-Structure which are more likely to he in a blurred image to determine the blur extent.

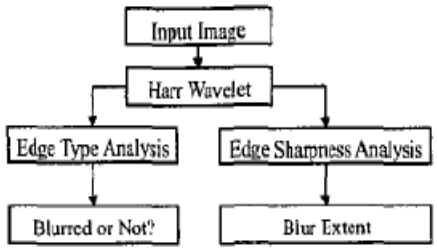


Fig.1 flow chart of blurr detection using Harr wavelet transform

IV. SIMPLE ALGORITHMFOR BLUR DETECTION WITHOUT USING TRANSFORM

Fig.2 context flow diagram

1) Input the images one by one , Imn is the array of images.

2) If array of images is two dimensional , calculate global variance value S2p for P no of difference sample values. If array of images is not two dimensional ,convert the same to two dimentional.

3) S2 p1 is sample variance value of the pre-image and S2 p2 is sample variance value of the taken image, if image is first one only i.e if n=1 and S2 p1 = S2 p, Go for the next image

4) If n>1 and S2 p2 = S2p , Calculate ratio R of sample variance values of pre-image and taken image.

5) If R =1 0r R < 1, the taken image is not blurred delete it and if R>1 the taken image is blurred.

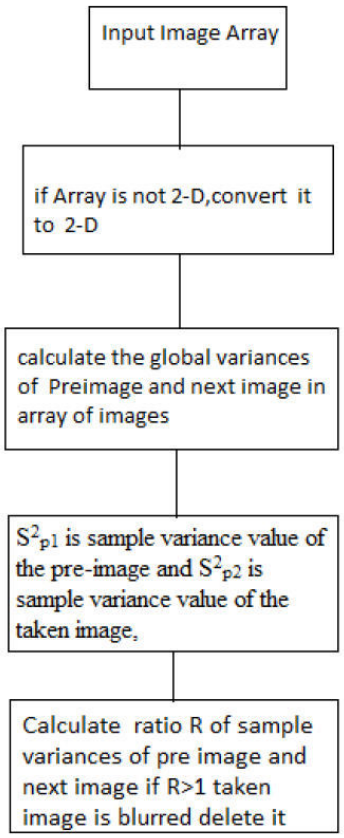


Fig. 3 flow chart for blurr detection algorithm without using transform

In order to estimate images, first apply only one part of the SIFT algorithm, that is, detecting local key points of the images' objects. Then, generate additional images from the given one through the linear diffusion process. And finally, we analyse the variance values calculated for the local key points of the original and its filtered images generated in the scale.

V. CONCLUSION:

From the above overall study of the blurr detection techniques , the blurr detection algorithm without using transform is very accurate and fast than the other two i.e. using DCT and Harr wavelet transform

REFERENCES

[1 http://dl.acm.org/citation.cfm

[2] Wiki Reference: http://en.wikipedia.org/wiki/digital image processing

[3] M. P. Ekstrom, ed., Digital Image Processing Techniques (Academic,Orlando, Fla., 1984).

[4] X. Marichal, W. Y Ma, and H. J. Zhang, "Blur determination in the compressed domain using DCT information,"Proceedings of the IEEE International Conferenceon Image Processing, pp 386-390, 1999.

[5] F. Rooms, and A. Pizurica, "'Estimating image blur in the wavelet domain," ProRISC 2001**,** pp. 568-572.

[6] E. Tsomko ,H.J. Kim and E. Izquierdo: "Linear Gaussian blur evolution for detection of blurry images" IET Image Process., 2010, Vol. 4, Iss. 4 pp. 302–312.

[7] Tong H., Mingjing L., Hongjiang Z., Changshui Z.:'Blur detection for digital images using wavelet transform'. IEEE Int. Conf. on Multimedia and Expo (ICME), 2004, pp. 17–20

❑❑❑

Combined Multi-Modal Biometric and Intrusion Detection System With Statistics Blending in High Security Mobile ADHOC Network

S. Deepan Chakravarthy, P. Infant Kingsly, Mahendran Sadhasivam & C.Jayakumar

Department of CSE, R.M.K Engineering College, Kavaraipettai, ch – 601206
E-mail : sdcdeepan@gmail.com, infantkingsly@gmail.com, mahent11@gmail.com, cjk.cse@rmkec.ac.in

Abstract - The application of multi-modal biometric methods in securing mobile ad-hoc network has been addressed in this paper. A mobile ad-hoc networks is an infra structure less network for mobile devices connected by wireless link. The mobile network is often vulnerable to security attacks even though there are many traditional approaches, due to its features of open medium and dynamic changing topology. Multimodal biometrics is deployed to work with intrusion detection systems to overcome the shortcomings of uni-modal biometric systems. The cluster head is elected in which Dempster-Shafer theory is evaluated in order to increase the observation accuracy to maintain high security and trusted MANET. This system improvises the security aspects by increasing the observation accuracy.

Keywords - *MANET - Mobile Ad-hoc Network, IDS -Intrusion Detection System, ANN Artificial Neural Networks and CA – Certificate Authorities.*

I. INTRODUCTION

The mobile ad-hoc networks (MANET) are becoming more attractive for use in military application. The MANETs are the recent advances in mobile computing and wireless communication. Supporting security – sensitive application in hostile environment has become an important research area for MANETs[1]. A MANET is a self-configuring infra structure less network of mobile devices connected by wireless link. Due to this mobile network is often vulnerable to security attacks. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger internet. In high security MANETs, user authentication is critical in preventing unauthorized user from accessing or modifying network resources. Hence in MANET authentication is done continuously and frequently [3]. User authentication can be performed by using one or more types of validation factors: knowledge factors, possession factors, and biometric factors. Knowledge factors (such as passwords) and possession factors (such as tokens) are very easy to implement but can make it difficult to distinguish an authentic user from an impostor if there is no direct connection between a user and a password or a token. Biometrics technology, such as the recognition of fingerprints, irises, faces, retinas, etc., provides possible solutions to the authentication problem [1]. In addition, intrusion detection systems (IDSs) are important in MANETs to effectively identify malicious activities and so that the MANET may appropriately respond. IDSs can be categorized as follows 1) network-based intrusion detection, which runs at the gateway of a network and examines all incoming packets; 2) router-based intrusion detection, which is installed on the routers to prevent intruders from entering the network; and 3) host-based intrusion detection, which receives the necessary audit data from the host's operating system and analyzes the generated events to keep the local node secure. For MANETs, host-based IDSs are suitable since no centralized gateway or router exists in the network [2].

II. RELATED WORKS:

Certificate Authorities (CA) for authentication in ad hoc mobile networks and proposed a method with multiple certificate authorities CAs based on threshold cryptography [6]. These multiple CAs have secret shares of a Certificate Authority Signing Key (CASK) while no CAs individually know the whole complete CASK, which can be known only when CAs of more than M nodes collaborate. An attacker has to break into a

threshold number of servers in order to get access to the secret key of the service. To prevent compromises of the server, share refreshing is periodically done. This approach has some weaknesses for example nodes that are designated to be servers have to work more than others. It is also difficult for the servers to know the Public keys of all the nodes in an ad hoc mobile network especially if it is large. In popular network authentication architectures, two entities authenticate each other via certificates issued by a trusted certification authority (CA).

The fully-distributed certificate authority extends the idea of the partially-distributed approach by distributing the certificate services to every node [6]. In this approach, after the bootstrapping phase, a new node can join the network at anytime through self-initialization. This node can obtain its own secret share of CASK with the help of M local neighbor nodes. Although this approach enhances scalability and availability, it still depends on an offline authority during the bootstrapping phase [6].

Narasimha pointed out the weakness with Luos' authentication approach that is the secret sharing, based on RSA signature does not provide an important property known as verifiability. They proposed the method for group admission control in peer-to-peer systems which are given a trustable CA. It is based on DSA signature which has verifiability [6].

Hubaux proposed a scheme based on a chain of Public-key certificates, which is scalable and self-organized. Their approach involves issuing certificates by the users themselves without the involvement of any certificate authority [6].

Capkun proposed an authentication method and asserted that, mobility helps security. Their key idea was that, if two nodes are in the vicinity of each other, they can establish a security association (SA) by exchanging appropriate cryptography materials through a secure channel with short transmission range [6].

Seongil pointed that, this direct solution takes a long time because it requires a node to encounter every node that it wants to communicate with. As years go both security issues and authentication methods are improving along the growth of MANET [6].

III. EXISTING SYSTEM:

3.1 Uni-modal biometric approach:

The various component of the networks are sensor (capable of distributing information), node or host. The individual sensor is responsible for validating the user request and respond instantly by the same sensor. The level of observation is minimum. The entire system is working in trust worthy basis node may not be aware of sensor state it blindly accept the resultproduced by the sensor. The two states of the sensors are secure and compromised. During the compromised state sensor will never validate and accept the node blindly. This may results in security breaches.

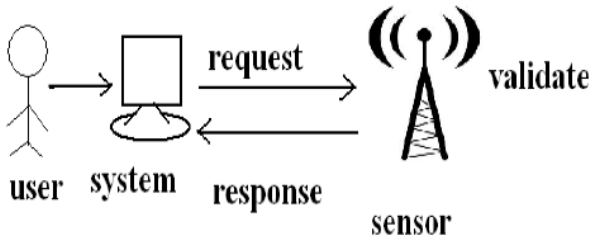


Fig. 3.1: Uni-modal approach

IV. PROPOSED SYSTEM

4.1 Multi – modal biometric approach

Distributed combined authentication and intrusion detection with data fusion in mobile ad-hoc networks (MANETs)[2][4]. Multimodal biometrics are deployed to work with intrusion detection systems (IDSs) to alleviate the shortcomings of uni-modal biometric systems [1][2]. Since each device in the network has measurement and estimation errors, more than one device needs to be chosen, and observations can be fused to increase observation accuracy using Dempster - Shafer theory for data fusion[2][4]. The system decides whether or not user authentication (or IDS input) is required, and which biosensors (or IDSs) should be chosen depending on the security posture. The decisions are made in a fully distributed manner by each authentication device and each IDS [2].

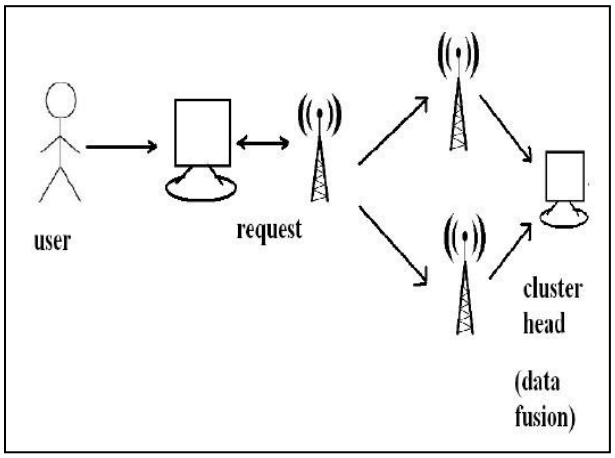


Fig. 4.1 : Multi-modal approach

V. METHODOLOGY USED IN HIGH SECURITY MANET

5.1 Biometric systems includes two kinds of system modals:

1. Identification.
2. Authentication.

The proposed system operates in authentication mode. It works based on a comparison of the matching score between the input sample and the enrolled template within each and every host with a decision threshold, each biometric system outputs a binary decision: accept or reject [1].

5.2 Intrusion detection system

Two main techniques:

- Misuse detection
- Anomaly based detection

Multiple algorithms have been applied to model attack signature or normal behavior patterns of systems [2]. Three common algorithms are

5.2.1 Naive bayes:

A naïve bayes classifier is based on a probabilistic model to assign the most likely class to a given instance[10]. The naive bayes probabilistic model abstractly, the probability model for a classifier is a conditional model

$$P(C \mid F_1, \ldots\ldots, F_n)$$

over a dependent class variable C with a small number of outcomes or *classes*, conditional on several feature variables F_1 through F_n. The problem is that if the number of features n is large or when a feature can take on a large number of values, then basing such a model on probability tables is infeasible. We therefore reformulate the model to make it more tractable.

Using Bayes' theorem, we write

$$P(C \mid F_1, \ldots\ldots, F_n) = \frac{P(C)\,P(F_1, \ldots\ldots, F_n \mid C)}{P(F_1, \ldots\ldots, F_n)}$$

5.2.2 Artificial neural networks (ANN):

The ANNs are very different from expert systems since they do not need a knowledge base to work. Instead, they have to be trained with numerous actual cases. An ANN is a set of elementary neurons which are connected together in different architectures organized in layers what is biologically inspired[10].

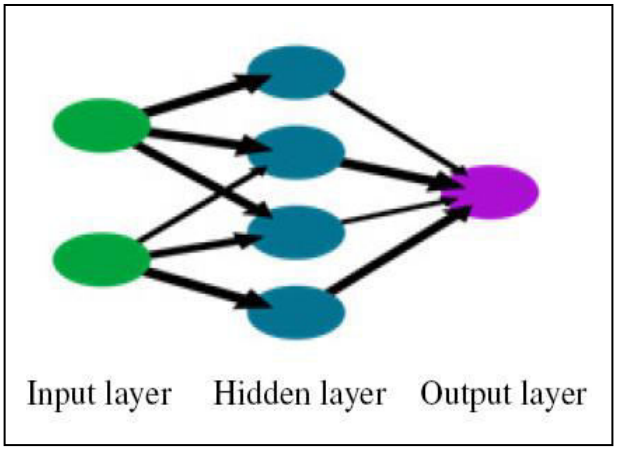


Figure 5.2.2 Neural Network

5.2.3 Decision tree (DT):

- DT, which is a useful machine learning technique, is used to organize the attack signatures into a tree structure.
- A DT takes an object (or) situation described by a se of attributes and returns the predicted output values for the input (i.e) “decision”.

5.3 Data fusion:

In proposed scheme, L sensor are chosen for authenticating and intrusion detection at each time slot to observe the security state of the network. To obtain the security state of the network, these observation values are combined and decision about the security state is made. Sensor might be in either of the state secure or compromised. If so sensor in compromised state they may result in inaccurate assessment. Its quite difficult to ascertain which observer are compromised. Therefore, choosing an appropriate fusion method is critical in our proposed scheme we use Dempster shafer theory for measuring probability of the secured state of sensor node [2][4].

VI. SYSTEM MODEL

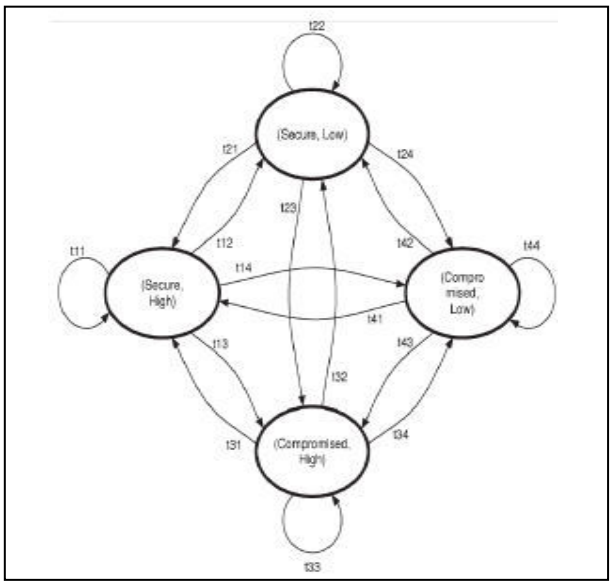


Fig. 6.1 Example of markov chain for a single node's state transition

Transition diagram for sensor states using markov chain model Security states of the sensor are either secure or compromised. Energy state of the sensors is either high or low.

VII. SIMULATION RESULTS

In this section, simulations used to evaluate the performance of the proposed scheme with and without using data fusion. The following simulation scenario: A MANET is equipped with two biosensors for continuous authentication, iris sensor, and fingerprint sensor.

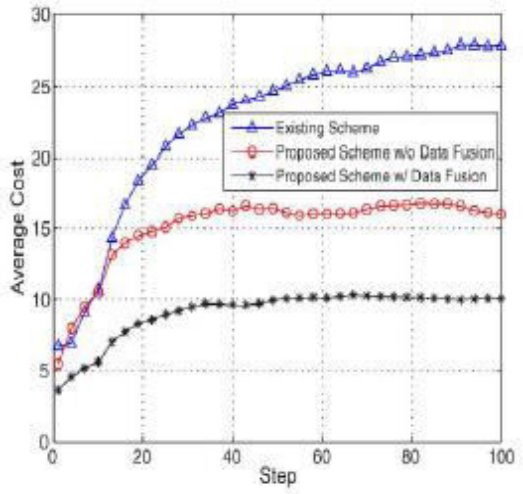


Fig. 7.1 : Cost comparisons

Figure 7.1 shows the cost estimation is done between existing and proposed scheme (with and without data fusion). The cost and networktraffic are directly proportional. In existing system, there are many possibilities of intruder to increases the network traffic. Thus the simulation result predict that cost increases exponentially in powers of 2(twice) when compared to the proposed system.

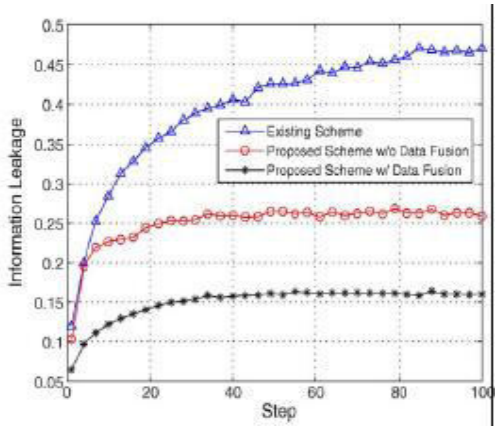


Fig. 7.2 : Information leakage

Figure 7.2 shows the leakage of information to the un-trusted node in both existing and proposed scheme. Due to the less observation the probability of intruder is high in the existing system. The simulation results at 20th step the proportion of information leakage is 0.35(bytes) in existing system and 0.15-0.25(bytes) in proposed system. Each sensor includes two security states, i.e., safe and compromised, and two energy states, i.e., high and low, which means that there are four states for each sensor. The iris sensor is more expensive and also provides more accurate authentication. The fingerprint sensor provides intermediate security authentication and has intermediate energy cost. There is an IDS in the MANET, which uses the least energy and has the least accuracy in detecting the security state.

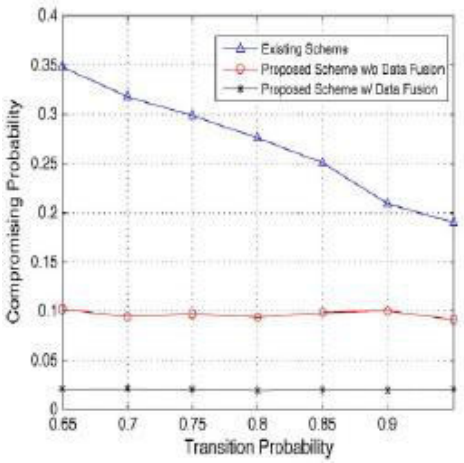


Fig. 7.3 : Network compromise comparisons

Figure 7.3 shows the compromising probability between uni-modal and multi-modal approach. Due to the estimated limitations of biosensors it needs to choose more number of sensors to validate. Since in uni-modal approach one sensor is responsible for authenticating the user the probability of sensor is high. The simulation result at a instant is 0.35 for existing system where as for proposed system is 0.1 probability.

VIII. CONCLUSION AND FUTURE WORK

Combining continuous authentication and intrusion detection can be an effective approach to improve the security performance in high-security MANETs [3][2] . In this paper, distributed scheme combining authentication and intrusion detection is presented. In the proposed scheme, the most suitable biosensors for authentication or IDSs are dynamically selected based on the current security posture and energy states. To improve upon this concept, Dempster–Shafer theory has been used for IDS and sensor fusion since more than one device is used at each time slot[2][4]. The distributed multimodal biometrics and IDS scheduling process can be divided into offline and online parts to mitigate the computational complexity [1]. Further work is in progress to reduce the computation complexity of the proposed scheme by searching for some structured solutions to the distributed scheduling problem. In addition, we plan to consider more nodes' states, such as mobility and wireless channels, in making the scheduling decisions in MANETs.

REFERENCES

[1] Q. Xiao, "A biometric authentication approach for high security mobile adhoc networks" Proceeding of IEEE Information Assurance Workshop, West Point, Newyork, 2004.

[2] Thomas M. Chen and Varadharajan Venkataramanan Southern Methodist University, "Dempster-Shafer Theory for Intrusion Detection in Ad Hoc Networks" IEEE Internet Computing, volume 3, pp 35-41, 2005.

[3] Sheng Zhang, Rajkumar Janakiraman, Terence Sim, and Sandeep Kumar "Continuous Verification Using Multimodal Biometrics" IEEE transactions on pattern analysis and machine intelligence, volume 29, pp 687 – 700, 2007.

[4] Huadong Wu1, Mel Siegel, Rainer Stiefelhagen, JieYang, Robotics Institute, Carnegie Mellon University "Sensor Fusion Using Dempster-Shafer Theory" proceedings of IEEE Instrumentation and Measurement Technology Conference Anchorage, AK, USA, volume 1, pp 7 – 12, 2002.

[5] A. Karygiannis, E. Antonakakis, and A. Apostolopoulos, National Institute of Standards and Technology "Detecting Critical Nodes for MANET Intrusion Detection Systems" Proceedings of the 2nd International Conference on Security, Privacy and Trust in Pervasive and Ubiquitous Computing , 2006.

[6] Godfrey onyait-omoda, Makerere University, "A Framework For Improving Network Security in Ad Hoc Mobile Networks", Computing and Information Technology 2006.

[7] A. Papanikolaou, C. Ilioudis, C. Georgiadis, and E. Pimenidis, "The importance of biometric sensor continuous secure monitoring," Proceeding of 3rd International Conference Digital Information Management, London, U.K, 2008.

[8] Jie Liu, F. Richard Yu, Chung-Horng Lung, and Helen Tang, "Optimal Combined Intrusion Detection and Biometric-Based Continuous Authentication in High Security Mobile Ad Hoc Networks", IEEE transactions on wireless communications, volume 8, pp 35-41, 2009.

[9] V. Krishnamurthy and B. Wahlberg, "Partially observed Markov decision process multiarmed bandits—Structural results," Mathematical operational research, volume 34, pp 30-76, 2009.

[10] Stuart Russell and Peter Norvig "Artificial Intelligence A Modern Approach", 2nd edition Pearson Education publication 2009.

❑❑❑

Development of Data Warehouse for Precision Farming

Kalyani Bhaskar & Sathya K

Department of Computer Science and Engineering, SSN College of Engineering, Kalavakkam, Chennai
E-mail : kalyanib@ssn.edu.in, sathya10197@cse.ssn.edu.in

Abstract - Precision farming is a concept that manages farming based on the observations of intra-field variations and appropriate responses which results in high yield on implementation. Decisions taken in this regard depends on comprehending the relationship between the agro-system and the factors influencing it which can be known by the analysis of the involved data. In this paper, a data warehouse of an agricultural system is developed that is suitable for the analysis of its operational data that can assist in carrying out precision farming methods. The work also attempts to adopt the method of Attribute Oriented Induction for data generalization and analysis. Initial results obtained from the case studies with real time data are presented.

Keywords - *Precision farming, attribute oriented induction, data generalization.*

I. INTRODUCTION

Data warehouses have been an essential source of information for over a decade and half in many organizations belonging to various sectors. Organizations are adopting data warehousing technology in place of traditional database systems as the former helps in data analysis and decision making which is lacking in the latter. Data warehouses facilitate managing on-line analytical processing, mining the data for the embedded knowledge and managing reports thus forming a basis for managing several aspects of an organization. A data warehousing helps in transforming the operational data into useful information. According to W.H. Inmon, a data warehouse is a subject-oriented, integrated, time-variant and nonvolatile collection of data in support of management's decision making process. The four key words distinguish a data warehouse from other data repository systems [1, 2].

Data warehousing as a process involves (i) extracting data from heterogeneous data sources (ii) cleaning and filtering the data for redundancy, missing values, and inconsistencies which is collectively called data preprocessing (iii) transforming the data into a common structure and finally (iv) storing the data in a structured way so that it can be easily accessed for analysis and report generation. Of the above four steps, the first three are collectively referred as extraction, transformation and loading (ETL) of the data.

Clearly, the industry and government sectors benefit a great deal from the development and usage of data warehouses. However, as Inmon points out government agencies have data sources and decision requirements that are significantly different than the industry [3]. The industry uses the data warehouses to increase the profit. To serve and protect the national interests, government demands accurate data analysis through fast access of data and better integration. Agriculture is one of the sectors of national interest.

The increasing population has resulted in a rapidly growing demand for food from the available resources. More than two-thirds of India's population depends on agriculture. The resources themselves are getting depleted due to several factors in India. Consequently, better (optimal) use of resources and management of agro-products are beneficial to India. The primary need is to understand an agricultural system which is gained by comprehending the complex relationships between the system and its influencing factors be it physical, chemical or biological [10]. Having understood the relationships one can develop mathematical models for the analysis of involved data. Once this data is analyzed, it throws light on better farming methods such as precision farming.

Precision farming is a concept that manages farming based on the observations of intra-field variations and appropriate responses which results in high yield on implementation. This scientific farming is based on the analysis of various operational data of observations over the years. Thus there is huge amount of data to be analyzed, which calls for reliable storage and analysis mechanisms. This paper attempts to develop a data warehouse that is suitable to assist in undertaking precision farming methods for better production.

The rest of the paper is organized as follows. Section 2 gives a survey of related works in this field.

This is followed by the explanation of warehouse design or model in section 3. The implementation of the design and case studies with the real time data are presented in the next section. Finally, the work concludes giving directions to future work.

II. STATE-OF-THE-ART

Data warehousing has been used in various domains such as sales and marketing, finance, call center integration, banking and health care [4, 5, and 6]. Recent years have witnessed the development of agricultural data warehouses. Probably, the US agricultural warehouse was one of the first few developed way back in 1997 by USDA_NASS [7, 8] whose goal was to standardize and aggregate the survey data collected by NASS. This brought together data from surveys and census from ranchers, farmers, agri-businesses and secondary sources.

The authors in [9] have explained the conceptual and logical models for data storage. The work presents a comparison of models in terms of efficiency, reusability, flexibility, complexity and redundancy. These measures will be useful in designing better data warehouse for the analysis. The data warehousing application is implemented using Microsoft OLAP server for sales and shipping systems.

A government data warehouse on pests, pesticides and meteorological data for the government of Pakistan is reported in [10]. Recently, Shree Nilakantha et.al have discussed the dimensional issues in developing a data warehouse for agricultural sector [11]. The authors have used star schema that is most popular to develop the warehouse and have shown that aggregation can be carried out using multidimensional model. The data warehouse [12] houses the various survey and census data that has been collected according to time and location dimensions. From this data model, OLAP analysis are explained with the increase or decrease of the livestock population, yield of the crop, water supply for domestic and irrigation purposes. The INARIS data warehouse is implemented and can be accessed by authorized web users.

AGRISOL_R [13] is a multidimensional data model that uses snowflake schema design to analyze the soil type, soil texture, micro nutrients in the soil to determine the soil quality for cropping system. This model uses various OLAP operations for soil properties to determine its quality without analysis. While AGRIC [14] describes the soil databases with soil profile, soil chemical property and soil classification. The authors have analyzed various soil type, texture, pH and electrical conductivity.

The soil nutrients content is another important factor for the growth of plants, yield and human health. In [15], the authors explain the effect of effluents from the tannery industries on soil macronutrients, plant growth and human health.

The next section describes the proposed design of the data warehouse for agricultural data.

III. PROPOSED METHODOLOGY

In this section, we explain the detailed workflow for designing a data warehouse for precision farming with system architecture. This helps us to implement the construction of multidimensional data model with OLAP operations that includes analysis and visualization techniques.

A. System architecture

Figure 1 shows the block diagram of the system design with various modules for building warehouse and using it for analysis and reporting. A brief description of these modules is presented here.

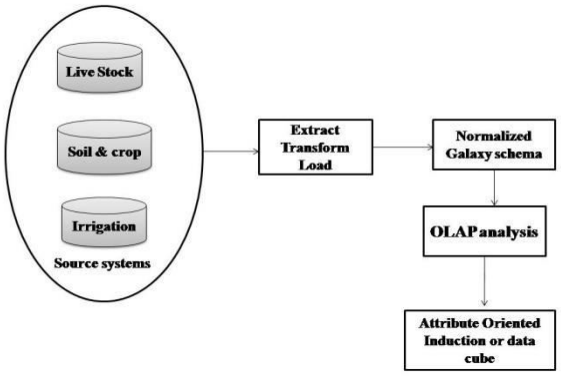


Fig. 1: System architecture for data warehouse design

1) Data collection

Indian agriculture is mainly concerned with varying factors such climate, soil, plantation crops, fertilizer applied, pesticides sprayed, water resources, and livestock. These heterogeneous data are mostly stored in log books, excel sheets, etc.

2) Extraction Transform Load

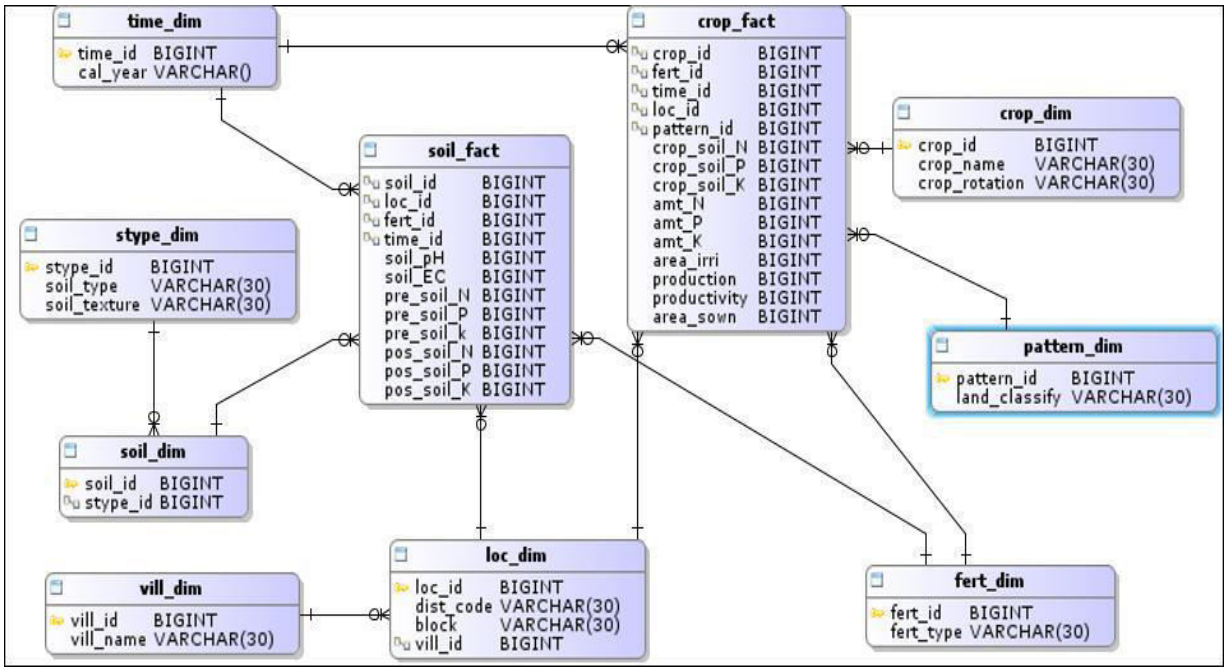
Extraction of data from different sources is a challenging task to perform as the data is stored in different file formats. It can be in excel sheet, comma separated values and text files from different locations. Building a dynamic procedure is an efficient way to perform ETL and it is helpful in integrating data from source systems to the targeted schema design.

3) Schema design

Data warehouse design is based on multidimensional model [1] for analytical processing with respect to time and location dimensions. The representation can adopt different schema designs such as star schema, snowflake schema or galaxy schema.

a) Star schema : Initially common data warehouse design uses star schema for OLAP analysis. So in order to design multidimensional cube and also to achieve the concept hierarchy, normalization to dimension tables is applied and thus star schema becomes snow flake schema

b) *Snow flake:* In snowflake schema, dimensions are in normalized form and thus it avoids the problem of data redundancy. The soil classification and cropping system uses the snowflake schema in the proposed data warehouse.



c) *Galaxy schema* **:** is a collection of star schema and is also called as fact constellation consists of more than one fact table connected with the commonly shared dimension tables.

d) *Normalized galaxy schema:* is the collection of snowflake schema as shown in figure 2. The soil classification and crop system uses the snowflake schema and both the schema has commonly shared dimension tables such as time, location and fertilizer dimensions. Thus it becomes normalized galaxy schema.

4) *OLAP analysis*

From the normalized galaxy schema, multidimensional cube is constructed and thus results are analyzed for different data. The analysis can be performed by using different aggregate functions and group-by operator. SQL statements include different in-built aggregate function such as count, sum, max (maximum), min (minimum), and avg (average). It is also observed that the number of joins increases as the schema gets complicated.

5) Attribute Oriented Induction

Attribute oriented induction is the query oriented, generalization based online analytical processing and thus the visualization can be achieved by using cross tabs, different charts. This overcomes the dimensionality issue from the data cube construction through generalization and analysis. The attribute oriented induction aims to collect the data relevant to data cube using the data base query. This fetches the relational table and takes as initial table to perform the generalization. The generalization method is given by the two rules (attribute removal and attribute generalization).Implementation and analysis of the operational data with this design is presented in the next section.

IV. IMPLEMENTATION AND ANALYSIS

The data warehouse is implemented using Oracle 11g, which is an open source software available. For this study, agricultural data for Dindigul district in Tamil Nadu has been chosen. The district consists of the following agricultural divisions: Dindigul, Natham, Nilakottai, Palani, Oddanchatram and Vedasandur. Data from different agricultural resources [16] are collected and stored into the relational tables.

The data from different sources are extracted and stored into the external tables. In this study, data for the soil and crop schema designs are populated from the csv (comma separated values), text and excel files using SQL programming. Then it is transformed from source to target by mapping the corresponding attribute in a schema and finally the data is loaded into the warehouse.

The data warehouse adopts normalized galaxy schema design for implementation. Figure 3 shows the query to list the information on soil, crops and macro ingredients.

A. OLAP analysis:

The fertility of soil can be determined by the land classification (dry lands, wet lands and garden lands), soil type (black, red, and alluvium soil), soil texture (sandy clay loam, loam and clay loam), pH, electrical conductivity, macronutrients and micronutrients which are the most essential factors for plant growth at all stages. This analysis can be performed according to the nutrient content recommended for different crops with the soil macronutrient present in the soil such as Nitrogen (N), Phosphorus (P) and Potassium (K) and explains the increase in the soil fertility after applying the fertilizer. The study is carried to assess the quantum of macronutrients present in the soil and deficiency of nutrient problems is also explained according to the essential nutrient needed by the different crops. The various calculations used to find the necessary/excess content of NPK in the soil with the recommended crop NPK is given as follows

```
SELECT
L.block, S.soil_type, S.soil_texture, T.cal_year, V.vill_id, V.vill_name, C.crop_id,,
C.crop_name, C.crop_duration, P.land_classify, FS.soil_pre_N, FS.soil_pre_P,
FS.soil_pre_K, FS.soil_pos_N, FS.soil_pos_P, FS.soil_pos_K, soil_crop_N, soil_crop_P, soil_crop_K
FROM
galaxy_soil FS, galaxy_crop FC, soil_sdim ST, stype_sdim S, loc_scdim L, vill_scdim V, fert_scdim F,
time_scdim T, crop_cdim. C, pattern_cdim P
where
ST.soil_id=FS.soil_id and S.stype_id=ST.stype_id and L.loc_id=FS.loc_id and
V.vill_id=L.vill_id and F.fert_id=FS.fert_id and T.time_id=FS.time_id and
L.loc_id=FC.loc_id and F.fert_id=FC.fert_id and C.crop_id=FC.crop_id and
P.pattern_id=FC.pattern_id
group by
(L.block, S.soil_type, S.soil_texture, T.cal_year, V.vill_id, V.vill_name, C.crop_id, C.crop_name,
C.crop_duration, P.land_classify, FS.soil_pre_N, FS.soil_pre_P, FS. soil_pre_K, FS.soil_pos_N,
FS.soil_pos_P, FS.soil_pos_K, soil_crop_N, soil_crop_P, soil_crop_K);
```

Let N_r, P_r, K_r represent the recommended values for the crops, N_{pref}, P_{pref}, K_{pref} represents the soil values before applying fertilizers, N_{pf}, P_{pf}, *and* K_{pf} represent the soil values after applying fertilizers. The amount of NPK is measured by parts per million (ppm) units. Then the calculation is given by

$$N_r - N_{pref} = \Delta N \quad (1)$$

$$P_r - P_{pref} = \Delta P \quad (2)$$

$$K_r - K_{pref} = \Delta K \quad (3)$$

Case study:

The analysis is performed for different land type such as dry lands, wet lands and garden lands in two blocks of Palani Division which under the Dindigul district. Here the block 1 represents Oddanchatram and block 2 represents Palani. From the equations 1, 2 & 3 the analysis determines the necessity of fertilizers or to reduce the excess amount of nutrient according to the recommended crop NPK. Here the analysis is performed for the crop Bajra and recommended crop NPK is given as (23, 4.5, and 321). These values are averaged over the period of plant growth up to the yield.

Case 1: if Npref>= Nr then ΔN is positive:

Positive values of ΔN, ΔP or ΔK indicate the need for applying fertilizers. From the table 1 P_r= 4.5 P_{pref} =3.7 substitute it in equation (2) then 4.5-3.7=0.8 determines that the phosphorus content should be increased by 0.8 ppm for growing Bajra in the year 2005.

Table 1: Recommended crop NPK, pre-soil NPK for Plant Bajra for block 1.

Year	N_r	P_r	K_r	N_{pref}	P_{pref}	K_{pref}
2005	23	4.5	321	44	3.7	200
2006	23	4.5	321	49	4.2	256
2007	23	4.5	321	49	4.8	165
2008	23	4.5	321	43	5.7	135
2009	23	4.5	321	53	6.6	150

Table 2: Re commended values for Post-soil NPK

ΔN	ΔP	ΔK
-21	0.8	121
-26	0.7	156
-26	09	71
-20	-1.2	186
-30	-2.1	171

Case 2: if Npref < Nr then ΔN is negative

When ΔN is negative, it means that the soil is having the required amount of N and application can be done at a later date. This necessitates soil monitoring. From the table 1 & 2 substitute N_r = 23, N_{pref} =44, in equation (1) then 23-44= -21. It means that the Nitrogen content in the soil should be reduced by 21 ppm. A similar argument holds good for P and K values. Similarly these calculations have been done for all crops that are grown in the different land types. These analyses can be expressed by using different graphical representation as shown below.

In figure 4 it can be observed that the nitrogen content is available in excess than recommended for growing the crop Bajra in the dry lands which come under the Oddanchatram block.

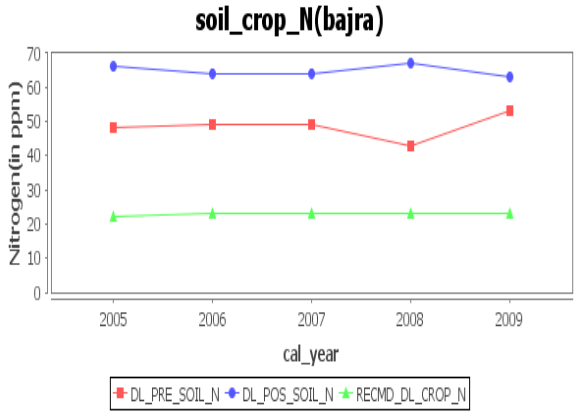


Figure 4 : Soil–crop analysis of Nitrogen content in the Bajra plant (DL) from 2005-2009

Figure 5 shows the deficiency of phosphorus contents available for growing Bajra in the dry lands before the application of fertilizers. However, the post fertilizer application values are higher than the required thus indicating that this can be controlled.

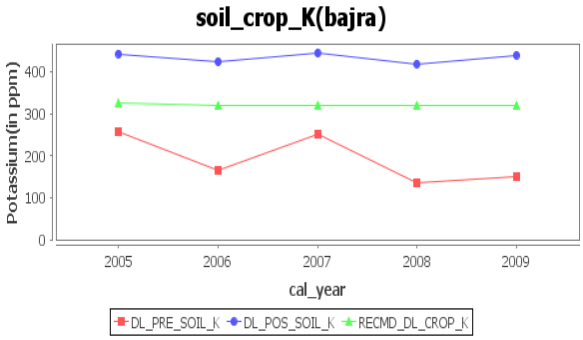


Fig. 6: Soil–crop analysis of Potassium content in the Bajra plant (DL) from 2005-2009.

Thus the analysis can be performed by the multidimensional cube. The data cube suffers the curse of dimensionality. To overcome this issue, attribute oriented induction is performed.

B. Attribute Oriented Induction or data cube

Attribute Oriented Induction is the visualization technique used in this study. Here the table describes that the attribute oriented induction is performed on the initial table. Every attribute in the relational table is preceded with generalization concept and decides the attribute removal and retention. The attribute as shown

in the table 2 discusses the attribute oriented induction performed in it.

Table2. Initial relation table to perform attribute oriented induction

Year	*Block*	*Vid*	*Cid*	*Land types*	N_{pref}	P_{pref}	K_{pref}	N_{pf}	P_{pf}	K_{pf}	N_r	P_r	K_r
2006	ODC	20139	91140	Dry	49	4.8	165	64	7.3	424	23	4.5	321
2007	ODC	20176	91177	Garden	56	4.2	265	64	7	440	23	4.5	321
2008	Palani	13566	50145	Wet	89	82	229	96	9	264	23	4.5	321
2009	ODC	20114	91115	Dry	48	4.2	256	66	7.3	443	23	4.5	321

Table 3: Generalized tables for the attribute oriented induction

Year	*Block*	*Land types*	N_{pref}	P_{pref}	K_{pref}	N_{pf}	P_{pf}	K_{pf}	N_r	P_r	K_r
2006	ODC	Dry	49	4.8	165	64	7.3	424	23	4.5	321
2007	ODC	Garden	56	4.2	265	64	7	440	23	4.5	321
2008	Palani	Wet	89	82	229	96	9	264	23	4.5	321
2009	ODC	Dry	48	4.2	256	66	7.3	443	23	4.5	321

Year: Time dimension is essential attribute to distinguish the variation of the data from 2005-2010. Thus the calendar year attribute is retained and performed an attribute oriented induction.

Block: There are only few distinct blocks that come under Dindigul district. So the attribute is retained and there is no generalization operation defined on it

Vid: There is large number of distinct values present in the attribute and then generalization is not performed .so the attribute is removed.

Cid: There is large number of distinct values present in the attribute and then generalization is not performed .so the attribute is removed.

Land types: This attribute has only three distinct classifications such as dry, wet and garden lands so the attribute is retained and no generalization operation is performed on it.

N_{pref}, P_{pref}, K_{pref}, N_{pf}, P_{pf}, K_{pf}, N_r, *Pr, and* K_r: These attribute has different numerical value and thus can be used for generalization for further analysis purpose. Finally the generalized relational table is obtained by the implementation of attribute oriented induction on the data is given in the table 3

1) Visualization of generalized table by the attribute oriented induction: The resulting generalized table can be presented in different forms of visualization such as cross–tabulations, bar charts and pie charts. Attribute values are grouped in the cross-tabs implementation.

The cross–tabs visualization for Bajra grown in the dry lands are grouped together with different blocks for the year 2006 and are given in table 4 from the generalized table.

Table 4: Cross –tabs implementation for the crop Bajra in the Dry_lands

The data for the Bajra crop grown in the dry lands for the year 2006 representation in cross- tabs visualization can be transformed into the 3D charts as shown in figure 7

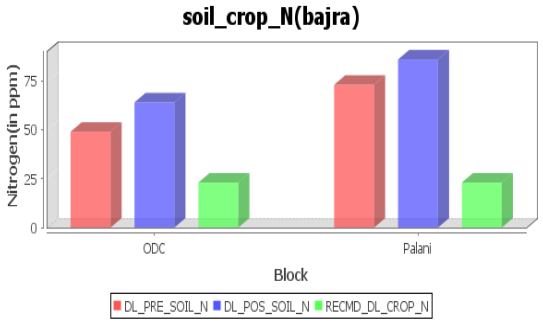


Fig. 7: Pre-post soil NPK and crop NPK for Bajra crop in the blocks of Palani and Oddanchatram in the year 2006.

V. CONCLUSION

This paper presents the normalized galaxy schema design for precision farming and also analyses the data for the quantum of macro ingredients of the soil with respect to that required by the plant. The analysis is done for different data with respect to time and location

dimensions. The results obtained from analysis will be helpful to the farmers for taking decision to improve the yield with respect to the presence of soil nutrients and also address the drawbacks in the method of farming techniques. This will create awareness among farmers to support scientific farming and also gives importance to the sustainable agriculture for future world. The construction of the multidimensional data cube suffers with the curse of dimensionality. In order to reduce the problem, attribute oriented induction is performed. The results can be viewed and analyzed through cross tabs visualization and different graphical format. The work presents the initial results in designing and testing the agricultural warehouse.

VI. FUTURE WORK

The future work involves handling of spatial images includes how to store images like Maps and also to perform SOLAP operations efficiently. Importance of precision agriculture which gives more yields can be compared with existing agriculture methods. Finally Warehouse design can be deployed in web for end users.

REFERENCES

[1] Han J., and Kamber M., Data Mining: Concepts and Techniques, Morgan Kaufmann, ISBN: 1-55860-489-8, 2000.

[2] Inmon W.H., Building the Data Warehouse, 3rd Edition, John Wiley, ISBN: 0-471-08130-2, 2002.

[3] W.H. Inmon, "Data warehousing from government", 2005.

[4] Vidette Poe, Patricia Klauer and Stephen Brobst, Building a data warehouse for decision support: 2nd Edition (Prentice Hall, 1998)

[5] S. Chaudhuri, and U. Dayal, An overview of data warehousing and OLAP technology: ACM SIGMOD Record, 26:6574, 1997.

[6] Mark Humphries, Michael W. Hawkins, Michelle C. Dy, "Data Warehousing: Architecture and Implementation", Prentice Hall, 1999.

[7] M. Yost and Jack Nealon, Using a dimensional data warehouse to standardize survey and census metadata: National Agricultural Statistics Service, U.S. Department of Agriculture, Fall 1999.

[8] National Agricultural Statistics Service: www.nass.usda.gov/

[9] Deepti Mishra, "A case study of data models in data warehousing"

[10] Ahsan Abdullah, M. Farooq Khan, Muhammad Umer, Stephen Brobst," The case for an agri data warehouse: enabling analytical exploration of integrated Agricultural data", in proceedings of The IASTED International Conference on Databases and Applications (DBA) 2004.

[11] Sree Nilakantaa, Kevin Scheibea, Anil Rai, "Dimensional issues in agricultural data warehouse design", Elsevier, Computers and electronics in agriculture, vol. 60, 2008.

[12] INARIS: http://www.inaris.gen.in/

[13] Constanta Zoie Radulescu, "A Multidimensional Data Model for Analysis of Agricultural Soil Characteristics", CANS'08, 2008

[14] Leisa J. Armstrong, "The application of data mining techniques to characterize agricultural soil profiles", In Proc. Sixth Australasian Data Mining Conference (AusDM 2007).

[15] Baby Shakila P (2010), "Effect of tannery effluent on water and soil profile, Plant growth and human health" Doctor of Philosophy Thesis, Avinashilingam Deemed University for Women, Coimbatore.

[16] Data centers: Agricultural extension Office, Palani, Statistical department, Collectorate Campus, Soil testing lab, Dindigul, Panchayat Union office, Oddanchatram

❑❑❑

Mobile Rover Enchiridion Using Android Mobile Application

S.Venkatasubramanian, G.N.Vijay Kumar, N.Suresh & C. Jayakumar

Department of CSE, RMK Engineering College, Kavaraipettai
E-mail : venkatasubramanian18@gmail.com, vijaykumargn1211@gmail.com, srs.yan@gmail.com, cjk.cse@rmkec.ac.in

Abstract - Information about the location, orientation, and context of a mobile device is of central importance for future multimedia applications and location-based services (LBSs). With the widespread adoption of modern camera phones, including powerful processors, inertial measurement units, compass, and assisted global positioning system (GPS) receivers, the variety of location and context-based services has significantly increased over the last years. Satellite navigation systems can provide sufficient positioning accuracy and a clear view. In current tourism system, whenever a tourist visits famous spots, to know more about the place he hires a guide. The hired guide then narrates history of the place. The proposed system does not require a physical guide. The Mobile application installed on the mobile of tourist can act as a guide. The application would help user to find out the weather forecast of the place. The mobile application has many modules. Location finder is responsible to retrieve user's current latitude and longitude using GPS. This will convert the coordinates into street address using geocoding technology. Video Search is responsible to do video search using Google search engine. The result of the search is list of videos related to the user's current location. Video player is responsible to play the video which user selects. Weather Forecast is responsible to retrieve the weather information from Google and display it to user. Routes information (train and bus) can also be obtained from the Google search and display it to user.

I. INTRODUCTION

Mobile Computing is a variety of wireless devices that has the mobility to allow people to connect to the internet, providing wireless transmission to access data and information from where ever location they may be. For example, Mobile devices [5]. The purpose is to ease the task of a traveler and to help the user with mobile application to act as a guide instead of hiring a physical guide. It is a standalone application developed for Android mobiles [10]. The application "Mobile Rover Enchiridion" solves all these problems (Have you ever gone to tour, and wished to get information of the place in your mobile? Check out the videos which explain the history/information of the place you are currently visiting? Quickly get the weather forecast for the place?). It offers many services such as Retrieves the user's current geological coordinates, Converts the Latitude/longitude to street address, Does video search for that place and displays those to user, User watches the video of his choice and Gets the weather forecast for the place.

Android is a free open source mobile platform. Android is a software stack for mobile devices that includes an operating system, middleware and key applications. The Android SDK provides the tools and APIs necessary to begin developing applications on the Android platform using the Java programming language [10].

The Global Positioning System (GPS) is a space-based global navigation satellite system that provides reliable location and time information in all weather and at all times and anywhere on or near the Earth where there is an unobstructed line of sight to four or more GPS satellites. It is maintained by the United States government and is freely accessible by anyone with a GPS receiver [1] [7].

A mobile application based on Location Based Services (LBS) using GPS as a location provider. This design implements a client-server system that helps users to locate their family members and receive alerts when friends are nearby. In this application the server receives the user's locations and alerts two friends if they are in the same location. The server was designed in PHP to overcome the server load. This information serves as a reference in developing Android Mobile application [1] [10].

The methodology to track and identify the location information both indoor and outdoor with room level accuracy uses accelerometer, digital compass, Wi-Fi and GPS technology to identify the location information both indoor and outdoor. This idea of GPS technology has been used to identify and provide location information using geocoding technique [2] [7].

A dedicated framework that supports mobile applications for GPS enabled mobile phones by

adjusting platform parameters for application performance uses "critical point" algorithm. This framework enhances the performance of the application by conserving the battery power. It used HTTP (Hyper Text Transfer Protocol) to transfer application data and UDP (User Datagram Protocol) to transfer location data. These ideas have been used to transfer location data updates from mobile phone to the YouTube server [3] [1] [7].

A Digital Travel System using the Network Service Platform framework system records travel logs using location data obtained from GPS and image files taken by a camera device. This framework NSP provides the ability to integrate robot services and internet services because it uses RSNP (Robot Service Network Protocol) an open protocol for providing robot services. These ideas are used to obtain necessary information about the GPS and Geocoding technique [4] [7].

II. SYSTEM ARCHITECTURE

Entire application is built using Android technology for getting location (longitude and latitude) of the user [10].

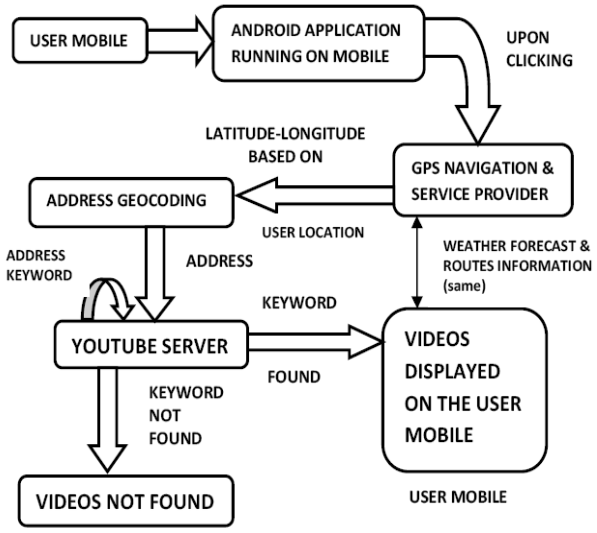


Fig. 1 : Overall Architecture

Fig. 1 represents the overall architecture of the system. This architecture provides information about the modules to be used for developing the application.

The mobile application has below modules

- **Location finder**

This module is responsible to retrieve user's current latitude and longitude using GPS navigation. This will convert the coordinates into street address using geocoding technology.

- **Video Search**

This module is responsible to do video search in YouTube server using the keyword. The result of the search is list of videos related to the user's current location [11].

- **Video player**

This module is responsible to play the video which user selects and it is displayed on the user mobile.

- **Weather Forecast**

This module is responsible to retrieve the weather information from Google and display it to user [12].

- **Routes Information**

This module is responsible to retrieve the routes information based on the bus route and train route from Google and display it to user.

- **Settings**

This module allows user to set some settings for the applications.

III. EXISTING SYSTEM

The existing system is having lot of web applications which provide information of the location but user have to manually login and search the details [7] [8].

Separate systems are only available for the below existing system

- GPS Navigation
- YouTube videos
- Weather forecasting
- Bus or Train information

These existing systems take more time to identify the place where the user visits. Consumption of time prevails in this existing system.

Now there is an existing android powered mobile application namely travel guide. But this application is implemented for only a particular city which contains only the pictures and history about the place as a document [4].

YouTube video application is available where the user clicks the application and manually enters the keyword to search for videos [3].

Weather forecast application is available in which a user can only know about the weather forecast of the place [12].

Bus or Train information application provides with data based on the bus or train information.

So these separate systems may cause more time consumption and makes the user feel difficult to use.

IV. PROPOSED SYSTEM

In the proposed system it contains design and implementation of the applications as a combined one namely "Mobile Rover Enchiridion".

It contains the combination of five applications into one which provides the user with less time consumption.

The proposed system provides the user with a single application (app) which the user feels convenient and helpful during the travel or visiting places.

Complexity is reduced as all the process will start by itself which the user needs just to click and select for some options alone.

The proposed system includes geocoding technique which is the root for all the three process (Weather forecast, YouTube videos, GPS, Routes information) to execute simultaneously in fetching the information.

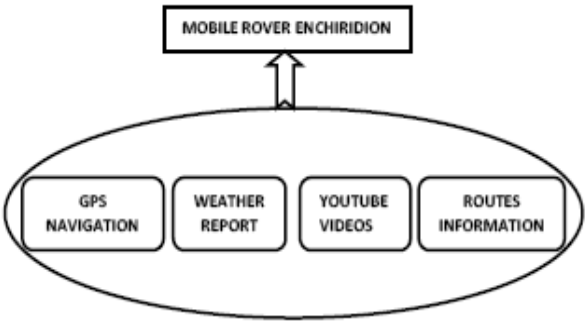


Fig. 2 : A Simple diagram representing the Proposed System

V. PRODUCT PERSPECTIVE

The Mobile Rover Enchiridion is an application under the domain mobile computing. The mobile computing is a domain which has larger scope, vast development and evolution. This is an application developed for only Android powered mobiles [10]. The application provides complete information along with the related videos of that place where the user visits. It makes the user to travel in an easy way and helps the user as a guide instead of hiring a guide. The existing system has separate applications for navigation, weather forecasting, video search, video player information on bus and train. This is a product which is self-contained of the above existing products.

VI. USER CLASSES AND CHARACTERISTICS

The users can easily access this application in an android powered mobile. This application can be kept in the android powered mobile in its home page. The user with less knowledge to browse the content of the mobile can make use of this. This application can be accessed using a single touch as most of the android powered mobiles have touch screen. Users with basic knowledge for operating an android mobile can access the application by knowing the basic information from the internet. It is portable hence it can be carried anywhere.

VII. RESULTS

The result shows as the application which contains the weather forecast, video search and location of the user with his mobile. It provides the accurate location where the user resides and provides the user with useful information about the place.

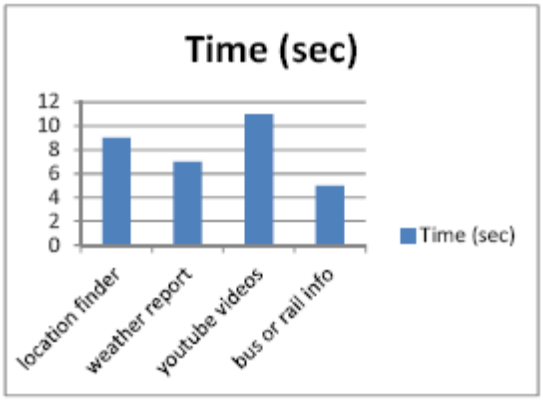


Fig. 3 : Time complexities of location finder, weather forecast and videos loading in 2-G mobile phones

Figure 3 shows the time complexities of location finder app, weather forecast app, videos loading (YouTube app), bus and train information in 2G mobiles phones. The time consumption is more for loading videos which is mostly from YouTube which takes approximately 11 seconds to load. The location finder provides the user with location where the user resides which takes approximately 9 seconds to load and display it to user. The weather forecasting takes approximately 7 seconds to display the user with weather report of the place [9]. The bus or train information applications take 5 seconds to display it to user.

Figure 4 shows time complexities of location finder application, weather forecast app, videos loading (YouTube app), bus and train information in 3G mobile phones. These comparisons show the different time consumption by these applications.

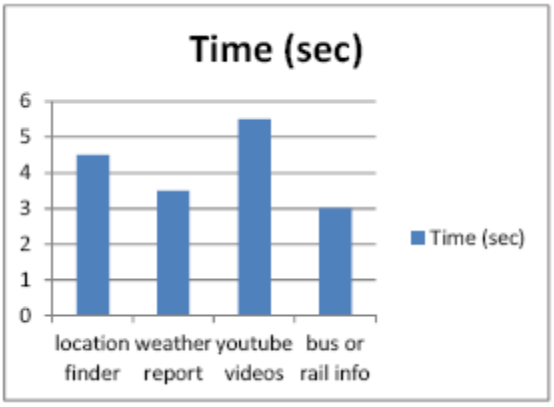


Fig. 4 : Time complexities of location finder, weather forecast and videos loading in 3-G mobile phones

3G connection provides a very good speed for browsing and for making even a video calls. Although it is slow in our India due to lack of signal towers for providing the service [5].

These applications run separately by manual operation of the user using the applications. The time consumptions of location finder reduced to approximately 4.5 seconds, weather forecast reduced to approximately 3.5 seconds and video loading from YouTube is reduced to 5.5 seconds and bus or train information app time is reduced to 3 seconds when compared with 2G mobiles.

Figure 5 represents the comparison figure of time complexities between individual applications and Mobile rover enchiridion which is the combination of all the five applications.

It depicts that the time complexity of mobile rover enchiridion application is less compared to the other individual applications.

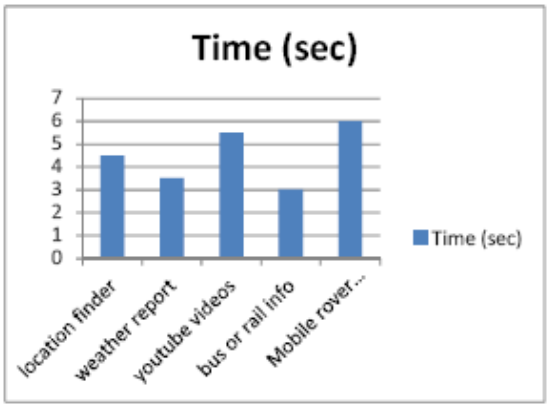


Fig. 5 : Comparison of time complexities between individual applications and Mobile rover enchiridion (integrated application)

Mobile rover enchiridion application will take maximum of 6 seconds to display the user with location where the user uses the application, weather forecast report about the place and finally it displays the related videos and bus and train information about the place. User selects the videos which takes again a minute to run the videos. This comparison is done for android mobiles using the 3G connections [5].

From this the performance measure of the mobile rover enchiridion is better than the individual applications as each application takes a lot time and the combined application takes less time to fetch all these information regarding the place the user visits.

VIII. CONCLUSION AND FUTURE WORKS

The main aim is to implement an app that consists of five apps into one application. By doing this the user may feel easy to access the application via internet. Just a touch is required to operate the app. This application mobile rover enchiridion will provide the user with the weather forecast, street address, YouTube videos, Bus and train information. Thus the user may get the information about the area he visits. This single app can do five apps job. Hence it has less time consumption and also makes the user to understand very well about the place he visits without any physical guide.

Future work may include a separate video server has to be maintained for this application for the maintenance and retrieving the correct street address videos using the geocoding technique. And further enhancement as per the user comments on the application can be done.

REFERENCES

[1] Ghaith Bader Al-Suwaidi and Mohamed Jamal Zemerly , “Locating Friends and Family Using Mobile Phones With Global Positioning System (GPS)” , Proceedings of IEEE/ACS International Conference on Computer Systems and Applications (AICCSA), pp. 555-558, August 2009.

[2] Yohan Chon and Hojung Cha, “Life Map: A Smartphone-Based Context Provider for Location-Based Services” Journal of IEEE Pervasive Computing, volume 10, no.2, pp. 58-67, June 2011.

[3] Sean J. Barbeau, Rafael A. Perez, Miguel A. Labrador, Alfredo J. Perez, Philip L. Winters and Nevine Labib Georggi, “A Location-Aware Framework for Intelligent Real-Time Mobile Applications” Journal of IEEE Pervasive Computing, Volume 10 Issue 3, July 2011.

[4] Soichiro Ushio, Yuka Ito, Kazunori Okada, Tomoki Kitahara, Hidenori Tsuji,Satoko Moriguchi, Masahiko Narita and Yuka Kato, "The Digital Travel Diary System using the Network Service Platform" Proceedings of International Conference on Advanced Information Networking and Applications, 2011.

[5] Y. Zhao, "Standardization of Mobile Phone Positioning for 3G Systems," IEEE Communication Magazines, volume 40, no. 7, pp. 108–116, 2002.

[6] Georg Schroth, Robert Huitl, David Chen,Mohammad Abu-Alqumsan, Anas Al-Nuaimi, and Eckehard Steinbach, "Mobile Visual Location Recognition" IEEE Signal Processing Magazine, July 2011.

[7] Khondker Shajadul Hasan, Mashiur Rahman, Abul L. Haque,M Abdur Rahman, Tanzil Rahman and M Mahbubur Rasheed, "Cost Effective GPS-GPRS Based Object Tracking System" Proceedings of the International MultiConference of Engineers and Computer Scientists(IMECS), volume 1, pp. 398-402, March 2009.

[8] Eric Abbott and David Powell, "Land-Vehicle Navigation Using GPS" Proceedings of the IEEE, Volume. 87, No. 1, January 1999.

[9] S.S.Jadhav, R.A.Deshmukh, S.M.Sangve, M.B.Salunke, "Mobile Location Tracking using GSM" Journal of IEEE Advanced Engineering & Application, January 2010.

[10] http://developer.android.com/.

[11] http://maps.google.com/street/ view.

[12] http://in.weather.com/.

❑❑❑

A Design of Swarm Intelligence Based on Intrusion Detection System

M. Sathya & R. Jayabhaduri

Computer Science and Engineering, Sri Venkateswara College of Engineering, Chennai, India
E-mail : Sathyame84@gmail.com, jaya@svce.ac.in

Abstract - Nowadays the security of Web applications is one of the key topics in Computer Security. Among all the solutions that have been proposed so far, the analysis of the HTTP payload at the byte level has proven to be effective as it does not require the detailed knowledge of the applications running on the Web server. The solutions proposed in the literature actually achieved good results for the detection rate, while there is still room for reducing the false positive rate. To this end, in this paper we propose HMMPayl, an IDS where the payload is represented as a sequence of bytes, and the analysis is performed using Hidden Markov Models (HMM).This paper explores the various classification of server overloading with false URL and Recursive Machine Interference and Prankster searching at extensive key lengths, and try to Firewall the unauthorized server accessing. The algorithm we propose for feature extraction and the joint use of HMM guarantee the same expressive power of n e gram analysis, while allowing to overcome its computational complexity. In addition, we designed HMMPayl following the Multiple Classifiers System paradigms to provide for a better classification accuracy, to increase the difficulty of evading the IDS, and to mitigate the weaknesses due to a non optimal choice of HMM parameters. A manual Overriding of these algorithms will be granted for a single use after a Proper Security Verification, This will make the System Flexible for Emergency Utilization.

Keywords - *Intrusion Detection System, Anomaly detection, Particle Swarm Optimization, Payload analysis.*

I. INTRODUCTION

The protection of Web applications is challenging, because they are in general large, complex, highly customized and often created by programmers with poor security background. On the other hand, a requirement that a tool to protect Web applications is desired to meet is being as autonomous as possible, i.e., it should not require extensive administration overhead. Several hardware and software solutions have been developed, and are available on the market. Among these , Web Application Firewalls are one of the most frequently used protection tools. Typically, they rely on a set of rules written by the administrator, who therefore must have an in-depth knowledge of the applications to be protected.. Our original contribution is a system design which is resilient to the noise in the training set, where the noiseis made up of attacks. Our system not only is able to effectively model the legitimate traffic, but also to detect attacks that are similar to the *noise* in the training set.To this end, we optimise IDS parameters on the basis of the fraction of non-legitimate queries we expect in the training set. Experimental results show that even a raw estimate for this parameter can effectively enhance the detection rate, with a small amount of false positives.

An intrusion is defined by “Heady“ as any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource. An earlier study done by Anderson uses the term “threat" in this same sense and defines it to be the potential possibility of a deliberate unauthorized attempt to access information, manipulate information, or render a system unreliable or unusable .An intrusion is a violation of the security policy of the system. The definitions above are general enough to encompass all the threats mentioned in the previous section. Any definition of intrusion is, of necessity, imprecise, as security policy requirements do not always translate into a well-defined set of actions. Whereas policy defines the goals that must be satisfied in a system, detecting breaches of policy requires knowledge of steps or actions that may result in its violation.

Detecting intrusions can be divided into two categories: anomaly intrusion detection and misuse intrusion detection. The first refers to intrusions that can be detected based on anomalous behavior and use of computer resources. For example, if user X only uses the computer from his once between 9 AM and 5 PM, an activity on his account late in the night is anomalous and hence, might be an intrusion. Another user Y might always login outside working hours through the company terminal server. A late night remote login session from another host to his account might be considered unusual. Anomaly detection attempts to quantify the usual or acceptable behavior and flags other

irregular behavior as potentially intrusive. One of the earliest reports that outlines how intrusions may be detected by identifying “abnormal" behavior is the work by Anderson. In his influential report, Anderson presents a threat model that classifies threats as external penetrations, internal penetrations, and misfeasance and uses this classification to develop a security monitoring surveillance system based on detecting anomalies in user behavior. External penetrations are defined as intrusions that are carried out by unauthorized computer system users; internal penetrations are those that are carried out by authorized users of computer systems who are not authorized for the data that is compromised; and misfeasance is defined as misuse of authorized data and other resources by otherwise authorized users.

In contrast, misuse intrusion detection refers to intrusions that follow well-defined patterns of attack that exploit weaknesses in system and application software. Such patterns can be precisely written in advance. For example, exploitation of the fingered and send mail bugs used in the Internet Worm attack would come under this category. This technique represents knowledge about bad or unacceptable behavior and seeks to detect it directly, as opposed to anomaly intrusion detection, which seeks to detect the complement of normal behavior.

II. RELATED WORK

This section discusses about the literature survey done on various issues like malware and spyware changes, various attacks, and malicious nodes, trust relationship among the group of nodes as well as security in the System Networks.

Seungmin et al. (2011) proposed two different approaches have been used in detecting intrusions. The first approach, commonly known as misuse detection, is a rule-based approach that uses stored signatures of known intrusion events to detect known attacks. This approach has been highly successful in detecting occurrences of previously known attacks. However, it fails to detect new attack types and variants of known attacks whose signatures are not stored. When new attacks occur, the signature database has to be manually modified for future use.The second approach is commonly known as an anomaly detection approach. Traditional anomaly detection, which is known as supervised anomaly detection, builds a model of normal data using labeled data and detects deviation from the normal model in observed data. In this approach, data mining techniques such as a support vector machine (SVM) and a neural network are usually used. However, such supervised anomaly detection is impractical since it is very difficult or impossible to obtain either labeled or purely normal data. To overcome this problem, there has been study on unsupervised anomaly detection, also known as anomaly detection over noisy data . This approach basically assumes that the volume of normal data vastly overwhelms that of anomalous data.To address these problems, a novel framework is developed in this paper for fully unsupervised training and online anomaly detection. The framework is designed so that an initial model is constructed and then it gradually evolves according to the current to state of online data.

Shelly Xiaonan Wu et al. (2010) proposed Artificial intelligence and machine learning techniques to discover the underlying models from a set of training data. Commonly used methods were rule based induction, classification and data clustering. The aim of this review is twofold: the first is to present a comprehensive survey on research contributions that investigate utilization of computational intelligence (CI) methods in building intrusion detection models; the second aim is to define existing research challenges, and to highlight promising new research directions. The scope of the survey is the core methods of CI, which encompass artificial neural networks, fuzzy sets, evolutionary computation methods, artificial immune systems, swarm intelligence and soft computing. Soft computing, unlike the rest of the methods, has the synergistic power to intertwine the pros of these methods in such a way that their cons will be compensated. This paper presents the state-of-the-art in research progress of computational intelligence (CI) methods in intrusion detection systems. The scope of this review was on core methods in CI, including artificial neural networks, fuzzy systems, evolutionary computation methods, artificial immune systems, and swarm intelligence.

Zihui Chef Xueyun Ji et al. (2010) proposed an effective method for intrusion detection based on hidden markov model and rough sets theory in order to realize the quick detection of known intrusion, an engine of quick detection inspired by hidden Markov model. There are two main methods for detect intrusions, anomaly detection and misuse detection. The former is the main field in intrusion detection system (IDS) research, it can detect unknown intrusions stably without too much knowledge on system flaw, but it has the shortcoming of high false alarm rate. The key of anomaly intrusion is to establish the system or user's normal behavior pattern (storehouse) and use the pattern (storehouse) to carry on the comparison and judgment to the current behavior. The HMM and rough set based approach can identify misuse and malicious intrusion by means of attributes reduction. It could acquire a better HMM with a relatively small number of training data. Our method can promote the detection rate and decrease the false alarm rate stably.

Saira Beg et al. (2010) proposed Intrusion detection , the method of identifying unauthorized use, misuse, and abuse of computer systems by both system insiders and external attackers. Intrusion detection is the method of identifying unauthorized use, misuse, and abuse of computer systems by both systems insiders and external attackers. Firewalls can prevent the system from being attacked by the outside attacker but can be intruded and bypassed by the insiders easily.Intrusion detection and prevention systems analyze packets deeply. During this process it is possible that administrator reveals sensitive and confidential information about the users. This may be harmful than the attack if misused. It can happen because IDS monitor network traffic and are allowed to access each and every packet.

Ke Wang et al. (2007) proposed this method to enables automatic signature generation that can be deployed immediately to network firewalls and content filters to proactively protect other hosts. The important principle demonstrated is that correlating multiple alerts identifies true positives from the set of anomaly alerts and reduces incorrect decisions producing accurate mitigation. In this paper, the payload anomaly detection and content alert correlation, either on the host or across hosts and sites, hold promise for the early detection of zero-day worm outbreaks. It is important to note that the range of worms tested and reported in the paper is limited in number.

In the existing scheme, the analysis of the HTTP payload at the byte level has proven to be effective as it do not require the detailed knowledge of the applications running on the Web server. The algorithm proposed here for feature extraction and the joint use of HMM guarantee the same expressive power of ne gram analysis, while allowing overcoming its computational complexity.

III. PROPOSED WORK

OBJECTIVE

To detect the unintelligible intrusion among network packets by means of its pattern matching.

PROBLEM DEFINIITON

A spyware or a malware can be morphed into a network data pattern and will be added to the normal downloaded content without the knowledge of user. so our user may suffer insecurity and instability due to the intrusion of packets.

SYSTEM ARCHITECTURE

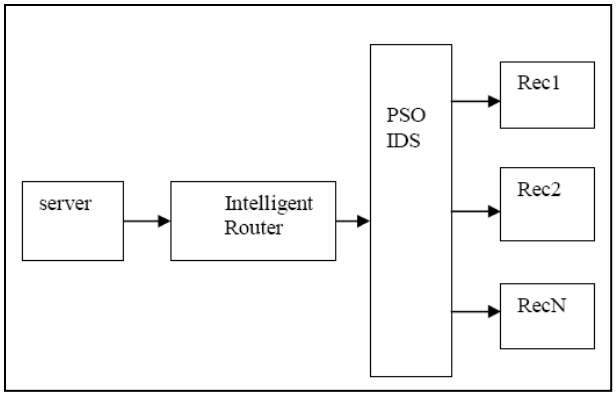


Fig. 1: Architecture Diagram of IDS

PARTICLE SWARM OPTIMIZATION:

Particle swarm optimization (PSO) is a population based stochastic optimization technique developed by Dr. Eberhart and Dr. Kennedy in 1995, inspired by social behavior of bird flocking or fish schooling. PSO shares many similarities with evolutionary computation techniques such as Genetic Algorithms (GA). The system is initialized with a population of random solutions and searches for optima by updating generations. However, unlike GA, PSO has no evolution operators such as crossover and mutation. In PSO, the potential solutions, called particles, fly through the problem space by following the current optimum particles. The detailed information will be given in following sections. Compared to GA, the advantages of PSO are that PSO is easy to implement and there are few parameters to adjust. PSO has been successfully applied in many areas: function optimization, artificial neural network training, fuzzy system control, and other areas where GA can be applied.

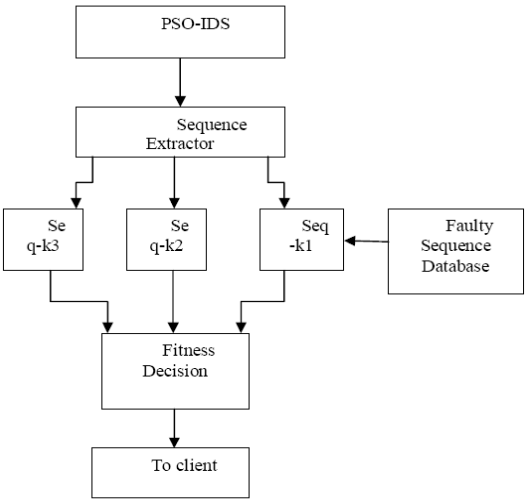


Fig. 2: Block Diagram of PSO-IDS

THE PSO ALGORITHM

As stated before, PSO simulates the behaviors of bird flocking. Suppose the following scenario: a group of birds are randomly searching food in an area. There is only one piece of food in the area being searched. All the birds do not know where the food is. But they know how far the food is in each iteration. So what's the best strategy to find the food. The effective one is to follow the bird which is nearest to the food. PSO learned from the scenario and used it to solve the optimization problems. In PSO, each single solution is a "bird" in the search space call as "particle". All of particles have fitness values which are evaluated by the fitness function to be optimized, and have velocities which direct the flying of the particles. The particles fly through the problem space by following the current optimum particles. PSO is initialized with a group of random particles (solutions) and then searches for optima by updating generations. In every iteration, each particle is updated by following two "best" values. The first one is the best solution (fitness) it has achieved so far. (The fitness value is also stored.) This value is called pbest. Another "best" value that is tracked by the particle swarm optimizer is the best value, obtained so far by any particle in the population. This best value is a global best and called gbest. When a particle takes part of the population as its topological neighbors, the best value is a local best and is called lbest.

The procedure is as follows
step 1: For each particle Initialize particle

step 2: Calculate fitness value, If the fitness value is better than the best fitness value (pBest) in history

step 3: set current value as the new pBest

step 4: Choose the particle with the best fitness value of all the particles as the gBest

step 5: Calculate particle velocity

step 6: Update particle position While maximum iterations or minimum error criteria is not attained

Fig. 3: PSO Algorithm

Particles' velocities on each dimension are clamped to a maximum velocity Vmax. If the sum of accelerations would cause the velocity on that dimension to exceed Vmax, which is a parameter specified by the user. Then the velocity on that dimension is limited to Vmax.

PSO Parameters

From the above case, it can learn that there are two key steps when applying PSO to optimization problems: the representation of the solution and the fitness function. One of the advantages of PSO is that PSO take real numbers as particles. It is not like GA, which needs to change to binary encoding, or special genetic operators have to be used. For example, try to find the solution for f(x) = x1^2 + x2^2+x3^2, the particle can be set as (x1, x2, x3), and fitness function is f(x). Then it can use the standard procedure to find the optimum. The searching is a repeat process, and the stop criteria are that the maximum iteration number is reached or the minimum error condition is satisfied.

ATTACK IMPLEMENTATION

Training set:Training set made up of normal traffic. Trained combination rules have been also proposed to better exploit additional knowledge of the domain at hand. whereas the trained combination are asymptotically optimal. The Training phase outputs the transition and emission matrices for each HMM includes in the IDS During the Training phase the estimate of the HMM parameters Is calculated with the goal of maximizing the probability assigned by the model to the sequences within the training set.

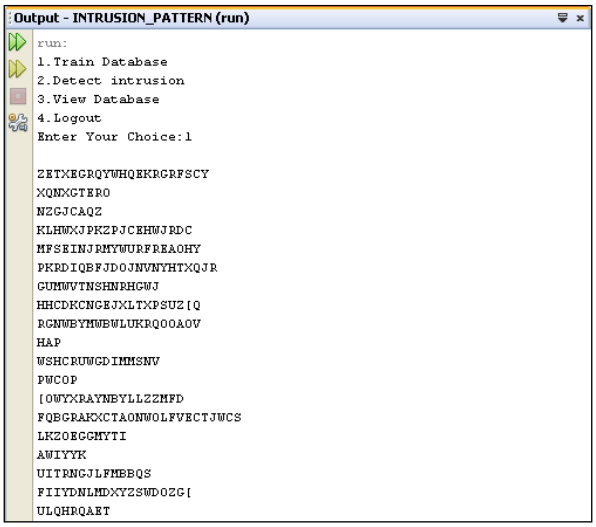


Fig. 4 : Training the data

Detection phase:Intruder Detection Systems try to detect who is attacking a system by analyzing his or her computational behavior or biometric behavior. This technique tries to identify the person behind an attack by analyzing their computational behavior. This concept is sometimes confused with Intrusion Detection (also known as IDS) techniques which are the art of detecting intruder actions.

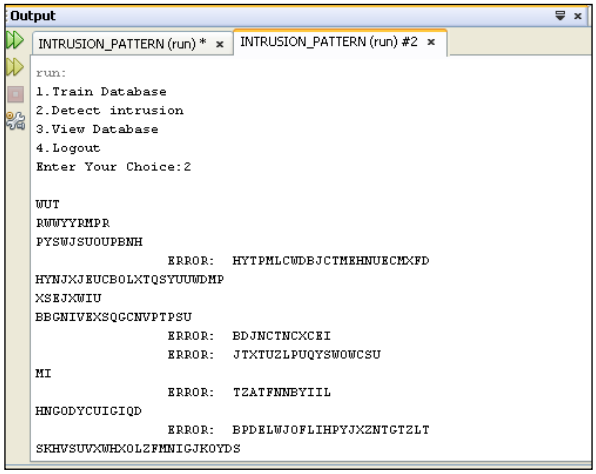


Fig. 5: Detecting the data

IV. CONCLUSION

An IDS designed to detect attacks against Web applications through the analysis of the HTTP payload by HMM proposed a new approach for extracting features which exploits the power of HMM in modeling sequences of data. HMMPayl has been thoroughly tested on three different datasets of normal traffic, and against four different dataset of attacks. the high computational cost of HMMPayl can be significantly reduced by randomly sampling a small percentage of the sequences extracted from the payload, without significantly affecting the overall performance in terms of detection and false alarm rates.

The high computational cost of HMMPayl can be significantly reduced by randomly sampling a small percentage of the sequences extracted from the payload, without significantly affecting the overall performance in terms of detection and false alarm rates.

In future First of all, HMMPayl does not take into account the length of the payload. As different lengths of the payload produce significantly different statistics, clustering the payloads by length, and using a different model for each cluster, would improve the overall accuracy.

The second improvement is related to the random sampling strategy, as the whole sequence set could be randomly split among all the classifiers in the ensemble. In such a way all the information inside the payload would be used, where a single HMM is asked to process a smaller number of sequences. Finally, the third improvement is related to the use of trained combination rules instead of a static rule to combine the HMM.

REFERENCES

[1] Ke Wang and Gabriela Cretu Salvatore J. Stolfo, (2007), ”Anomalous Payload-based Worm Detection and Signature Generation”, Recent Advances in Intrusion Detection-Springer, pp. 227-246.

[2] Saira Beg, Umair Naru, Mahmood Ashraf and Sajjad Mohsin, (2010), ”Feasibility of Intrusion Detection System with High Performance Computing”, International Journal for Advances in Computer Science. vol 1, Issue 1 ISSN - 2218-6638 .

[3] Seungmin Lee, Gisung Kim and Sehun Kim, (2011), “Self-adaptive and dynamic clustering for online anomaly detection”, Expert Systems with Application-Elsevier, vol. 38 no. 12, pp. 14891-14898.

[4] Shelly Xiaonan Wu and Wolfgang Banzhaf, (2010), “The use of computational intelligence in intrusion detection systems“, Applied Soft Computing 10-Elsevier, vol. 10 no. 1, pp. 1-35.

[5] Zihui Che Xueyun Ji, (2010), ”An Efficient Intrusion Detection Approach based on Hidden Markov Model and Rough Set”, International IEEE Conference on Machine Vision and Human-machine Interface, pp. 476-479

❑❑❑

Trust Model For Secure QOS Routing In Manets

J. Aswin Brindha & R. Ramachandran
Sri Venkateswara college of Engineering , Sriperumbur Chennai
E-mail : aswinbrindha@gmail.com & rrama@svce.ac.in

Abstract - Due to the dynamic topology, limited and shared bandwidth, limited battery power of the mobile ad hoc network (MANET), providing Quality of Service(QoS) routing is a challenging task in MANET. The presence of malicious nodes in the network causes internal threats that disobey the standard and degrades the performance of well-behaved nodes significantly. However, little work has been done on quantifying the impact of internal attack on the performance of ad hoc routing protocols using dynamic key mechanism. In this paper, we focus on the impact of Byzantine attack implemented by malicious nodes on AODV routing protocol as an extension of the previous work. Here, we propose at rust model in which the trustworthiness of each node is evaluated based on trust value and remaining energy of each node. Association level of each node is estimated based on the trust value calculated. Route selection is done using the trustworthiness and performance requirement of each route which is calculated based on both link capacity and traffic requirement to achieve QoS. Determine the trustworthiness of the node. These policies, based on shamir's key distribution method ensure the maximum security in MANETs.

I. INTRODUCTION

MANET is vulnerable to various types of attacks because of open infrastructure, dynamic network topology, lack of central administration and limited battery-based energy of mobile nodes. These attacks can be classified into external attacks and internal attacks. Several schemes had been proposed previously that solely aimed on detection and prevention of external attacks But most of these schemes become worthless when the malicious nodes already entered the network or some nodes in the network are compromised by attacker. Such attacks are more dangerous as these are initiated from inside the network and because of this the first defence line of network become ineffective. Since internal attacks are performed by participating malicious nodes which behave well before they are compromised therefore it becomes very difficult to detect.

Routing protocols are generally necessary for maintaining effective communication between distinct nodes. Routing protocol not only discovers network topology but also built the route for forwarding data packets and dynamically maintains routes between any pair of communicating nodes. Routing protocols are designed to adapt frequent changes in the network due to mobility of nodes. Several ad hoc routing protocols have been proposed in literature and can be classified into proactive, reactive and hybrids protocols. Due to several issues, routing protocol design has become a challenging task.

The basic problem with most of the routing protocols is that they trust all nodes of network and based on the assumption that nodes will behave or cooperate properly but there might be a situation where some nodes are not behaving properly. Most adhoc network routing protocols becomes inefficient and shows dropped performance while dealing with large number of misbehaving nodes. discovery traffic but interrupt the data flow, causing

The routing protocol to restart the route process or to select an alternative route if one is available. The newly selected routes may still include some of misbehaving nodes, and hence the new route will also fail. This process will continue until the source concludes that data cannot be further transferred .Thus, the routing algorithm must react quickly to topological changes as per the degree of trust of a node or a complete path between a source and a destination pair. Nodes in MANETs communicate over wireless links. Therefore efficient calculation of trust is a major issue because an ad hoc network depends on cooperative and trusting nature of is nodes. The nodes are dynamic the number of nodes in route selection is always changing, thus the degree of trust also keep changing .Another challenging issue is energy efficient routing. Especially energy efficient routing is most important because all the nodes are battery powered. Failure of one node may affect the entire network. If a node runs out of energy the probability of network partitioning will be increased. Since every mobile node has limited power supply,

energy depletion is become one of the main threats to the lifetime of the network. So routing in MANET should be reliable in such a way that it will use the remaining battery power in an efficient way to increase the life time of the network.

1.2 SECURITY PROBLEMS IN AD HOC NETWORKS

The use of wireless link renders an ad hoc network susceptible to link attacks ranging from passive eavesdropping to active interfering. Unlike fixed hardwired networks with physical defence at firewalls and gateways, attacks on an ad hoc network can come from all directions and target at any node. Damage includes leaking secret information, interfering message and impersonating nodes, thus violating the basic security requirements. All these mean that every node must be prepared for encounter with an adversary directly or indirectly Autonomous nodes in an ad hoc network have inadequate physical protection, and therefore more easily to be captured, compromised, and hijacked. Malicious attacks could be launched from both outside and inside the network. Because it is difficult to track down a particular mobile node in a large scale of ad hoc network, attacks from a compromised node are more dangerous and much harder to detect. All these indicate that any node must be prepared to operate in a mode that should not immediately trust on any peer. Any security solution with static configuration would not be sufficient because of the dynamic topology of the networks. In order to achieve high availability, distributed architecture without central entities should be applied. This is because introducing any central entity into security solution may cause fatal attack on the entire network once the centralized entity is compromised. Generally, decision making in the ad hoc networks is decentralized and many ad hoc network algorithms rely on the cooperation of all nodes or partial nodes. But new type of attacks can be designed to break the cooperative algorithm. Malicious nodes could simply block or modify the data traffic traversing them by refusing the cooperation or hacking the cooperation. As can be seen from the above, no matter what security measures are deployed, there is always some vulnerability that can be exploited to break in. It seems difficult to provide a general security solution for the ad hoc networks.

Traditional cryptographic solution is not adapted for the new paradigm of the networks. As can be seen from the above analysis, what is lacked in the ad hoc networks is trust since each node must not trust any other node immediately. If the trust relationship among the network nodes is available for every node, it will be much easier to select proper security measure to establish the required protection. It will be wiser to avoid the un-trusted nodes as routers. Moreover, it will be more sensible to reject or ignore hostile service requests. Therefore, the trust evaluation becomes a before-security issue in the ad hoc networks. The security solution should be dynamic based on the changed trust relationship.

1.2.1 Intrusion Detection

The ad hoc networks have inherent vulnerabilities that are not easily preventable. Intrusion prevention measures, such as encryption and authentication, are required to protect network operation. But these measures cannot defend compromised nodes, which carry their private keys. Intrusion detection presents a second wall of defence. It is a necessity in the ad hoc networks to find compromised nodes promptly and take corresponding actions to against. A distributed and cooperative architecture for better intrusion detection.

1.2.2 Secure Routing

The ad hoc networks, routing protocol should be robust against topology update and any kinds of attacks. Unlike fixed networks, routing information in an ad hoc network could become a target for adversaries to bring down the network. There are two types of threats.

The first one comes from external attackers. The attacks include injecting erroneous routing information, replaying old routing information, and distorting routing information. With these ways, the attackers can successfully partition a network or introduce excessive traffic load into the network, thus cause retransmission and ineffective routing. Using cryptographic schemes, such as encryption and digital signature can defend against the external attacks.

The second threat comes from compromised nodes, which might send malicious routing information to other nodes. Typical attacks fallen into this category are black hole attacks, routing table overflow attacks, impersonation and information disclosure, etc. .The internal attacks from malicious nodes are more severe because it is very difficult to detect because the compromised nodes can also generate valid signature. Existing routing protocols cope well with the dynamic topology, but usually offer little or no security measures In a set of design techniques for intrusion resistant ad hoc routing algorithm was presented mainly to against denial-of-service attacks. Secure aware ad hoc routing in uses security properties (e.g. time stamp, sequence number, authentication password or certificate, integrity, confidentiality, and non-repudiation) as a negotiable metric to discover secure routes in an ad hoc network. The SAR can be implemented based on any on-demand ad hoc routing protocol with suitable modification. But it only considers the effect of security properties on the trust. In a secure routing solution is

proposed for the black hole problem. But unfortunately, this solution does not solve the problem caused by cooperation of multiple malicious nodes.

1.2.3Key Management

Traditional cryptographic mechanisms, such as digital signature and public key encryption, still play vital roles for the security of the ad hoc networks. All these mechanisms require a key management service to keep track of key and node binding and assist the establishment of mutual authentication between communication nodes. Traditionally, the key management service is based on a trusted entity called a certificate authority (CA) to issue public key certificate of every node.

The trusted CA is required to be online in many cases to support public key revocation and renewal. But it is dangerous to set up a key management service using a single CA in an ad hoc network. It will be the vulnerable point of the network. If the CA is compromised, the security of the entire network is crashed. In and a threshold cryptography is used to provide robust and ubiquitous security support for the ad hoc networks. The CA functions are distributed through a threshold secret sharing mechanism. This approach is very complicated to implement. It is also hard to survive from multiple hijacked nodes that have secret shares.

The security for the ad hoc networks is still in its infancy. Existing solutions cannot solve this issue well. What is missed is an effective mechanism that can provide reasonable inference based on available knowledge, such as intrusion detection result, past experience, communication data value, and preferences, to evaluate trust relationship among network nodes. With the evaluation result, it is possible to make correct decision or close-correct decision on security protection. New mechanisms are expected to adapt the special characteristics of the new network paradigm.

PROPOSED SYSTEM

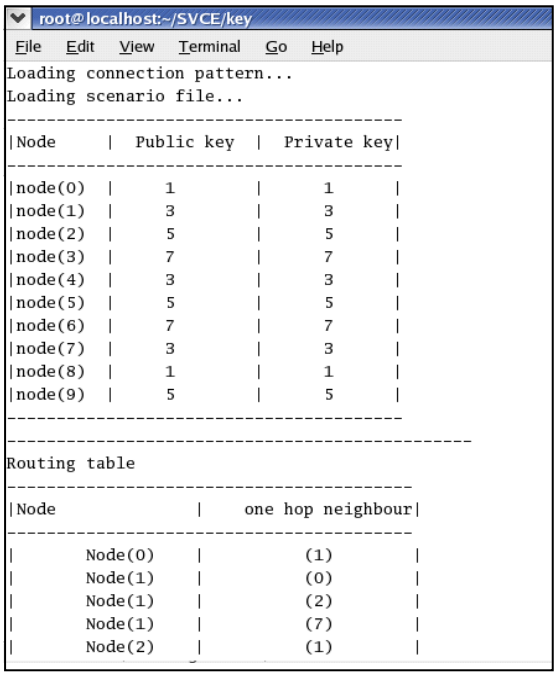
3.1 OVERVIEW

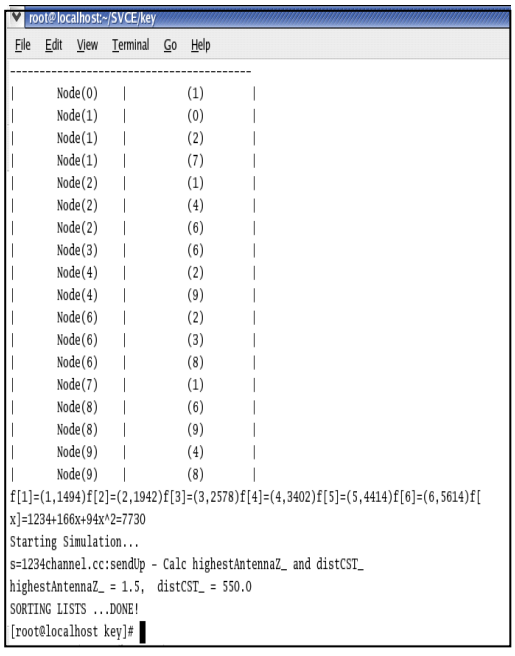
A trust evaluation based security solution for the ad hoc networks. It introduces a fair and rational security mechanism.

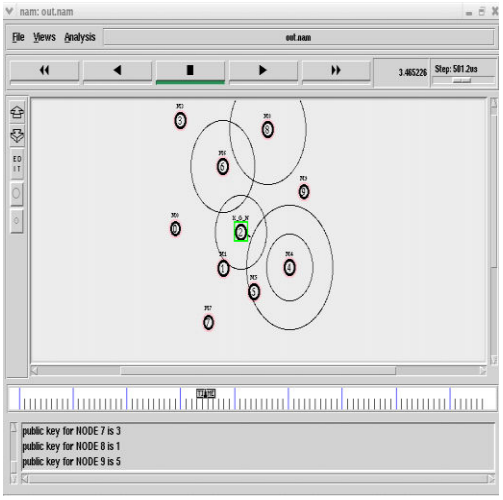
3.3 Secret Key issuing

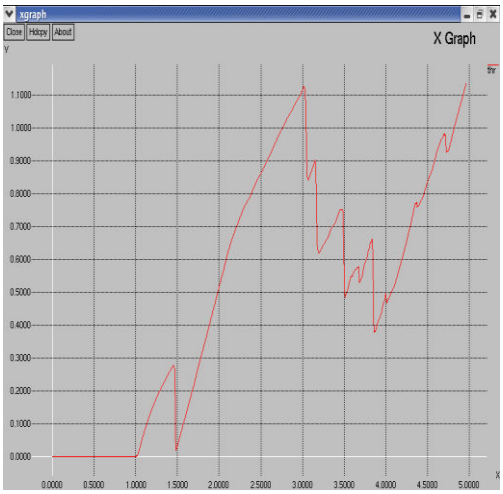
Shamir's scheme is very ancient in the sense that all shares have the same size as the secret, measured in the number of bits you need to store them For every probability distribution with which the secret s is chosen, and for any secret sharing scheme, the entropy of every share is at least the entropy of the secret. In particular, an optimal encoding requires at least as any bits to write down a share as to write down the secret. Suppose the entropy of the secret is l bits. Without loss of generality, assume we look at the _rest share s1. Take some set of shares Such that A is insouciant to determine s, Then, by the privacy property, given A you have 0 bits of information on s. But given A and s, you have l bits of information. Thus by being told that the entropy of s must be at least that large. Sometimes you want a more general solution than what threshold secret sharing can provide. Suppose you are protecting a password s that gives access to executing a particular critical operation in some system.

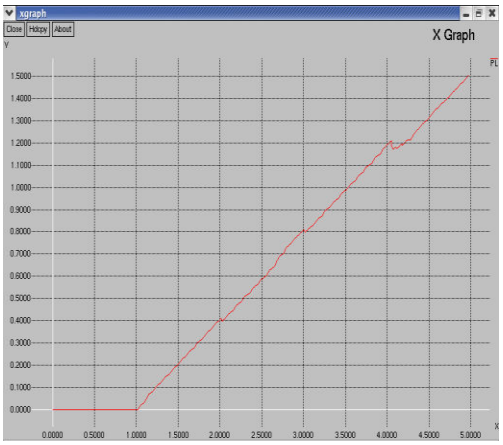
IMPLEMENTATION AND RESULTS











CONCLUSION AND FUTURE ENHANCEMENT

The Nodes credit and the trustworthiness of the network is normally checked and verified using Shamir policy and the communication between the source and destination is normally carried out. By using query rating policy to find o the suspicious node Now the Particular Network is said as Trust Network and hence the packets are been transferred

REFERENCE

1. Chi Zhang. Xiaoyan Zhu, Yang Song and Yuguang (2010)"A formal Study of trust based routing in wireless Ad hoc Networks" IEEE INFOCOM Department of computer engineering
2. Marias G.F., Georgiode P., Flitzanis D., Mandalar k. (2006)"Co-operation enforcement schemes for Manets" wireless communication and mobile computing Department of Informatics and Telecommunications,
3. Peter T. Dinsmore, David M.Balenson, Michael Heyman,Peter S.Kruus, Caroline D. Scace, and Alan T. Sherman,(2011)"policy based security Management for Large Dynamic groups" International Journal of innovative technology & creative engineering.
4. Shilpa S.G., Sunitha N.R, Amberker B.B(2011) "A Trust Model for secure and Qos Routing in MANETS" International journal of innovative Technology &creative Engineering
5. Qiuna Niu (2009)"A Trust Based Message Encryption scheme for mobile ad hoc Networks" University of science and Technology Qingdao, china
6. Zheng Yan ,Peng Zhang(2008)"Trust Evaluation Based Security solution in Ad hoc Networks"Nokia Resarrch center Finland

❑❑❑

"TALKFREE"
Mobile To Mobile Voice Communication

Tejas Patil, Mangesh Patil, Vishwas Madaswar, Akshay Patil & Kavita P. Moholkar.
Computer Department Of Engg, University Of Pune,Pune, India.
E-mail : patil.tejas@hotmail.com, vishwas4022@rediffmail.com, akshay7.patil@hotmail.com

Abstract - The proposed system in this paper is to design system that uses WIFI in Peer to Peer or WLAN (Wireless Local Area Network) as a means of communication between mobile phones at no cost. The existing voice telephony over mobile is currently uses service provider such as GSM, CDMA or using IP provider at cheaper cost. The system will allow users to search for other individuals within WIFI range and to establish free peer to peer connections between them for voice communication. This system will use SIP (Session Initiation Protocol) and VOIP (Voice Over Internet Protocol) protocols for the communication. The system will use a hashing algorithm to store the IP address of mobile. The current system will only allow user to voice conversation, sending SMS, file transfer.

Keywords - *VoIP; WIFI, SIP*

I. INTRODUCTION

IP telephony try to reduce the cost for supporting this service over mobile phone, but it is facing difficulties since the same feature is supported on desktop and laptop at lower complexity. The challenge is to provide the same service over mobile phone at no cost, as it has been described in this paper. VOIP [1] (Voice over Internet Protocol) is used for communication of two persons by sending voice packets in a real time fashion. Various protocols are involved in implementing VoIP [1]. The major task is to establish a session between the two communicating parties. Currently servicing IP addressing in traditional networks are managed by two technologies, the DNS (Domain Name System), and DHCP (Domain Host Configuration Protocol). DNS Servers resolve human friendly domain names to IP addresses for computers and resources on the Internet globally. DNS keeps website addresses consistent regardless of the physical location or routing protocol. DHCP helps to make automatic network configuration, IP address allocation, for network device. Whenever a new device is connected to the network the device will request for an IP address from the server, which will allocate the address to the networked device for a specific time of period, where dynamic network addressing is used. The DNS mechanism cannot be applied to peer to peer Ad hoc network, and therefore a better solution is suggested in the proposed system in this paper, which is based on WIFI technology. The protocols involved in establishing the session are called as Control plane protocols. Session Initiation Protocol and H.323 are some of the control plane protocols. These protocols are also called as signaling protocols as they are used to establish sessions between the users. Due to various advantages which are offered by Session Initiation Protocol (SIP) [2], it has been majority adopted by the telecommunication industry. One of the main advantages of SIP is that it is human readable and is less complex when compared with H.323 which is mainly binary. So, in this application we implemented SIP as our signaling protocol [2].

The proposed system will be very useful in software companies for their employee for • Making call to their colleague in company

• User friendly

• Cost free

II. SCOPE AND NEED :-

The efficient, fast communication between the employees is very important in company. This leads to more informed employees with the ability to make better, faster decisions. This in turn leads to better productivity. The proposed system can be used for communication in company by their employee. This system will provide good quality of communication within the company employee with no charges. Communication with this system will not be PSTN (public switched telephone network so system will be less expensive. The system uses Wireless technology particularly wireless LANs) offers a good solution to the problems of mobility, flexibility and availability. In proposed system, the server will store the IP address and details of the users, call logs. The client side will be on the mobile phones of users by which they will register with server and will able to make call other registered users.

III. WORKING OF THE SYSTEM:-

The proposed system will work with Wi-Fi network and mobile phones having Wi-Fi. When mobile user S1 willing to call other registered mobile user S2, S1 will register to the server by with unique key and IP address.

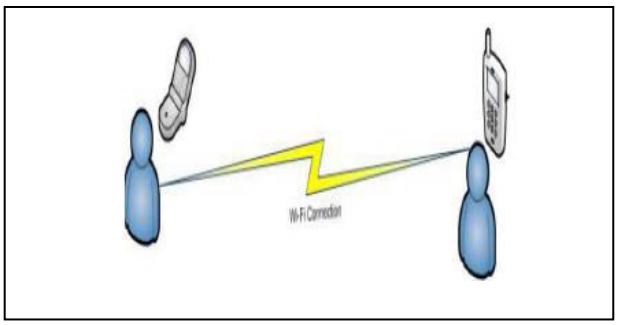


Fig.1-Peer to Peer Network For Wi-Fi

The calling request of S1 will be send to sever, sever with respond with IP address of user S2. Then S1 will try to establish the peer to peer connection with S2 with virtual connection between S1 and S2. If S2 accepts the calling request, mobile phones S1 and S2 will able to communicate to each other use VOIP [1]. However, if caller or receiver are not covered by any WIFI network, a message will be popped up to user asking if he/she is willing to continue the call through GSM. Then the user would have the choice to carry on or cancel the call. Hashing algorithm would allow the mapping the IP addresses.

A. Advantages

The system has following advantages:-

- It is used to make voice communication
- Communication is cost free
- It has call logs.

B. Drawbacks

The System has following drawbacks:-

- It does not allow call wait and call conference
- It only work in Wi-Fi network
- Cost of devices is high

IV. FUTURE OF PROJECT:-

The proposed system can be used in various organizations like IT companies where there needs frequent communication between employees.

V. CONCLUSION

Voice over IP has made the communication cheaper. The work presented in this paper is a first step for developing a peer to peer voice communication between two mobile users in the same network using VOIP and SIP protocol. The system described in this paper play a major role in field of cost effective and mobile communication in future.

REFERENCES

[1] Samrat Ganguly, Sudeept Bhatnagar "VoIP: Wireless, P2P and New Enterprise Voice over IP" 2008

[2] Henry Sinnreich, Alan B. Johnston "Internet Communications Using SIP: Delivering VoIP and Multimedia Services with Session Initiation Protocol"

[3] William Stallings "Wireless Communications & Networks 2nd Edition "

[4] Hui Min Chong and H. Scott Matthews, "Comparative Analysis of Traditional Telephone and Voice over- Internet Protocol (VoIP) Systems", IEEE 2004

[5] Bernardo A. de la Ossa Perez, "Voice over IP: Study of H.323 and SIP", 5th September, 2004.

[6] Taylor D. Edgar, "TCP/IP Complete", 1st. New Jersey: McGraw Hill, 1998.

[7] J. Distefane, and A. Ronan, "Guide To Wireless Enterprise Application Architecture", 1st ed. NY, New York: John Wiley & Sons Inc, 2002.

[8] S. Gast, and Mathew, "802.11 Wireless Networks the Definitive Guide", 1st. California: Orielly, 2000.

[9] William Lee, "Wireless and Cellular Telecommunications. 3rd", New York, NY: McGraw Hill, 2006. 272.

❑❑❑

An Intelligent Scheduler Approach to Multiprocessor Scheduling of Aperiodic Tasks

Induraj. P. R
Department of electronics and communication, Bharath university, BIST selaiyur- India.
E-mail : induraj.gandhian@yahoo.com

Abstract - This paper presents a new scheduler capable of scheduling aperiodic tasks at real time in multiprocessor system. The algorithm proposes a new way to determine dynamically tasks of high priority and low priority finding the elapsed execution time and remaining execution time, and the amount of resource availability and deadline of task, with no prior knowledge of task arrival time and also ensures that no processor remains ideal thus utilizing processors at all times.

Keywords*-remaining execution time, elapsed execution time.*

I. INTRODUCTION

The periodic tasks and a periodic tasks are more common in real time systems. Periodic task are those that appear at regular intervals, while a periodic tasks are those that appear at any instant i.e. at irregular time intervals.

The classic book on real time systems by C.M.Krishna & Kang G.Shin[3] details the scheduling of both periodic and aperiodic tasks using static priority algorithms and dynamic priority algorithms. The static priority algorithms are based on scheduling tasks with least period by assigning them highest priority and those tasks with highest period the lowest priority. While the dynamic priority algorithm schedule's tasks based on deadlines.

The EDF and least laxity first algorithms that are uniprocessor online scheduling algorithms are optimal algorithms, which means any a set of tasks if schedulable by them then the same set of job can be feasibly schedulable by other algorithms. But in the case of multiprocessor systems there are no online scheduling algorithms that are optimal. This was shown by simplest multiprocessor model by HONG & LEUNG [2].

In this study job, consideration of new scheduling algorithm for a multiprocessor system that can deal with responding to a periodic tasks and dynamically assigning priority to tasks by taking into account the execution time of arriving task based on resource availability, the elapsed & remaining execution time of the task executing in processor.

We relax the assumption that tasks need to start essentially at the same time to coordinate their execution and computation put forward by gang scheduling algorithm, since gang scheduling demands that no task execute unless other tasks in gang starts executing, this would cause processor to remain idle irrespective of some high priority task ought to be run.

This algorithm demonstrates online scheduling of tasks and assigning priority to tasks dynamically for preemption based on the elapsed execution time and the execution time remaining. Unlike static priority based algorithms which utilize the processors only 70% or less, This algorithm schedules task dynamically so it can be viewed that processor is utilized to its great extent i.e. 100% theoretically proving through a theorem derived to prove that EDF algorithm utilizes processors to maximum extent [1].

II. DESCRIPTION

The dynamic algorithms give high priority to tasks with least deadline, but the execution time for that particular task can high or low. If we take into consideration that a task with least deadline but with highest execution time is given highest priority then if the processor is scheduled to complete this task by preemption it takes greater execution time equal to the execution time of least dead lined task. Thus causing the processor to stall in only one task executing all the way to complete it within deadline, thus we relax this idea of giving priority to task with least deadline and highest execution time. The execution time a task takes is dependent on various factors like resource availability and the number of lines in the task which constitutes the length of task, etc.

We consider here a stochastic model with a set of M processors in the multiprocessor system. Stochastic model is the one with uncertainties in both arrival rate and service rate and let job with infinite number of tasks ranging from T_0 to T_∞ arrives. We also consider that the average service rate of processor is more than the average arrival rate of tasks to prevent building up

infinite queue. I.e. for average service rate to be more than the average arrival rate, the processors are to be operating at higher frequencies.

Assumption:

1. No task starts executing at the same time.
2. No task within the same gang execute for same time.
3. Task preemption is possible for satisfying conditions.
4. Scheduler is capable of handling the both periodic and aperiodic tasks arriving.
5. Addition of new processor to a set of M processor is tolerable.
6. The time for comparisons made among processors is negligible.
7. Processor is capable of completing maximum percentage of tasks total execution time before next job arrives.

For M set of processor, scheduler is scheduling T_0 to T_{m+i} where i=0 for initial scheduling of task to M processor. As soon as the T_0 task is scheduled on a processor it starts executing independent of other task, the same applies for other task scheduled in other processors. After initial scheduling of T_{m+i} (i=0 for initial schedule of M processors), when new tasks T_{m+i} (i=1 to ∞) arrivers the following need to be answered,

1. How this new task is to be scheduled?
2. Whether by preempting previous task or by scheduling the new task to execute as soon as the previous task is completed?
3. Based on what the high priority task is chosen for the scheduler to allow preemption of previous task?
4. Whether there are sufficient resources available for successful execution of the task.

The block diagram of intelligent scheduling is shown in figure 1.

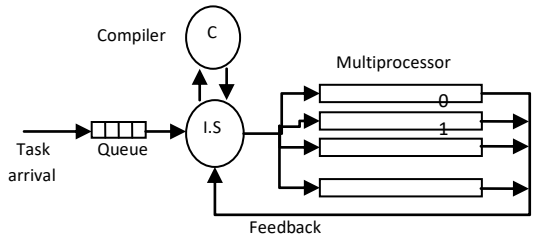


Figure 1. Block diagram

When new task arrives the compiler estimates and announces the execution time E_t that a task would take respective of resource availability as resource availability would seriously affect the execution of task to the scheduler, a comparison is done among processor by the intelligent scheduler as to which processor has zero utilization and how much execution time has elapsed and how much execution time is remaining, where the remaining execution time is the difference between the total execution time E_t and the elapsed executed time E_{t-k}. The execution time is directly related to the time taken to execute instruction counts on the processor running at certain clock rate and resource availability.

Case1:

Theorem1:

A set of task represented by T (A_i, E_t, D_i) is readily schedulable in the processor if the utilization of the processor is found zero i.e. U (n^{th}) =0;

A processor is said to be in zero utilization only if it has completed executing its task and no task are in queue waiting to execute or no task are scheduled to run.

In our case after initial scheduling on M processor only chance for any of our M processor to be in zero utilization is due to task completion. If such processor with zero utilization is found then new task with execution time E_t is scheduled to run on it

Theorem 2:

A set of task represented by T (A_i, E_t, D_i) is schedulable in the processor if the utilization of the processor is less than one i.e. U (nth) < 1

The utilization of a processor is found by

$$\frac{E_t - E_{(t-k)}}{} = u\,(n^{th})$$

Where U (n^{th}) is utilization of n^{th} processor in set a set of M processor and E_t-E_{t-k} is the remaining time to finish a task, D_{j-t} is the remaining deadline at the instant new task arrives.

But other than this condition for scheduling tasks in a processor the condition to be satisfied are given in case 2.

Case 2:

When new task arrives if the processors are busy executing their previous task, the remaining execution time E_t-E_{t-k} for every processor is calculated,

Condition 1:

Consider we have the remaining execution time E_t-E_{t-k} of tasks executing in processors to be both lesser and greater than the execution time of new task found by intelligent scheduler considering the resource availability. Then the processor executing task with least remaining execution time E_t-E_{t-k} within multiprocessor and task with highest execution time within the job is chosen.

Condition 1a:

If this least remaining execution time E_t-$E_{(t-k)}$ is less than the execution time E_t of new task then schedule is made such that new task is scheduled to execute after the task on corresponding processor is complete. This guarantees continuous and quick output since the preemptions of task about to complete would result in longer waiting for result of the task.

Condition1b:

If the remaining execution time is same as the execution time of new task then previous task can either preempted or new task can be scheduled to run after the task executing by comparing the deadline of both task, i.e. if the new task is found to have lowest deadline then it is given higher priority so it preempts the executing task, if the new task is found to have higher deadline compared to executing task then it is scheduled to run after completion of the task.

Condition2:

If this remaining execution time E_t-$E_{(t-k)}$ is more than the execution time in all cases, then the processor executing task with least remaining execution time among all processor is preempted such that the processors with high remaining execution time are allowed to execute with their own task thus not overloading the processor. If it is considered that another new task i.e aperiodic task arrives at the very next moment then the new remaining execution time in corresponding processor at that very moment is the sum of the remaining execution time of previous task and the execution time of new task scheduled,

I.e. New remaining time is

$\sum [E_t\text{-}E_{(t-k)}\text{ (previous)} + E_t\text{ (new)}]$

This new remaining execution time is then compared with other processor.

III. ALGORITHM:

1) Initially tasks are scheduled to run on M processor with no conditions Loop;

2) when new task with Et arrives

2.1 If U (nth) = 0 for a processor

- Schedule processor with new task

2.2 If U (nth) = 0 for many processor

- Schedule task randomly until no processor is ideal

2.3 If U (nth) ≠ 0 for all processor, Compare processors for E_t-$E_{(t-k)}$

2.3.1 If E_t-$E_{(t-k)}$ is both more and less in different processor, Find processor with least E_t-$E_{(t-k)}$

a) If E_t-$E_{(t-k)}$ < E_t (new task)

Schedule new task to run after completion of previous task

b) If E_t-$E_{(t-k)}$ = E_t (new task)

If deadline of new task < executing task

Preempt executing task & schedule new task

Else

Schedule new task to run after completion

of executing task

2.3.2 If E_t-$E_{(t-k)}$ in different processor is only more than E_t of new task,

Find processor with least E_t-$E_{(t-k)}$ such that

E_t-$E_{(t-k)}$ > E_t (new task)

- Preempt previous task by new task

New Et-$E_{(t-k)}$ is

$\sum [E_t\text{-}E_{(t-k)}\text{ (previous)} + E_t\text{ (new)}]$

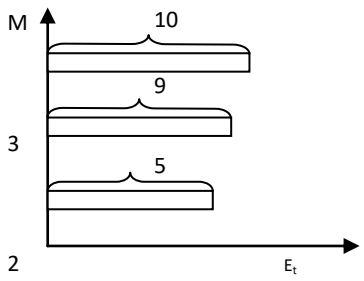
Continue loop;

Example:

Lets consider a multiprocessor system with M set of processor (M=3) and a job with the following tasks arrives.

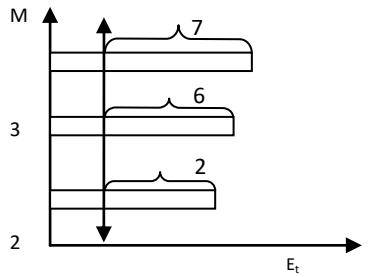
Task	T1	T2	T3	T4	T5	T6	T∞
et	10	9	5	6	3	4	..
Dj	5	8	1	2	6	5	..

Figure a. describes the initial schedule in M processors



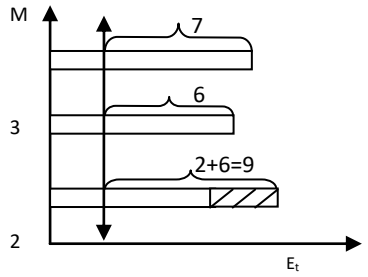
a. Initial schedule of Tm tasks

Figure b. represents the comparison of remaining execution time during arrival of new task tm+i (i=1) with execution time 6 as soon as 3 second elapses.



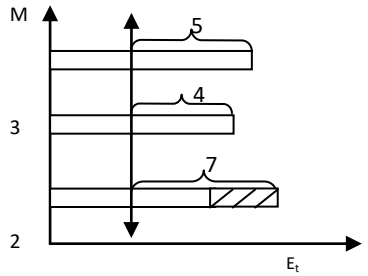
b. Arrival of new task Tm+i (i=1)

Figure c. represents the schedule of new task tm+i satisfying condition 2.3.1.a



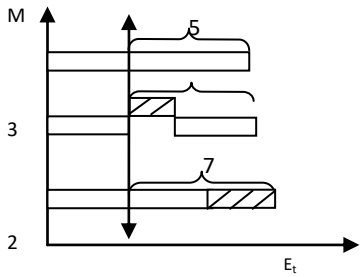
c. Schedule of new task -Tm+i (i=1)

Figure d. represents the comparison of remaining execution time during arrival of new task tm+i (i=2) with execution time of 3 as soon as 2 second elapses.



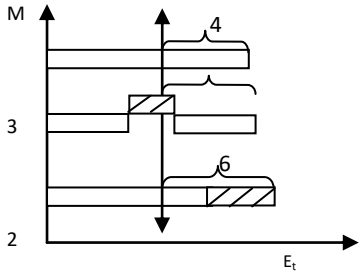
d. Arrival of new task Tm+i (i=2)

Figure e. represents the schedule of task tm+i (i=2) satisfying condition 2.3.2.



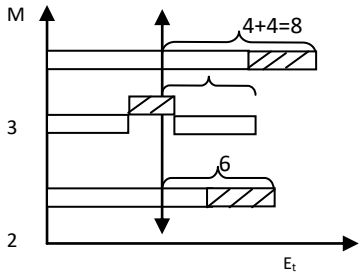
e. Scheduling of task Tm+i (i=2)

Figure f. represents the comparison of remaining execution time during arrival of new task tm+i (i=3) as soon as 1 second elapses.



f. At the arrival of task Tm+i (i=3)

Figure g. represents the schedule of task tm+i (i=3) satisfying condition 2.3.1.b

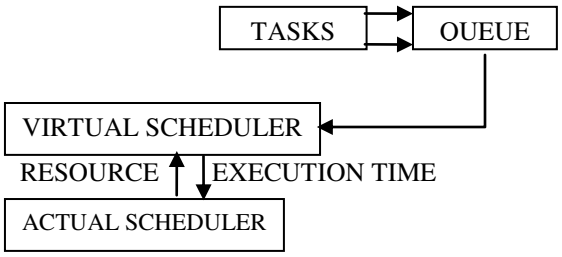


g. Scheduling of task Tm+i (i=3)

IV. IMPLEMENTATION

To schedule tasks based on execution time and resources, the algorithm must know prior to scheduling the execution time a code will take and the amount of resource present to schedule. Execution time of any task can be found only by either running the task or by tracing the entire source code. The number of lines to be traced can vary from tens to several thousands; making it impossible to trace the entire source code. Due to impossibility in tracing the source code, we emphasize the method of running the code in a fictitious environment comparable to the real environment called virtual scheduler. The execution time and remaining execution time are found by using the concepts of virtual scheduler approach and are given to scheduler to schedule the tasks as per our algorithm. The virtual scheduler is run on the same machine running actual scheduler. Initially tasks are made to run on the virtual scheduler in the order of arrival even though two or more task arrives at same time, but the tasks arriving at the same time are notified to actual scheduler to make it schedule tasks considering the remaining execution time

to be found by virtual scheduler. While a task is executing if a task arrives, a timestamp in respective timers is made denoting the elapsed time. The remaining execution time is consequently found from the total execution time and the elapsed time. This information's such as remaining execution time and total execution time are conveyed to actual scheduler to schedule tasks.



Virtual scheduler on cloud network accessing clouds services such as platform as service and software as service is another alternative for implementation where virtual scheduler processes tasks at a remote location accessed by cloud and returns the remaining execution time and the execution time to the scheduling environment.

REFERENCE

[1] C.L.Liu and James W. Layland, "scheduling algorithms for multiprogramming in a hard real time environment" published in journal of ACM (JACM) volume 20 issue 1 -1973.

[2] Hong, K. and Leung.J, "online scheduling of real time tasks". Appeared in IEEE transaction on computers, volume 41, issue 10, page 1326.

[3] C.M.Krishna and Kang G.shin "real time systems" -international edition 1997.

[4] Damir isovic and Gerhard fohler "Efficient scheduling of sporadic, aperiodic and periodic task with complex constraints" at the proceeding of 21st IEEE real-time system symposium, 2000.

[5] inki hing, miodrag potkonjak and mani B. srivastava "On-line scheduling of hard real time tasks on variable voltage processor" appeared in IEEE/ACM international conference on nov-1998 in page 653.

[6] Bhaskar dasgupta and Michael A. Palis, "online real-time preemptive scheduling of jobs with deadlines on multiple machines" published in APPROX`00 proceedings of third international workshop on Approximation Algorithms for Combinatorial Optimization.

[7] yi-ping you, chingren lee, jenq-kuen lee and wei-kuan shih "Real-time task scheduling for dynamically variable voltage processors" IEEE workshop on power management for real time and embedded systems.

[8] Christopher Clarke and Julie Howrath, "Intelligent Scheduler, Prioritize on Fly".

[9] wei zhao,Krithi ramamritham and john A. Stankovi, "Preemptive scheduling under time and resource constraints", IEEE transaction on computers, Vol c-36, No 8, August 1987, page 949.

[10] Kamaljit Kaur, Amit Chhabra and Gurvinder Singh, "Heuristics Based Genetic Algorithm for Scheduling Static Tasks in Homogeneous Parallel System", international journal of computer science and security 2010, volume 4, issue 2, page 183-198.

[11] Ramamritham. K and Stankovic. J.A., "Scheduling algorithms and operating systems support for real-time systems" proceedings of the IEEE jan 1994, volume 82, issue 1, page 55-67.

[12] Jovanovic.N and bender.M.A, "Task scheduling in distributed systems by work stealing and mugging - a simulation study" 24th international conference on information technology interfaces, 2002, ITI 2002, volume 1, page 259-264.

[13] Oliver Sinnen- "**Task Scheduling for Parallel Systems-** Wiley Series on Parallel and Distributed Computing".

[14] Alejandro Masrur, Sebastian Drossler, Thomas Pfeuffer and Samarjit Chakraborty, "**VM-Based Real-Time Services for Automotive Control Applications"** Proceedings of the 2010 IEEE 16th International Conference on Embedded and Real-Time Computing Systems and Applications.

[15] Jun Fang, shoubao yang, wenyu zhou and hu song, "Evaluating I/O Scheduler in Virtual Machines for Mapreduce Application" 2010 9th International Conference on grid and cooperative computing (GCC), page 64-69.

[16] Jia tian, yuyang du and hongliang yu, "Characterizing SMP Virtual Machine Scheduling in Virtualization Environment", 2011 international conference on internet of things (iThings/CPScom) and 4th international conference on cyber, physical and social computing, page 402-408.

[17] Forsberg.N, Nolte.T, Kato.S and Asberg.M, "Towards real-time scheduling of virtual machines without kernel modifications", 2011 IEEE 16th Conference on Emerging Technologies & Factory Automation (ETFA), page 1- 4.

[18] khalid.o, Maljevic.I., Anthony.R, Petridis.M, Parrott.K, and Schulz.M, "Deadline Aware Virtual Machine Scheduler for Grid and Cloud Computing", 2010 IEEE 24th International Conference on Advanced Information Networking and Applications Workshops (WAINA), page 85-90.

[19] yoginath.S.B and perumalla.K.S, "Efficiently Scheduling Multi-Core Guest Virtual Machines on Multi-Core Hosts in Network Simulation", 2011 IEEE Workshop on Principles of Advanced and Distributed Simulation (PADS), page 1-9.

[20] Castrillon.J, Shah.A, Murillo.L.G, Leupers.R and Ascheid.G, "Backend for virtual platforms with hardware scheduler in the MAPS framework", 2011 IEEE Second Latin American Symposium on Circuits and Systems (LASCAS), page 1- 4.

[21] Mohammad I.Daoud and Nawwaf kharma, "A hybrid heuristic-genetic algorithm for task scheduling in heterogeneous processor networks" Journal of Parallel and Distributed Computing, Volume 71, Issue 11, November, 2011.

❑❑❑

Development of a Decision Support System for Aiding Individuals in Opting for Insurance Policy

M. K. Kavitha Devi, K.Vinitha & P. Petchimuthu

Dept. of Information Technology, Thiagarajar College of Engineering, Madurai-15.
E-mail :mkkdit@tce.edu, vinithakamaraj@gmail.com

Abstract - In this paper, our focus is to develop a decision support system with soft computing techniques using Fuzzy Logic system and Analytical Hierarchy process(AHP) for helping individuals in choosing the Insurance Policies that is best suited for them. Three factors are considered and ranked and then fuzzy techniques are used to arrive at the decision support system. The data set has been collected from the web and the model is tested by the students. The empirical evaluation shows that the model performs well.

Keywords-*Soft Computing, Fuzzy Logic, Analytical Hierarchical process, Decision Support System*

I. INTRODUCTION

The ever growing list of Insurance companies and its wide and varied range of policies often pose an ambiguity to any insurance buyer. The commoners are often put into a dilemma as to what policy to go with, which features are suitable and what are the compromises that are to be made. Then, the list is narrowed down based on the factors and upon short listing, it is reduced to one or two from which the final decision is made. This study aims at mimicking this thought process of the human brain using soft computing techniques like the fuzzy logic approach and an evaluation model for purchasing life insurance and annuity insurance using analytical hierarchy process (AHP).

The Analytic Hierarchy Process (AHP) is a theory of measurement through pairwise comparisons and relies on the judgements of experts to derive priority scales. It is these scales that measure intangibles in relative terms. The comparisons are made using a scale of absolute judgements that represents, how much more, one element dominates another with respect to a given attribute. [1]

Three factors are considered as the inputs of the proposed model including age, annual income and risk preference. To build the AHP model, we interviewed five experts with at least three years of working experience in an insurance company. The AHP is utilized to generate the weights for the evaluation model for the decision support system. For an active user input, the proposed model use fuzzy logic to perform necessary mappings to the policy. Based on the comparison between the preference given by the user and the experts input, recommendations for the policy are given.

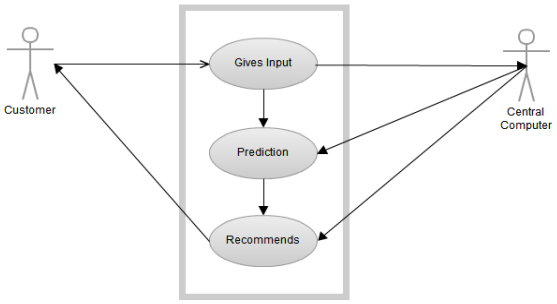


Fig 1: Outline of the Decision Support System

II. FUZZY LOGIC

Fuzzy logic is a methodology for the representation and manipulation of imprecise and vague information. One common way of using fuzzy logic in a Decision Support System is creating a fuzzy rule based system. A fuzzy rule based system has the advantages that it can represent domain knowledge in the form or rules, similar to an expert system, but it can also reason with uncertain information and perform numerical calculations. [2]

Fuzzy logic has the advantage that the solution to the problem can be cast in terms that human operators can

understand. This makes it easier to mechanize tasks that are already successfully performed by humans.

The input variables in a fuzzy control system are in general mapped into by sets of membership functions similar to this, known as "fuzzy sets". The process of converting a crisp input value to a fuzzy value is called "fuzzification". The membership function is a graphical representation of the magnitude of participation of each input. It associates a weighting with each of the inputs that are processed, define functional overlap between inputs, and ultimately determines an output response. The rules use the input membership values as weighting factors to determine their influence on the fuzzy output sets of the final output conclusion. [3].

The figure below shows the process involved in fuzzy sets

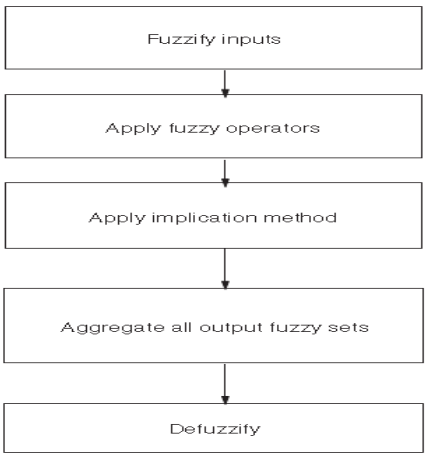


Fig 2: Working of a Fuzzy Logic System

III. FACTORS AFFECTING THE DECISION SUPPORT SYSTEM

The decision making process of choosing an Insurance policy can be broadly classifies based on three factors, which are: Age, Salary and Risk Preference. The type of insurance policy varies from individual to individual based on their ages. Also, the salary has to be taken into account because the person must be able to pay the premium amount. Risk preference is an individual's likelihood to spend more towards insurance policies. The table below shows a database of 3 insurance plans.

Table 1: Insurance Database

Factors	Life insurance(lic)	Pension plan(sbi)	Investment plan (aegon relivare)
Age at entry	18-65	18-65	25-68
Age at maturity	70	48-70	75
Premium amt min	1250/month	7500/month	50000/month
Premium	250000 lakhs	10%of annual premium on every 5th policy anniversary.	1517863 for 5 yrs.

IV. ANALYTICAL HIERARCHY PROCESS

Recently, the use of multi-criteria quantitative evaluation methods for solving social and economic problems has grown considerably. One of two major components of quantitative multi-criteria evaluation methods strongly influencing the evaluation results is associated with the criteria weights. In practice, the criteria weights are determined in assessing the economic development of the state and its regions, the commercial activity and strategic potential of enterprises, the effectiveness of particular investment projects, etc. Several theoretical and practical methods of determining the significance (weight) of criteria by experts are known. Pair-wise comparison of criteria is widely applied, and the most well-known, widely applied and mathematically grounded technique is the so-called Analytic Hierarchy Process (AHP). However, the application of this method is limited because of a great number of evaluation criteria, contradicting expert estimates and incompatible matrices obtained.

These methods are based on the statistical data on the criteria describing the compared objects (alternatives) A_j (j = 1, 2, … , n), or expert estimates and the criteria weights (significances) ω_i (i = 1, 2, … , m), where m is the number of criteria, n is the number of the objects (alternatives) compared. The evaluation is aimed at ranking the alternatives A_j by using quantitative multi-criteria methods for the particular purpose of the research. [4]

The influence of the criteria describing a particular object with the aim of investigation differs considerably. Therefore, the weights of the criteria used should be determined. Usually, the so-called subjective evaluation technique is applied, when the criteria weights are determined by experts, though objective and generalized evaluation methods are also used. The values of the criteria weights and the accuracy of evaluation results largely depend on the way of determining the criteria weights and the number of criteria because it is difficult for an expert to determine accurately the interrelationships between the criteria weights, when the number of criteria is continually growing.

The well-known mathematical problem of matrix **P,** Eigen values with Eigen vector **ω**:

$$\mathbf{P}_{\omega} = \lambda\boldsymbol{\omega}$$

Where, $\lambda = m$ is an Eigen value; m is the order of matrix **P**, i.e. the number of the criteria compared.

The weights in Saaty's approach – the vector **ω** are normalized components of eigenvector corresponding to the largest Eigen value λ_{max}:

$\mathbf{P}_{\omega} = \lambda_{max}\boldsymbol{\omega}$.

In an ideal case, when the matrix is absolutely consistent and the elements of the columns are proportional, $\lambda_{max} = m$. In this case, matrix consistency is characterized by the difference $\lambda_{max} - m$ and the order m of the matrix **P**. [5]

The flow of data in the AHP is depicted below:

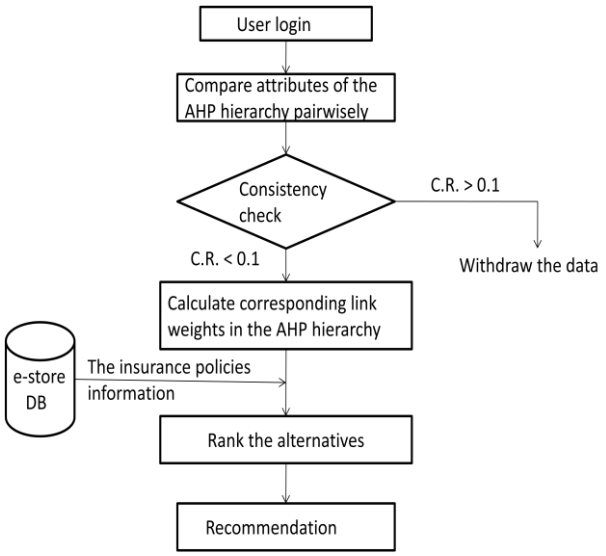


Fig 3: Flow of data in an AHP

The AHP method is based on the pair-wise comparison matrix P = ‖ p_{ij} ‖ (i, j = 1, 2, … , m). Experts compare all the evaluation criteria R_i and R_j (i, j = 1, 2, … , m), where m is the number of the criteria compared. In an ideal case, the elements of the matrix present the relationships.

The main principle of filling in the matrix is simple because an expert should indicate how much more important is a particular criterion than another. A widely known 5-point scale (1-3-5-7-9) is used for evaluation. The evaluation of the criteria ranges from p_{ij} = 1, when R_i and R_j are equally significant, to p_{ij} = 9, when the criterion R_i is much more significant than the criterion R_j with respect to the research aim.

V. STEPS IN AHP

Pair-Wise Comparison:

It is a process where two factors are considered and ranked on a scale of 1 to 10 based on the relative importance of each other. The number gives the weightage or importance of one parameter over the other.

Making Comparison Matrix:

Since we have three comparisons, we develop a 3 by 3 matrix. The diagonal elements of the matrix are always 1 and we only need to fill up the upper triangular matrix. It is filled using the following rules:

1. If the judgment value is on the left side of 1, we put the actual judgment value.
2. If the judgment value is on the right side of 1, we put the reciprocal value.

To fill the lower triangular matrix, we use the reciprocal values of the upper diagonal. If a_{ij} is the element of row column of the matrix, then the lower diagonal is filled using this formula: $\mathbf{a_{ji} = 1 / a_{ij}}$, $a_{ij} > 0$

Priority Vector:

Having a comparison matrix, now we would like to compute priority vector, which is the normalized Eigen vector of the matrix. We have 3 by 3 reciprocal matrix from paired comparison .We sum each column of the reciprocal matrix. Then we divide each element of the matrix with the sum of its column, we have normalized relative weight. The sum of each column is 1. The normalized principal Eigen vector can be obtained by averaging across the rows. The normalized principal Eigen vector is also called priority vector**.** Since it is normalized, the sum of all elements in priority vector is 1. The priority vector shows relative weights among the things that we compare.

VI. TRAPEZOIDAL FUNCTIONS

The membership function is a graphical representation of the magnitude of participation of each input. It associates a weighting with each of the inputs that are processed, define functional overlap between inputs, and ultimately determines an output response. The rules use the input membership values as weighting factors to determine their influence on the fuzzy output sets of the final output conclusion. [6]

Trapezoidal curves depend on four parameters and are given by:

$$f(x,a,b,c,d)=\begin{cases} 0 & for\ x < a \\ \frac{x-a}{b-a} & for\ a \le x < b \\ 1 & for\ b \le x < c \\ \frac{d-x}{d-c} & for\ c \le x < d \\ 0 & for\ d \le x \end{cases}$$

The boundary values for a, b and c vary for each factor i.e. for age, salary and Risk Preference. Thus three fuzzy functions are defined. Based on the user data, the values for these functions will vary.

$$X1 = f(age) = \begin{cases} 0 & x < 20 \\ \frac{x-20}{25-20} & 20 < x < 25 \\ \frac{x-25}{30-25} & 25 < x < 30 \\ 1 & x > 30 \end{cases}$$

$$X2 = f(salary) = \begin{cases} 0 & x < 0 \\ \frac{x-0}{25000-0} & 0 < x < 25000 \\ \frac{x-25000}{75000-25000} & 25000 < x < 75000 \\ 1 & x > 75000 \end{cases}$$

$$X3 = f(risk\ pref.) = \begin{cases} 0 & x < 2 \\ \frac{x-0}{5-2} & 2 < x < 5 \\ \frac{x-5}{8-5} & 5 < x < 8 \\ 1 & x > 8 \end{cases}$$

This trapezoidal process gives us the value of Y which is the output value to recommend the policy.

$Y = 0.2828X_1 + 0.6434X_2 + 0.0738X_3$

VII. EXPERIMENTAL SETUP

In order to evaluate the effectiveness of the proposed methodology, experiments have been performed using the real world data set. The data set has been collected from the web, which consists of four companies {MetLife, Bajaj, LIC, India first} and four types of policies {Term Insurance Policy, Whole Life Policy, Endowment Policy, Money Back Policy}.

We had experts from the insurance sector rank the three attributes, age, salary and risk preference for each of the four policies and their cumulative rankings are shown in table below.

Table 2: Experts Input

These are the values given by the experts for each plan. From this we infer than for plan A Salary is given more weight and for plan B age is preferred more and for plan C risk preference is considered the highest and for the plan D again age is valued more.

Attributes	Life Insurance Plan Wieghtage			
	Plan A	Plan B	Plan C	Plan D
Age (10)	5	8	3	7
Salary (10)	9	4	6	3
Risk pref (10)	3	7	8	4

VII. RUNNING THE PROGRAM

Firstly, the program checks for consistency. This is done to confirm with the experts views

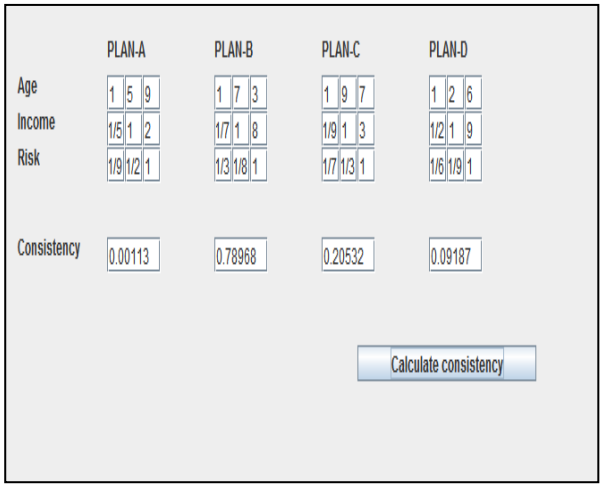


Fig 4: Consistency Check

Then, user gives the input variables, which include age, salary and risk preference.

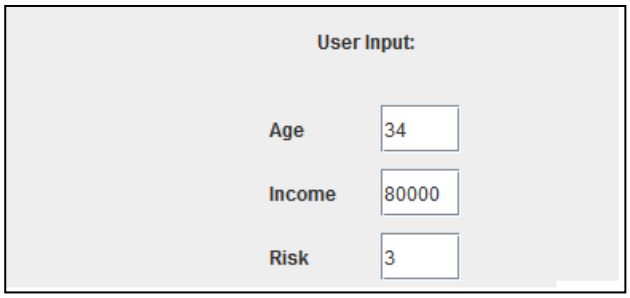


Fig 5: User Input

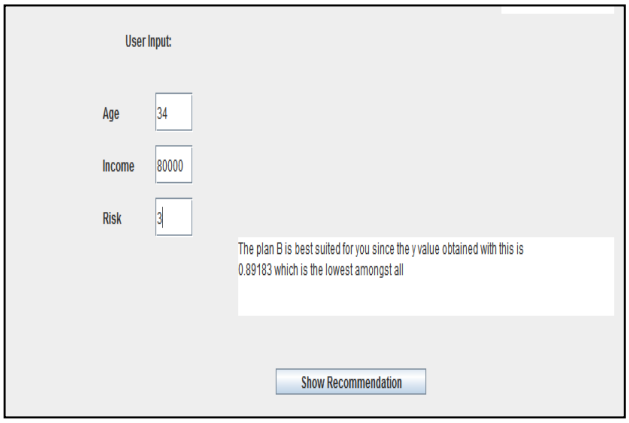


Figure 6: Recommendation Window

The user then clicks the recommendation button which calculates the value by comparing it with the matrix given by the experts. Thus recommendation is provided. The recommendation can be given for any number of input.

IX. RESULTS AND CONCLUSION

Thus, the Decision Making system for choosing insurance is designed. The paper mainly concentrates on eliminating the confusions about the policy and providing the right solution. Analytic Hierarchy Process provides accurate predictions and recommendations are done quickly when compared to other methods, by ranking the attributes. The major advantage would be user friendly.

As the behavior of the users is vague, Fuzzy Logic is used to give better recommendation. It helps the users by fixing a suitable insurance plan and increases their saving, which mimics the human thinking process. The program simulation is made and verified and the performance is found to be better than the other approaches.

Thus, with the help of this tool, users can make their insurance policy decisions easily and in a systematic and logical approach rather than random guessing based on certain assumptions.

REFERENCES

[1] Thomas L. Saaty, Decision making with the analytic hierarchy process, Int. J. Services Sciences, Vol. 1, No. 1, 2008

[2] Kevin Self (November 1990) "Designing With Fuzzy Logic", IEEE SPECTRUM, , 42:44,105.

[3] Ivars Peterson (July 24, 1993) "Fuzzy Sets" (Science News, Vol. 144, pp. 55).

[4] Figuera, J., Greco, S. and Ehrgott, M. (Eds) (2005) Multiple Criteria Decision Analysis, State of the Art Surveys, New York: Springer.

[5] Saaty, T.L. (2005) Theory and Applications of the Analytic Network Process, Pittsburgh, PA: RWS Publications.

[6] J Ren_e van Dorp and Samuel Kotz. Generalized Trapezoidal Distributions. Metrika, 58(1):85{97, 2003.

❑❑❑

Security Maintenance in VoIP Networks: Flow Analysis Attacks and Defense

Manjunath K S & Manju Devi

Dept. of Electronics & Communication, ,Professor, Dept. of Electronics and Communication,
BTL Institute of Technology and Management, Bangalore 560 099
Email: KSnayakaApril29@gmail.com

Abstract - Most VOIP networks do not provide an acceptable security and privacy level because of the flexibility of VOIP system i.e. convergence of voice and data networks. In this paper we document various security issues that a VOIP infrastructure may face and analyse the challenges and solutions. Thus this paper proposes a practical solution to address these challenges using a quantifiable k-anonymity approach and privacy aware VOIP route setup and route maintenance protocol.

Keywords: *VoIP networks, privacy, k-anonymity, mix networks, flow analysis attacks*

I. INTRODUCTION

The mix network provides good anonymity for high-latency communications by routing network traffic through a number of nodes with random delay and random routes. However, emerging applications, such as VoIP, online gaming, etc., have additional quality of service (QoS) requirements; for instance, International Telecommunication Union (ITU) recommends up to 250-ms one-way latency for interactive voice communication, while latencies over 400 ms significantly deteriorate the quality of voice conversations. This paper examines anonymity for QoS sensitive applications on mix networks using peer-to-peer VoIP service as a sample application. A peer-to-peer VoIP network typically consists of a core proxy network and a set of clients that connect to the edge of this proxy network (see Fig. 1). This network allows a client to dynamically connect to any proxy in the network and to place voice calls to other clients on the network. VoIP uses the two main protocols: route setup protocol (RSP) for call setup and termination, and real-time transport protocol (RTP) for media delivery. In order to satisfy QoS requirements, a common solution used in peer-to-peer VoIP networks is to use a route setup protocol that sets up the shortest route on the VoIP network from a caller src to a receiver dst.1 RTP is used to carry voice traffic between the caller and the receiver along an established bidirectional voice circuit.

In such VoIP networks, preserving the anonymity of caller-receiver pairs becomes a challenging problem. In this paper, we focus on attacks that attempt to infer the receiver for a given VoIP call using traffic analysis on the media delivery phase. We make two important contributions. First, we show that using the shortest route (as against a random route) for routing voice flows makes the anonymizing network vulnerable to flow analysis attacks. Second, we develop practical techniques to achieve quantifiable and customizable k-anonymity on VoIP networks.

II. EXISTING SYSTEM

Traditional VOIP network uses H.323 and session initiation1 protocol (SIP) for call setup and management.

PROBLEMS WITH SIP:

A. SIP REGISTRATION HIJACKING

The SIP is an application layer control protocol that can establish, modify, or terminate user sessions. In SIP and other VoIP protocols, a user agent (UA)/IP phone must register itself with an SIP proxy/registrar (control node), which allows the proxy to direct inbound calls to the phone. Registration hijacking occurs when an attacker impersonates a valid UA to a registrar and replaces the legitimate registration with its own address. This attack causes inbound calls intended for the UA to be sent to the rogue UA .Registration hijacking can result in loss of calls to a targeted UA.

B. SIP MESSAGE MODIFICATION

SIP message have no built-in integrity mechanism. By executing one of the man-in-the-middle attacks (IP spoofing, SIP registration), an attacker can intercept and modify an SIP message, changing some or all of the attributes of the message. This could include the person being called in a session initiation message, giving the

victim the impression that he was calling one person while the system connects them to another. By modifying the SIP message, the attacker could impersonate a caller or reroute a call to an unintended party.

C. SIP CANCEL/BYE ATTACK

The attacker can create an SIP message with the Cancel or Bye command in its payload and send it to an end node to terminate an ongoing conversation. If the attacker sends a steady stream of these packets to the end node, the end node will not be able to place or receive calls.

D. MALFORMED SIP COMMAND

The SIP protocol relies upon an hypertext mark-up language (HTML) like body to carry command information. This makes the SIP protocol very flexible and extensible for implementing VoIP features. The downside is that it becomes very difficult to test the SIP parser with every possible input. Attackers can exploit these vulnerabilities as they find them by forming packets with malformed commands and sending them to susceptible nodes. This will either degrade or decommission the node that is attacked making part or all of the VoIP system unavailable.

III. PROPOSED SYSTEM

In this paper we are using Route setup protocol (RSP) for call setup and maintenance and Real time transport protocol (RTP) for media delivery, finally we develop some flow analysis attacks and defending procedure.

FLOW ANALYSIS ATTACKS

In this section, we describe flow analysis attacks on VoIP networks. These attacks exploit the shortest path nature of the voice flows to identify pairs of callers and receivers on the VoIP network. Similar to other security models for VoIP networks, we assume that the physical network infrastructure is owned by an un-trusted third party. Hence, the VoIP service must route voice flows on the un-trusted network in a way that preserves the identities of callers and receivers from the un-trusted network.

NAIVE TRACING ALGORITHM

Let source be the caller. We use a Boolean variable f(p) belongs to {0, 1} to denote whether the node p is reachable from src using the measured flows on the VoIP network. Let us consider a sample topology shown in Figure 1. For the sake of simplicity, assume that each edge has unit latency. The label on the edges in Figure 1. indicates the number of voice flows. A trace starting from caller p1 will result in f(p1) =f(p2) =f(p3) =f(p4)= f(p5)=1. Filtering out the VoIP proxy nodes (p5) and the caller (p1), the clients p2, p3, and p4 could be potential destinations for a call emerging from p1.However, the tracing algorithm does not consider the shortest path nature of voice routes. Considering the shortest path nature of voice paths leads us to conclude that p2 is not a possible receiver for a call from p1. If indeed p2 were the receiver, then the voice flow would have taken the shorter route p1 → p2 (latency =1), rather than the longer route p1 → p5→ p2 (latency =2) as indicated by the flow information. Hence, we now have only two possible receivers, namely, p3 and p4.

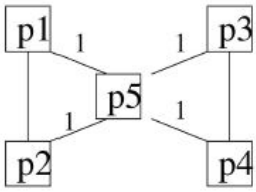


Figure 1: Tracing voice calls.

```
TRACE(Graph G=⟨V, E⟩, Caller src)
(1)   for each vertex v ∈ V
(2)       f[v] = 0; label[v] = false
(3)   end for
(4)   f[src] = 1; label[src] = true
(5)   while pick a vertex v labeled true
(6)       label[v] = false
(7)       for each node u such that (u, v) ∈ E
(8)           if (f[u] = 0)
(9)               f[u] = 1; label[u] = true
(10)          end if
(11)      end for
(12)  end while
```

Naive Tracing Algorithm

SHORTEST PATH TRACING

In this section, we describe techniques to generate a directed sub graph G1 (E1, V1), from G which encodes the shortest path nature of the voice paths. Given a graph G and a caller source, we construct a sub graph G1 that contains only those voice paths that respect the shortest path property. Figure 2 uses a breadth first search on G to compute G1.One can formally show that the directed graph G1 satisfies the following properties: 1) if the voice traffic from source were to traverse an edge e does not belongs to E1, and then it violates the shortest path property. 2) All voice paths that respect the shortest

path property are included in G1. 3) The graph G1 is acyclic

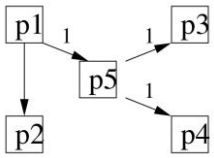


Figure 2: Shortest Path Tracing Algorithm

```
SHORTEST PATH TRACING(Graph G=⟨V, E⟩, Caller src)
(1)   for each vertex v ∈ V
(2)       dist[v] = ∞; label[v] = false; prev[v] = null
(3)   end for
(4)   dist[src] = 0; label[src] = true
(5)   while pick a labeled vertex v with minimum dist[v]
(6)       label[v] = false
(7)       for each node u such that (u, v) ∈ E
(8)           if (dist[u] < dist[v] + w(u, v))
(9)               dist[u] = dist[v] + w(u, v)
(10)              prev[u] = {v}; label[u] = true
(11)          end if
(12)          if (dist[u] = dist[v] + w(u, v))
(13)              prev[u] = prev[u] ∪ {v}
(14)          end if
(15)      end for
(16)  end while
(17)  G^1 = ⟨V^1, E^1⟩: V^1 = V, E^1 = (u → v) ∀u ∈ prev[v], ∀v ∈ V
```

VOIP PRIVACY USING k-ANONYMITY

In this section, we develop a k-anonymity approach to protect the identity of a receiver from flow analysis attacks. We define k-anonymity for identical voice flows as follows:

K-ANONYMITY: A voice flow from source to destination is said to be k-anonymous if the size of a candidate receiver set identified by an adversary using the naive tracking algorithm is no smaller than k. One way to achieve k-anonymity is to mix a flow from source to destination with k -1 dummy voice flows; however, this approach can increase aggregation bandwidth consumption by k-fold. In this section, we propose an anonymity-aware route setup protocol. AARSP reroutes and mixes existing voice flows (without adding dummy traffic) with the goal of 1) meeting k-anonymity, and 2) satisfying latency-based QoS guarantee.

CONCLUSIONS

In this paper, we have addressed the problem of providing privacy guarantees in peer-to-peer VoIP networks. First, we have developed flow analysis attacks that allow an external observer to identify a small and accurate set of candidate receivers even when all the nodes in the network are honest. We have used network flow analysis and statistical inference to study the efficacy of such an attack. Second, we have developed mixing-based techniques to provide a guaranteed level of anonymity for VoIP clients. We have developed an anonymity-aware route setup protocol that allows clients to specify personalized privacy requirements for their voice calls using a quantifiable k-anonymity metric. We have implemented our proposal on the client and presented detailed experimental evaluation that demonstrates the performance and scalability of our protocol, while meeting customizable privacy guarantees.

REFERENCES

[1] "Skype—The Global Internet Telephone Company," http://www.skype.com, 2010. [1] K. Romer and F. Mattern, "The design space of wireless sensor networks," IEEE Wireless Communications, vol. 11, no. 6, pp. 54–61, December 2004.

[2] M.J. Freedman and R. Morris, "Tarzan: A Peer-to-Peer Anonymizing Network Layer," Proc. Ninth ACM Conf. Computer and Comm. Security (CCS), 2002.

[3] D. Goldschlag, M. Reed, and P. Syverson, "Onion Routing for Anonymous and Private Internet Connections," Comm. ACM, vol. 42, no. 2, 1999.

[4] G.I. Sound, "VoIP: Better than PSTN?" http://www.globalip sound.com/demo/tutorial.php, 2010.

[5] V. Shmatikov and M.H. Wang, "Timing Analysis in Low Latency Mix Networks: Attacks and Defenses," Proc. 11th European Symp. Research in Computer Security (ESORICS), 2006.

[6] X. Wang, S. Chen, and S. Jajodia, "Tracking Anonymous Peer-to-Peer VoIP Calls on the Internet," Proc. 12th ACM Conf. Computerand Comm. Security (CCS), 2005.

❑❑❑

Location Aware Cluster based Routing in Wireless Sensor Networks

S. Jerusha, K.Kulothungan & A. Kannan

Department of Information Science and Technology , Anna University, Chennai, India
E-mail : jerujere@gmail.com, Kulo_tn@annauniv.edu & kannan@annauniv.edu

Abstract - Wireless sensor nodes are usually embedded in the physical environment and report sensed data to a central base station. Clustering is one of the most challenging issues in wireless sensor networks. This paper proposes a new cluster scheme for wireless sensor network by modified the K means clustering algorithm. Sensor nodes are deployed in a harsh environment and randomly scattered in the region of interest and are deployed in a flat architecture. The transmission of packet will reduce the network lifetime. Thus, clustering scheme is required to avoid network traffic and increase overall network lifetime. In order to cluster the sensor nodes that are deployed in the sensor network, the location information of each sensor node should be known. By knowing the location of the each sensor node in the wireless sensor network, clustering is formed based on the highest residual energy and minimum distance from the base station. Among the group of nodes, one node is elected as a cluster head using centroid method. The minimum distance between the cluster node's and the centroid point is elected as a cluster head. Clustering of nodes can minimize the residual energy and maximize the network performance. This improves the overall network lifetime and reduces network traffic.

Keywords*: wireless sensor network; distance estimation; clustering; K means; Centroid point; routing.*

I. INTRODUCTION

A Wireless Sensor Network (WSN) is a collection of sensor nodes, capable of collecting information from their environment. These nodes have the ability of sensing, computing, and wireless communicating. Wireless sensor networks are widely being used in different environments to perform various monitoring tasks such as search, rescue, disaster relief, target tracking and a number of tasks in smart environments. In many such tasks, Clustering is one of the fundamental challenges in wireless sensor network.

By knowing the location of a sensor node, cluster the sensor nodes based on the highest energy and least distance. In that group of nodes, one node is select as a Cluster head (CH). This is to avoid communication over head between the sensor nodes. Clustering of nodes shows that the network is more stable and efficient. This increases the overall network lifetime and reduces traffic of the network. Each node in a cluster can directly communicate with their Cluster head. The Cluster head can forward the sensed information to the Base station (BS) through other Cluster heads.

Sensor nodes are battery-constrained and inexpensive nodes. They have limited communication, processing and memory storage resources. Each sensor node can act as a cluster head or a cluster member. A cluster member directly communicates with its cluster head; there is no communication between sensors. In other words, there is 1-hop communication between a node and the CH. Further, Cluster heads can communicate with each other or directly to the base station, and there is multi-hop communication between the Base station and the Cluster head.

In this paper a modified K means clustering algorithm is used to cluster the sensor nodes based on highest energy and shortest path distance. Centroid method is used to find the Cluster mean. The least distance between the Cluster mean and the Cluster member is select as a Cluster head.

The remainder of this paper is structured as follows: Section II provides the related work in the domain of Clustering of nodes in the WSN. It gives the different techniques used for Clustering in WSN. Section III provides detail about how the proposed system is implemented and describes the algorithm used. It includes system architecture and detailed design of various phases involved in the project. It describes the internal working of the system. Section IV deals with the performance evaluation. Finally, Section V describes the conclusion and future enhancement.

II. RELATED WORK

Shahram Babaie, Ahmad Khadem Zade and Ali Hosseinalipour have proposed a [5] new clustering method for increasing of network lifetime. Several sensors are distributed with a high-energy for managing

the cluster head and to decrease their responsibilities in network. The performance of the proposed algorithm via computer simulation was evaluated and compared with other clustering algorithms like LEACH (Low energy Adaptive Clustering Hierarchy) and SEP (Stable Election Protocol). The simulation results show the high performance of the proposed clustering algorithm. In this paper sensor nodes and gateways are fixed and motionless.

Wei Peng and David J Edwards have proposed a novel cluster-head selection algorithm [8] is presented and analyzed which uses the minimum mean distance between sensor nodes as a selection parameter. The proposed algorithm has clear advantages and takes 1.2 times longer to reach the point where 50% sensor nodes remain alive than the Low Energy Adaptive Clustering Hierarchy algorithm (LEACH) while maintaining information throughput at a high level. This minimizes the energy consumption.

Dragos Niculescu and Badri Nath have proposed an Ad Hoc Positioning System (APS) Using AOA. In APS [1] a reduced number of beacon nodes (e.g., three or more) is deployed with the unknown nodes. Then each node estimates its distance to the beacon nodes in a multihop way. Once these distances are estimated, the nodes can compute their positions using trilateration. Three methods of hop-by-hop distance propagation are proposed: Dv-Hop, Dv-Distance, and Euclidean. In Dv-Hop APS the beacon nodes start the propagation of their position information. Working as an extension of the distance vector algorithm, all nodes receive the position information of all beacon nodes as well as the number of hops to these beacons. An advantage of the APS is that its localization algorithm requires a low number of beacon nodes in order to work. However, the way distances are propagated, especially in Dv-Hop and Dv-Distance, as well as the way these distances are converted from hops to meters in Dv-Hop, result in erroneous position computation, which increases the final localization error of the system.

Inderjit S. Dhillon, Yuqiang Guan and Brian Kulis have proposed Kernel k-means, [3] Spectral Clustering and Normalized Cuts. Kernel k-means and spectral clustering have both been used to identify clusters that are non-linearly separable in input space. Weighted kernel k mean's spectral clustering algorithm with normalized cuts are used to group the sensor node. Nodes are clustered by using positive definite matrices. It is also applicable for non-linear environment. It is not suitable for indefinite matrices. It's only suitable for positive definite matrices.

Zhexi Pan, Yuanyuan Yang and Dawei Gong have proposed a [10] distributed clustering algorithms for WSNs by taking into account of the lossy nature of wireless links. First formulate the one-hop clustering problem that maintains reliability as well as saves energy into an integer program and prove its NP hardness. Then propose a metric based distributed clustering algorithm to solve the problem and adopt a metric called selection weight for each sensor node that can indicate both link qualities around the node and its capability of being a cluster head. Further extend the algorithm to multi-hop clustering to achieve better scalability.

Veena, K.N. and Vijaya Kumar have proposed a method for clustering and their analysis to study the cluster formation, their behavior with respect to the system parameters and applications requirement. The most important challenge in Wireless Sensor Networks (WSNs) is to improve the operational efficiency in highly resource constrained environment based on dynamic and unpredictable behavior of network parameters and applications requirement. The technique involves the adoption of computational intelligence to form clustering. Nero-Fuzzy technique [7] is used to obtain dynamic clustering. The simulations are carried out to evaluate the performance of the proposed method with respect to different parameters of sensor node and applications requirement.

The large-scale deployment of wireless sensor networks (WSNs) and the need for data aggregation necessitate efficient organization of the network topology for the purpose of balancing the load and prolonging the network lifetime. Clustering has proven to be an effective approach for organizing the network into a connected hierarchy. Younis, O, Krunz, M. and Ramasubramanian [9] have discussed about the challenges in clustering a WSN, the design rationale of the different clustering approaches and classify the proposed approaches based on their objectives and design principles and several key issues that affect the practical deployment of clustering techniques in sensor network applications.

Geographic routing has been proven to be efficient to provide scalable unicast routing in resource-constrained sensor networks. However, its applications in multicast routing remain largely unexplored. Recently GMR (Geographic Multicast Routing) and DCGM (Destination Clustering Geographic Multicast) have been proposed by Gang Zhao, Xiangqian Liu and Kumar, [2] which preserve the distributed computation of geographic routing while delivering data packets to multiple destinations with efficient routes. To further reduce the number of transmissions, a clustering strategy is applied to GMR and DCGM. This strategy improves the performance of GMR and DCGM by dividing the destinations into many clusters and sending the packet first to the closest destination in each cluster,

which then sends the packet to other nodes in the cluster. Simulation results show that the strategy can reduce the number of transmissions up to 35% percent.

Seema Bandyopadhyay and Edward J. Coyle have proposed a distributed, randomized clustering algorithm [6] to organize the sensors in a wireless sensor network into clusters. A wireless network consisting of a large number of small sensors with low-power transceivers can be an effective tool for gathering data in a variety of environments. The data collected by each sensor is communicated through the network to a single processing center that uses all reported data to determine characteristics of the environment or detect an event. The communication or message passing process must be designed to conserve the limited energy resources of the sensors. Clustering sensors into groups, so that sensors communicate information only to cluster heads and then the cluster heads communicate the aggregated information to the processing center, may save energy. This algorithm is extended to generate a hierarchy of cluster heads and observe that the energy savings increase with the number of levels in the hierarchy. Results in stochastic geometry are used to derive solutions for the values of parameters of our algorithm that minimize the total energy spent in the network when all sensors report data through the cluster heads to the processing center.

Kihyum Kim, Honggil Lee, Byeongjik Lee, Youngmi Baek and Kijun Han have proposed [4] an Energy Efficient Intersection Routing Protocol in Mobile Sensor Networks. Typically, sensor networks consist of fixed sensor nodes. Sometimes, creating such a fixed sensor networks could be a daunting task. Sensor nodes assume deploying a stationary sensor network over a dangerous area such as a battlefield. Even if an advanced method to make the deployment safer is used, diverse element will cause a coverage holes. Even though perfect coverage can be achieved initially, various factors such as malicious attacks will certainly degrade network coverage as time goes on. However, mobile sensor networks can solve some of the problems. Each node of mobile sensor network is mounted on various unmanned vehicles as a result the sensor nodes have mobility. Mobility reinforces fault-tolerance and the scalability of the network. But conventional sensor routing protocols find it hard to deal with the mobile sensor networks. Therefore, this study suggests an energy efficient routing scheme by using the location information of a global positioning system (GPS) and the energy levels of sensor nodes.

III. PROPOSE SCHEME

The location aware cluster based routing uses three phases in wireless sensor networks. In the first phase, the location information of each sensor node is computed by using the localization algorithm such as Trilateration, Triangulation etc; in the second phase, the sensor nodes are clustered to minimize the residual energy and maximize the network performance then the Cluster head is elected based on the minimum distance between the cluster node's and the centroid; in the third phase, Routing takes place between the cluster head and the cluster members and also between the cluster head and the base station.

A. Location of Sensor node

The location information of each sensor node should be known to form a cluster in the wireless sensor network. The nodes which are deployed in the sensor network, knows their location information. The coordinates (x_i, y_i) of each sensor node are used to estimate the distance between two sensor nodes. Based on minimum distance and highest residual energy, the sensor nodes are clustered by using Modified K means clustering algorithm.

When a node has information about distances or angles and positions, it can compute its own position using any one of the localization method. Several methods can be used to compute the position of a node such as trilateration, multitrilateration, triangulation etc.

Trilateration is a geometric principle which is used to find a location, if their distances from other nodes are known. It computes a node's position via the intersection of three circles. To calculate the unknown node's location, trilateration uses the known locations of two or more reference points, and the measured distance between the unknown node and each reference point. To accurately and uniquely determine the relative location of a node using trilateration, generally at least three reference points are needed. The three reference nodes are assumed like a GPS enabled node.

The distance between reference nodes is computed by using this formula,

$$Distance = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2} \quad (1)$$

Where, (x_1, y_1) and (x_2, y_2) are the coordinates of the reference node.

The new coordinate is computed by using this formula,

$$x = \frac{y(y_a - y_b) - V_b}{(x_b - x_c)} \quad (2)$$

$$y = \frac{V_b\,(x_b - x_c) - V_a(x_b - x_a)}{(y_a - y_b)(x_b - x_c) - (y_c - y_b)(x_b - x_c)} \quad (3)$$

Where,

x, y is the new coordinate.

V_a and V_b are the relative distance between two spheres.

x_a, x_b, x_c and y_a, y_b, y_c are the x and y coordinates of three reference points.

TABLE 1: LOCATION INFORMATION OF SENSOR NODE

LOCATION INFORMATION		
Node ID	X_i	Y_i
Node 1	200	300
Node 2	460	580
Node 3	300	600
Node 4	350	480

B. Cluster Formation

K means is an exclusive clustering algorithm and it is the one of the simplest unsupervised learning algorithms that solve the clustering problem. Wireless Sensor Network has number of nodes, which are randomly scattered over the sensor network. The location information of each node is required, because it is essential to know where the information is sensed in the sensor network. The sensor nodes which are deployed in the sensor network, knows their location information. The coordinates (x_i, y_i) of each sensor node are used to estimate the distance between two sensor nodes. Based on minimum distance and highest energy, the sensor nodes are clustered by using Modified K means clustering algorithm.

In the first step, randomly select c cluster head with their x_i, y_i coordinates. Then calculate the distance between each sensor node and the randomly selected cluster head and also get the energy of each node. Assign the sensor nodes to the cluster head whose distance from the cluster head is minimum of all the cluster heads and has the highest residual energy. In the next step, re-compute the cluster head by using centroid method. Calculate the sum of all x coordinate of sensor node in the cluster and divide it by the number of cluster nodes, similarly for y coordinate. This is the centroid method.

Cluster head selection:

After the formation of cluster, re-compute the centroid of the clusters resulting from the calculated distance. Calculate the centroid point of each cluster in the wireless sensor network. The centroid point is the new coordinate which is not equal to any position of sensor node in the wireless sensor network. So, this new coordinate cannot be select as a cluster head, because it is a location based clustering scheme. The current position of the cluster head should be known. After finding the centroid position, find the minimum distance between the centroid position and the cluster members. The sensor nodes which have the minimum distance from the centroid point is a new cluster head. In some cases, if a cluster head gets down, when the threshold value becomes less than the fixed threshold value, recompute the cluster head based on minimum distance and highest energy.

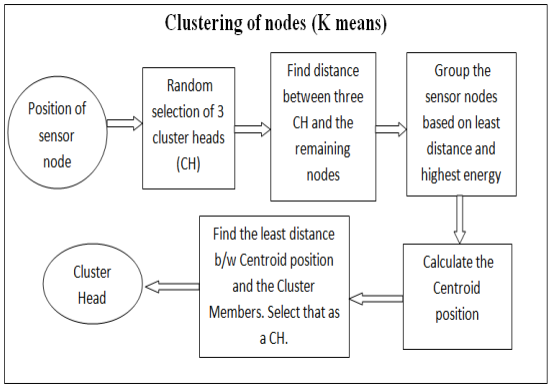


Figure 1 System architecture

C. Routing Protocol

Routing is the process of selecting paths in a wireless sensor network along which to send network traffic. Ad-hoc On Demand Distance Vector (AODV) is a distance vector routing protocol. It is a reactive routing protocol; therefore, routes are determined only when needed. In this paper, the modified K means Clustering algorithm is added to the existing AODV protocol, to form a new K-AODV where K represents the K means clustering algorithm.

Routing takes place between the cluster head and the cluster members and also between the cluster head and the base station. There is no direct communication between the cluster members and the base station. The Cluster members forward the packets to the respective cluster heads and the cluster head will forward the packets to the base station. If the base station is far away from the cluster head, multihop communication will takes place. The cluster head will forward the packets to the nearest cluster head and this nearest cluster head will send the packets to the base station.

Algorithmic steps for Modified k-means clustering:

Input : Position of each node and their distance and energy Output : Grouping of nodes

Let $X = \{x_1, x_2, x_3, \ldots\ldots, x_n\}$ be the set of nodes and $C = \{c_1, c_2, \ldots\ldots, c_n\}$ be the set of centers.

Step 1: Randomly select *'c'* cluster centers.

Step 2: Calculate the distance between each node and cluster centers and also get the energy of each node.

$$D = \sum_{i=1}^{c} \sum_{j=1}^{ci} (\|x_n - c_n\|)2$$

where, 'D' is the distance between each node and the cluster centers.

'$\|x_n - c_n\|$' is the Euclidean distance between x_n and c_n.

'c_i' is the number of nodes in i^{th} cluster.

'c' is the number of cluster centers.

Step 3: Assign the node to the cluster center whose distance from the cluster center is minimum of all the cluster centers and has highest energy.

Step 4: Recalculate the new cluster center using:

$$C(x) = \left(\frac{1}{ci}\right) \sum_{j=1}^{ci} xi \qquad (5$$

Similarly for y coordinate.

$$C(y) = \left(\frac{1}{ci}\right) \sum_{j=1}^{ci} yi$$

where,

C(x) and *C(y)* is the x and y coordinates of the cluster centre.

c_i represents the number of sensor node in i^{th} cluster.

xi represents the x coordinate of the sensor node.

yi represents the y coordinate of the sensor node.

Step 5: Calculate the minimum distance between the Centroid position and the cluster nodes. Then elect it as a new Cluster head.

Step 6: If no node was reassigned then terminate the process, otherwise repeat from step 3.

IV. PERFORMANCE EVALUATION

The simulation of Clustering is done in ns2. In the simulation model, there are 30 sensor nodes deployed in a 800x600 m^2 field. All the nodes are set as static nodes. The type of the wireless propagation model is TwoRayGround. Routing protocol which is used in this simulation is AODV. Table 1 shows the various parameters used for simulation.

TABLE 2: SIMULATION PARAMETERS

Parameter	*Value*
Number of nodes	30 nodes
Mac Layer Type	802.11
Topology size	800 x 600 (mxm)
Routing protocol	AODV
Propagation model	TwoRayGround
Energy model	Energy Model

The graph shows the overall network energy before the formation of cluster and after the formation of cluster using modified k means algorithm.

TABLE 3: OVERALL NETWORK ENERGY

ENERGY EFFICIENCY		
Time	*Energy - AODV*	*Energy –K means*
5	30	30
10	28	29
15	27	28
20	26	27
25	25	26
30	22	25
35	20	24
40	18	24

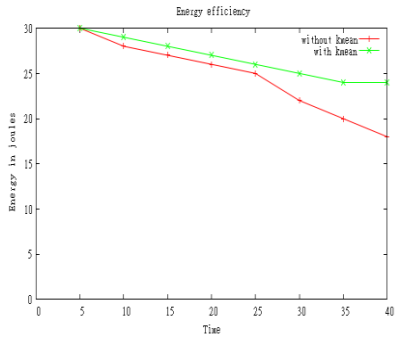


Figure 3 Overall network energy

This graph shows the packet delivery ratio, before and after using k means algorithm. This shows the better performance of packet delivery after using the modified k means clustering algorithm.

TABLE 4: PACKET DELIVERY RATIO

PACKET DELIVERY RATIO		
No. of nodes	***% of packets successfully delivery -AODV***	***% of packets successfully delivery – K means***
5	50000	50000
10	48000	50000
15	45000	48000
20	40000	47000
25	30000	45000
30	25000	40000

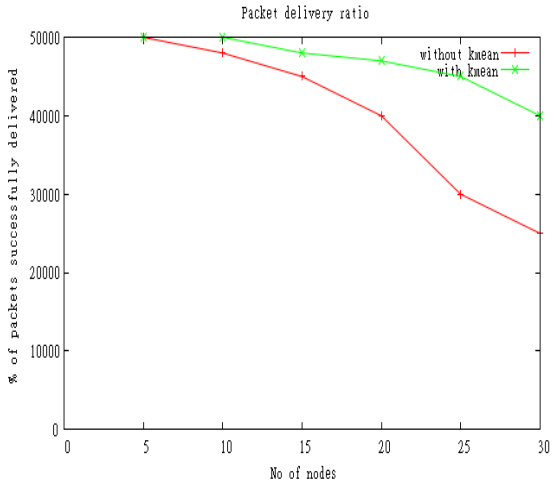


Figure 4 Packet delivery ratios

V. CONCLUSION

Clustering is an important issue in Wireless Sensor Network. Information gathering and routing are carried out based on the position of the sensor node. It can be easily achieved by enabling GPS in every node. The sensor nodes are deployed in the wireless sensor network which aware of their own position information. By knowing the position of the entire sensor node in the WSN, cluster the sensor nodes based on the energy, shortest path distance. The cluster head will be selected based on Centroid position Clustering of nodes by using modified k means clustering algorithm can minimize the residual energy and maximize the performance. It improves the network lifetime and reduces network traffic.

Future Work:

Wireless sensor networks are widely being used in location monitoring, military surveillance etc. In these cases, the information transmitted from the nodes to the base station should be secure (i.e.) communication between two nodes must be encrypted. This requires the generation of secure keys between the sensor nodes in the wireless sensor networks to avoid attackers.

REFERENCES

[1] Dragos Niculescu and Badri Nath "Ad Hoc Positioning System (APS) Using AOA" IEEE Conference on Computer and Communication Societies, INFOCOM 2003.

[2] Gang Zhao, Xiangqian Liu and Kumar, A., "Geographic Multicast with K-Means Clustering for Wireless Sensor Networks" IEEE Conference on Vehicular Technology, on page(s): 233 - 237 VTC Spring 2008.

[3] Inderjit S. Dhillon, Yuqiang Guan and Brian Kulis "Kernel k-means, Spectral Clustering and Normalized Cuts" ACM, International Conference on knowledge discovery and data mining 2004.

[4] Kihyum Kim, Honggil Lee, Byeongjik Lee, Youngmi Baek and Kijun Han, "A Location Based Energy Efficient Intersection Routing Protocol in Mobile Sensor Networks" International Conference on Multimedia and Information Technology, IEEE 2008.

[5] Shahram Babaie, Ahmad Khadem Zade and Ali Hosseinalipour "New clustering method to decrease probability of failure nodes and increasing the lifetime in WSNs" International Journal of Computer Science and Information Security (IJCSIS), Vol. 7, No. 2, 2010.

[6] Seema Bandyopadhyay and Edward J. Coyle, "An Energy Efficient Hierarchical Clustering Algorithm for Wireless Sensor Networks" Twenty-Second Annual Joint Conference of the IEEE Computer and Communications, Vol.3, Page(s):1713 - 1723, IEEE INFOCOM 2003.

[7] Veena, K.N., Vijaya Kumar, B.P.," Dynamic clustering for Wireless Sensor Networks: A Neuro-Fuzzy technique approach" International Conference on Computational Intelligence and Computing Research (ICCIC), No. 1-6, IEEE 2010.

[8] Wei Peng and David J Edwards "K-Means Like Minimum Mean Distance Algorithm for wireless sensor networks" International Conference on Computer Engineering and Technology (ICCET), Vol.1,No.120 -124, 2010.

[9] Younis, O., Krunz, M.and Ramasubramanian, S., "Node clustering in wireless sensor networks: recent developments and deployment challenges" IEEE journals on Network, Volume: 20, Page(s): 20 – 25, IEEE 2006.

[10] Zhexi Pan, Yuanyuan Yang and Dawei Gong "Distributed Clustering Algorithms for Lossy Wireless Sensors" 9th IEEE International Symposium on Network Computing and Applications (NCA), 2010.

[11] Saeed Mehrjoo, Hassan Aghaee, Hossein Karimi , "A Novel Hybrid GA ABC based Energy Efficient Clustering in Wireless Sensor Network" Canadian Journal on Multimedia and Wireless Networks Vol. 2, No. 2, April 2011.

❑❑❑

Tracking of Moving Object in Wireless Sensor Network

D.Charanya & G.V.Uma
Department of Information Science and Technology, Anna University, Chennai, India
E-mail : charanya.march@gmail.com umagv23@gmail.com

Abstract - A Wireless Sensor Network is a collection of sensor nodes distributed into a network to monitor the environmental conditions and send the sensed data to the Base Station. Wireless Sensor Network is one of the rapidly developing area in which energy consumption is the most important aspect to be considered while tracking, monitoring, reporting and visualization of data. An Energy Efficient Prediction-based Clustering algorithm is proposed to track the moving object in wireless sensor network. This algorithm reduces the number of hops between transmitter and receiver nodes and also the number of transmitted packets. In this method, the sensor nodes are statically placed and clustered using LEACH-R algorithm. The Prediction based clustering algorithm is applied where few nodes are selected for tracking which uses the prediction mechanism to predict the next location of the moving object. The Current Location of the target is found using Trilateration algorithm. The Current Location or Predicted Location is sent to active Cluster Head from the leader node or the other node. Based on which node send the message to the Cluster Head, the Predicted or Current Location will be sent to the base station. In real time, the proposed work is applicable in traffic tracking and vehicle tracking. The experiment is carried out using Network Stimulator-2 environment. Simulation result shows that the proposed algorithm gives a better performance and reduces the energy consumption.

Keywords - *Wireless Sensor Networks; LEACH-R; tracking; prediction; trilateration*

I. INTRODUCTION

Wireless Sensor Networks (WSN) is group of heterogeneous sensor nodes which are small, low cost, placed randomly and conn0ected by wireless media to form a sensor field. The sensors are spatially distributed to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants and to cooperatively pass their data through the network to the Base Station (BS). WSN has the ability to dynamically adapt to changing environments.

Object tracking is one of the challenging and non trivial applications for Wireless Sensor Network in which network of wireless sensors are involved in the task of tracking a moving object. Several factors are considered when developing algorithms for tracking moving objects include single vs. multiple targets, stationary vs. mobile nodes, target motion characteristics, energy efficiency and network architecture. Object Tracking is widely used in many applications like military application, commercial applications, field of surveillance, intruder application and traffic applications.

There are various metrics for analysing object tracking such as cluster formation, tracking accuracy, cluster head life time, miss rate, total energy consumed, distance between the source and object, varying speed of the target, etc. The open issues in object tracking are detecting the moving object's change in direction, varying speed of the target, target precision, prediction accuracy, fault tolerance and missing target recovery. In all tracking process, more energy is consumed for messages or data transmission between the sensor nodes or between the sensor and sink.

In a target tracking application, the sensor nodes which can sense the target at a particular time are kept in active mode, while the remaining nodes are to be retained in inactive mode so as to conserve energy until the target approaches them. To continuously monitor mobile target, a group of sensors must be turned in active mode just before target reaches to them. The group of active sensor nodes varies depending on the velocity of moving object and the schedule by cluster head. The sensor nodes detect the moving object and transmit the information to the sink or the base station.

The traditional target tracking methodologies make use of a centralized approach. As the number of sensors increases in the network, more messages are passed on towards the base station and will consume additional bandwidth. Thus, this approach is not fault tolerant as there is single point of failure and lacks scalability. Moreover in traditional target tracking methods, sensing task is usually performed by one node at a time resulting in less accuracy and heavy computation burden on that

node. In WSN, each node has very limited power and consequently traditional tracking methods based on complex signal processing algorithm are not applicable.

Therefore, the object tracking algorithm should be designed in such a way that it result in good quality tracking with low energy consumption. The good quality tracking extends the network lifetime and achieves a high accuracy. In order to obtain an energy efficient tracking with low energy consumption, an assumption is made that all the sensor nodes have same energy level. Because, even if a sensor node fails, other sensor node can take the responsibility and carry out the tracking process.

The remainder of this paper is structured as follows: Section II discusses related work. Section III presents the proposed system, section IV discusses about the performance evaluation and conclusion remarks are given in section V.

II. RELATED WORK

In general, the tracking algorithm is mainly based on the network architecture-Tree based, Cluster based and Prediction based algorithm. Tree-based methods organize the network into a hierarchy tree. Some examples are STUN (Scalable Tracking Using Networked Sensors), DCTC (Dynamic Convoy Tree-based Collaboration) and OCO (Optimized Communication and Organization). H. T. Kung *et al.* [6] have proposed STUN where cost is assigned to each link of network graph, which is computed from the Euclidean distance between the two nodes. Construction of the tree is based on the costs. The leaf nodes are used for tracking the moving target and then sending collected data to the sink through intermediate nodes. Distance travelled by the tracking object is limited (bounded) here.

Wensheng Zhang [14] has proposed DCTC algorithm, dynamically constructs a tree for mobile target tracking and depending on the target location, a subset of nodes participate in tree construction. The tree in the DCTC is a logic tree and does reflect the physical structure of the sensor network. Sam Phu Manh Tran *et al.* Have proposed, OCO [11] is a tree-based method for target tracking that provides self organizing and routing capabilities with low computation overhead on sensor nodes. Authentication and other security features are not considered in OCO.

Li-Hsing Yen *et al.* have proposed, Mobility Profiling Using Markov Chains [7] which estimates the mobility profile (link between nodes and weight of each link) from the historical statistics. By this the problem of energy consumption for update the location information to the sink is reduced, while passing message between the sink and sensor nodes (directly). Cannot get the accurate speed and direct of the objects (random value) and up-to-date information may not be available in the sink.

Some of the examples for Cluster based tracking are RARE, Dynamic Clustering Tracking Algorithm DCTA and Adaptive Dynamic Cluster-based Tracking (ADCT). Wei-Peng Chen *et al.* have proposed, Dynamic clustering algorithm [13] for acoustic target tracking in WSNs, constructs a voronoi diagram for CHs and nearest CH to target in each interval time is the CH that the target is placed in its cell. This CH is selected as active CH. Then active CH broadcasts a packet and nodes that receive this packet reply and send the information that have sensed from target for it. Active CH, calculates current target's location and sends it to the sink. Conflict may occur when more than one CH has the same pre-determined threshold, which lead complication in CH selection.

A cluster-based algorithm for tracking proposed by Khin Thanda Soe has proposed [5] consists of three main phases, target detection, acoustic source localization and target state estimation and tracking. Olule, E. *et al.* have proposed [10] is based on two algorithms, RARE-Area (Reduced Area REporting) and RARE-Node (Reduction of Active node REdundancy). RARE-Area reduces number of nodes participating in tracking and RARE-Node reduces redundant information.

Dan Liu, Nihong Wang *et al.* have proposed, Dynamic cluster based algorithm [2] wake up or slept the sensing nodes though predicting the moving track of the target, reduce the number of tracking nodes to minimize network energy consumption. Selecting the optimal nodes to conduct the tracking task along the predicted moving track though the energy consumption of communication function will guarantee load balancing and extend the network lifetime.

Examples of prediction-based algorithm are PES (Prediction-based Energy Saving), DPR (Dual Prediction-based Reporting) and DPT (Distributed Predicted Tracking) .These methods focus on reduction of energy consumption by keeping most of nodes in sleeping mode.

Yingqi Xu *et al.* have proposed, DPR [17] ,where the next location of target is calculated at both sensor nodes and sink. When the difference between real location and predicted location is acceptable, no update message send to sink and therefore the number of packets transmitted decrease.DPR reduces the energy consumption of radio components by minimizing the number of long distance transmissions between sensor nodes and the base station with a reasonable overhead.

In DPR, both the base station and sensor nodes make identical predictions about the future movements of mobile objects based on their moving history. Error in sensor detection and communication collisions in network is not recoverable.

H. Yang *et al.* have proposed, Distributed Predictive Tracking [DPT] [16], uses separate algorithms for nodes and CHs. The CH uses the target descriptor to identify target and predicts its next location. The protocol uses a clustering based approach for scalability and a prediction based tracking mechanism to provide a distributed and energy efficient solution. The protocol is robust against node or prediction failures which may result in temporary loss of the target and recovers from such scenarios quickly and with very little additional energy use. To achieve low miss rate, the DPT algorithm should be extended.

Mohammad-Taghi Abdizadeh *et al.* have proposed, Adaptive Prediction-based Tracking (APT) [9] scheme is proposed that enables tracking in the sensor network to achieve a certain level of self cognition for modifying the tracking time interval for movement patterns with acceleration, which results in significantly decreasing the network power consumption and achieving a smaller miss probability.

Guojun Wang *et al.* have proposed, Two-level cooperative and energy-efficient tracking algorithm (CET) [4] reduces energy consumption by requiring only a minimum number of sensor nodes to participate in communication, transaction, and perform sensing for target tracking in wireless sensor networks. It is expected that only the nodes adjacent to the target are responsible for observing the target to save the energy consumption and extend the network lifetime as well by using a wakeup mechanism and a face-aware routing.

III. PROPOSED SYSTEM

The proposed work is an energy efficient prediction-based method in a clustered network which consists of nodes at same energy level and range of communication. Initially the nodes are clustered using LEACH-R (LEACH- Reward) protocol in which a node is selected as a Cluster Head (CH). When a target enters the wireless sensor network, the CH that detects the target becomes active while other nodes are in sleep mode. Then the active CH selects three sensor nodes of its members for tracking in which one node is selected as Leader node. The selected nodes sense the target and current target location is calculated using trilateration algorithm.

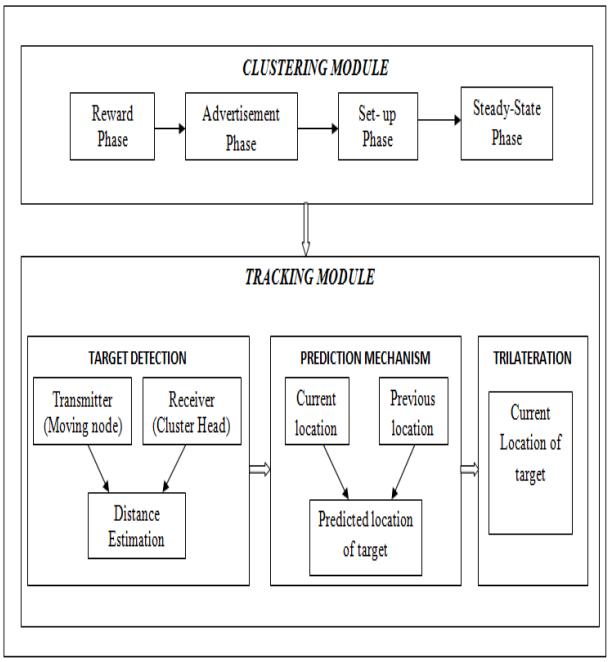


Figure 1: Architecture Diagram

In this algorithm three sensor nodes are selected each time in which two nodes calculates its distance from the moving object and sends the data to the leader node. The localization of the moving object is done by leader node whereas in previous methods it's done by CH.

Using prediction based clustering method energy consumed in the network will be reduced since the transmission power of the nodes is directly proportional to the distances. The three nodes selected for tracking are close to each other, thus the energy consumed for sending a data between the nodes is lower than sending a data from one of the selected nodes to its CH. In LEACH-R, a reward value is calculated by each CH every time in order to eliminate the cluster that has no members and thereby save the energy.

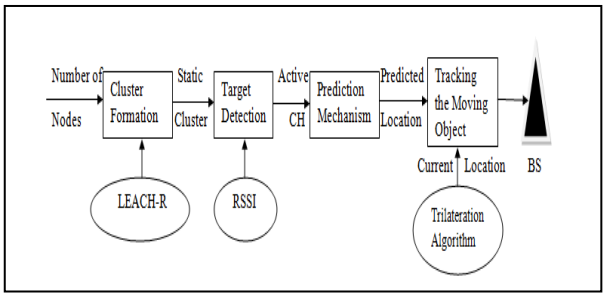


Figure 2: Block Diagram

A. Clustering Of Nodes

Clustering is a technique used to extend the lifetime of a sensor network by reducing energy consumption.The LEACH-R (Low-Energy Adaptive Clustering Hierarchy-Reward) algorithm, involves four phases are as follows

Reward Phase - Reward Calculation

Advertisement - Elections and membership

Set- up phase - Schedule creation

Steady state phase - Data flow between the nodes

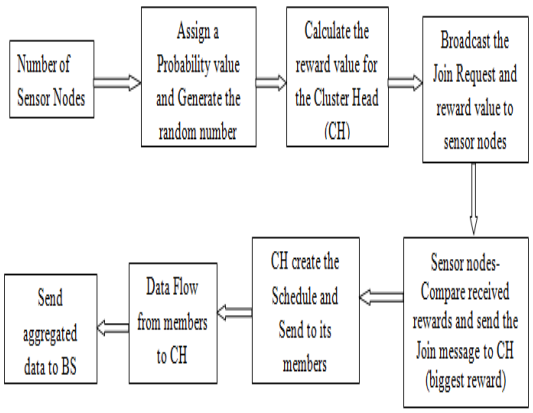


Figure 3: Flow Diagram for LEACH-R

In LEACH-R, each sensor nodes generate a random value x between 0 and 1 which is compared with the probability value P. If the x is less than P, then the node announce itself as CH and calculate its reward values as

$Reward_i = Old\ Reward_i + Cluster\ member + Energy + Distance\ from\ BS$

The relation consist of 4 parts, first is the old reward value assigned for the node. Second part is the members in the cluster. Third part is the energy of the node and last is the distance of the node from the BS.

While broadcasting the reward value is also sent along with the join request. The members join with the CH that has biggest reward by comparing the reward values. Then the CH creates a TDMA schedules for its members and send it to its cluster members. The data flow occurs between members and CH. In LEACH, the cluster that doesn't have members is also considered and schedule is created. By using reward value the CH that doesn't have any members is removed and energy is saved.

B. Target Detection

The target detection is done using Received Signal Strength Indicator [RSSI] method. It estimates the distance between two sensors by measuring the power of the signal transmitted from sender to receiver. Theoretically, the signal strength is inversely proportional to squared distance, and a known radio propagation model can be used to convert the signal strength into distance. The main advantage is its low cost, because most receivers are capable of estimating the received signal strength. In some cases, there may be inaccuracies of distance estimation due to noise and interference.

But, considering its low cost, it is possible that a more sophisticated and precise use of RSSI (e.g., with better transmitters) could become the most used technology of distance estimation. In the Figure3.4, a sender node sends a signal with a determined strength that fades as the signal propagates. The bigger the distance to the receiver node, the lesser the signal strength when it arrives at that node.

C. Prediction Mechanism

A prediction-based algorithm uses a prediction mechanism that predicts the next location of target is a linear prediction method. This mechanism with current and previous location of target, predicts next location of target.

Using (x_i,y_i) and (x_{i-1},y_{i-1}) ,co-ordinates of nodes i and i-1 at time t_i and t_{i-1} the target's speed v and the direction θ is calculated .The predicted location (x_{i+1},y_{i+1}) of the target after the given time t is calculated using the target speed and direction. If the predicted location is within the current cluster, then the active CH selects the three nodes which are nearest to the location. If the predicted location is placed out of the current cluster, active CH selects nearest CH to that location as next active CH and gives the tracking task to the new active CH.

D. Trilateration Algorithm

After receiving the distance message from two other selected nodes, the leader node calculates current location of moving object using trilateration algorithm. Trilateration algorithm forms relation between three nodes and by solving three formed relations the coordinate of target (x,y) is obtained.

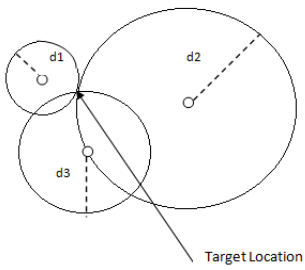


Figure 4: Trilateration Algorithm

In Lateration, the mobile nodes are localized using overlapping circles as shown in Figure 3.5. The circumference radii are equal the estimated distance among nodes.

E. Tracking Of Moving Object

In general, tracking system track the moving targets in a WSN by sensing capability of sensors (like acoustic, vision, thermal). Since sensor nodes have limited battery power and replacement of battery is impossible, energy saving is an issue in tracking process.

Input : Number of nodes

Output : Current location of the Moving Object

Steps 1 : Initially the nodes are clustered using LEACH-R.

Steps 2 : The moving object is detected by the sensor using RSSI and the CH which is close to moving object becomes the Active CH.

Steps 3 : The Active CH uses the prediction mechanism and predict the next location of the moving object as (x_{i+1},y_{i+1}).

Steps 4 : If the predicted location is within the cluster members, then the active CH selects the three nodes to calculate the current location using trilateration algorithm.

Steps 5 : Else if the predicted location is outside the current cluster, then the CH near to the predicted location becomes Active CH and Step 4 is followed.

IV. PERFORMANCE EVALUATION

A. Energy Consumption

In the proposed algorithm the energy consumed is reduced since only activated nodes in the network is involved in tracking and rest of nodes remain in standby mode. Figure 5 show the graph comparing the energy consumption before and after the proposed algorithm.

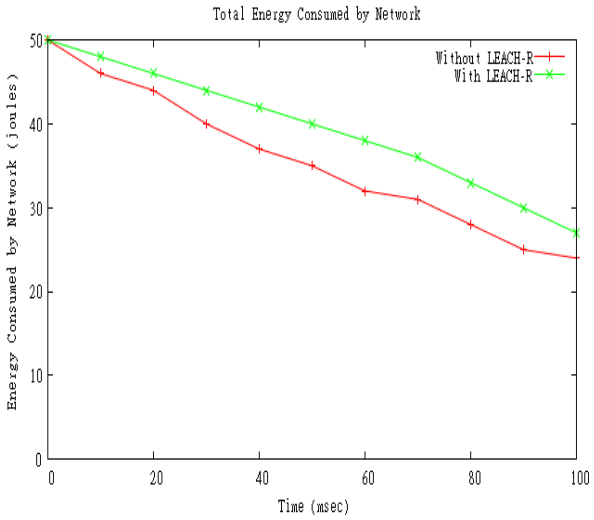


Figure 5: Energy Consumed

B. Number of Alive Nodes

The number of alive nodes decreases as the time increases. In the proposed algorithm, there is a steady decrease in the number of alive nodes.. Figure6 show the comparison by taking time versus number of live nodes as (x,y) co-ordinates.

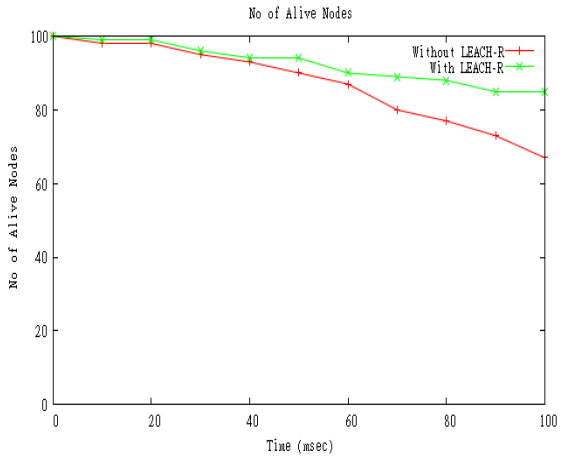


Figure 6: Number of Alive Nodes

C. Network Lifetime

The network lifetime is directly proportional to the number of nodes in the network. Figure 7 show the increase in the network lifetime as number of nodes in the increase.

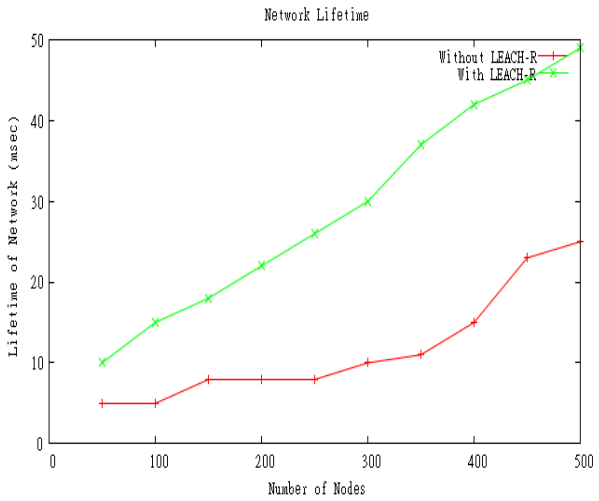


Figure 7 : Network Lifetime

V. CONCLUSION

In this paper, a system is developed in such a way that target tracking in WSN is done in efficient way using an energy efficient prediction- based clustering algorithm. Energy efficient prediction- based Clustering algorithm, reduces the average energy consumed by sensor nodes and thereby increase the lifetime of the network. The tracking of the moving object is accurately done.

Future Work:

As a future enhancement, the tracking algorithm can be extended for multiple targets by forming dynamic clustering. Dynamic cluster reduces overlapping between the inter-clusters and also avoid duplication and unwanted transmission of data. By this method, the tracking accuracy is increased and reduces energy consumed in the network. Then the received data can be analysed and visualized using an effective visualization tool.

REFERENCES

[1] Chih-Yu Lin, Wen-Chih Peng, and Yu-Chee Tseng, "Efficient In-Network Moving Object Tracking in Wireless Sensor Networks" , IEEE Transaction on Mobile Computing, Vol 5,Issue:8 , Pg: 1044 – 1056, August 2006.

[2] Dan Liu, Nihong Wang and Yi An, "Dynamic Cluster Based Object Tracking Algorithm in WSN", 2010 Second WRI Global Congress on Intelligent Systems, vol : 1 ,Pg:397-399, Dec 2010.

[3] Fatemeh Deldar and Mohammad Hossien Yaghmaee, "Designing a Prediction-based Clustering Algorithm for Target Tracking in Wireless Sensor Networks",2011 International Symposium on Computer Networks and Distributed Systems (CNDS), February 23-24, 2011, Page(s): 199 - 203 ,February 2011.

[4] Guojun Wang, Md. Zakirul Alam Bhuiyan and Li Zhang, "Two-level cooperative and energy-efficient tracking algorithm in wireless sensor networks", Concurrency and Computation: Practice and Experience, September 2009.

[5] Khin Thanda Soe, "Increasing Lifetime of Target Tracking Wireless SensorNetworks" ,World Academy of Science, Engineering and Technology 42 2008.

[6] H.T. Kung and D. Vlah, "Efficient Location Tracking Using Sensor Networks", Proceedings of 2003 IEEE Wireless Communications and Networking Conference (WCNC), March 2003 , Page(s): 1954 - 1961 vol.3.

[7] Li-Hsing Yen and Chia-Cheng Yang, "Mobility Profiling Using Markov Chains for Tree-Based Object Tracking in Wireless Sensor Networks" , IEEE Conference on Sensor Network 2006, Vol:6, Pg:220 – 225, June 2006.

[8] R. Mardeni ,Othman and Shaifull Nizam, "Node Positioning in ZigBee Network Using Trilateration Method Based on the Received Signal Strength Indicator (RSSI)",European Journal of Scientific Research 2010, ISSN 1450-216X Vol.46 No.1, Page(s): 048-061 .

[9] Mohammad-Taghi Abdizadeh, Hadi Jamali Rad and Bahman Abolhassani, "A New Adaptive Prediction-Based Tracking Scheme for Wireless Sensor Networks", 2009 Seventh Annual Communication Networks and Services Research Conference, Pg:335-341,May2009.

[10] Olule, E., Guojun Wang, Minyi Guo and Mianxiong Dong," RARE: An Energy-Efficient Target Tracking Protocol for Wireless Sensor Networks", 2007 International Conference on Parallel Processing Workshops (ICPPW 2007), September 2007.

[11] Sam Phu Manh Tran and T. Andrew Yang, "OCO: Optimized Communication & Organization for Target Tracking in Wireless Sensor Networks", IEEE International conference on Sensor network, vol 1, Pg:428-435, June 2006.

[12] Samer Samarah, Muhannad Al-Hajri, and Azzedine Boukerche, "A Predictive Energy-Efficient Technique to Support Object-Tracking Sensor Networks", IEEE Transactions on Vehicular Technology, vol. 60, no. 2, February 2011.

[13] Wei-Peng Chen, Jennifer C. Hou and Lui Sha, "Dynamic Clustering for Acoustic Target Tracking in Wireless Sensor Networks", 11th IEEE International Conference on Network Protocols (ICNP'03), vol:3, Issue:3 ,Pg:258-271, Aug 2004.

[14] WenCheng Yang, Zhen Fu, JungHwan Kim, and Myong-Soon Park*, "An Adaptive Dynamic Cluster-Based Protocol for Target Tracking in Wireless Sensor Networks", APWeb/WAIM'07 Proceedings of the joint 9th Asia-Pacific web and 8th international conference on web-age information management conference on Advances in data and web management Springer-Verlag Berlin, Heidelberg ©2007, pp. 157–167.

[15] Wensheng Zhang, "DCTC: Dynamic Convoy Tree-Based Collaboration for Target Tracking in Sensor Networks", IEEE transactions on wireless communications, vol. 3, no. 5, September 2004.

[16] H. Yang and B. Sikdar, "A Protocol for Tracking Mobile Targets using Sensor Networks", 2003 IEEE International Workshop on Sensor Network, Pg:71-81, May2003.

[17] Yingqi Xu, Julian Winter and Wang-Chien Lee, "Dual Prediction-based Reporting for Object Tracking Sensor Networks", 2004 First Annual International Conference on Networking and services, Pg:154-163,August2004.

[18] Fatemeh Deldar, Mohammad Hossien Yaghmaee, "Energy Efficient Prediction-based Clustering Algorithm for Target Tracking in Wireless Sensor Networks", 2010 International Conference on Intelligent Networking and Collaborative Systems, Pg:315 – 318, November 2010.

❑❑❑

Machine Learning

Ankit Nirwan, Pakshal Bapna, Nagabhairava Venkata Siddartha, Nabankur Sen
SRM UNIVERSITY
E-mail : ankitn55@gmail.com,pakshalbapna007@yahoo.com,
nagabhairavasiddartha@gmail.com,nab.rockstar@gmail.com

Abstract - Learning, like intelligence, covers such a broad range of processes that it is difficult to define precisely.There are several parallels between animal and machine learning. Certainly, many techniques in machine learning derive from the efforts of psychologists to make more precise their theories of animal and human learning through computational models. It seems likely also that the concepts and techniques being explored by researchers in machine learning mayilluminate certain aspects of biological learning.

I. INTRODUCTION

As regards machines, we might say, very broadly, that a machine learns whenever it changes its structure, program, or data (based on its inputs or in response to external information) in such a manner that its expected future performance improves. Some of these changes, such as the addition of a record to a data base, fall comfortably within the province of other disciplines and are not necessarily better understood for being called learning. But, for example, when the performance of a speech-recognition machine improves after hearing several samples of a person's speech, we feel quite justified in that case to say that the machine has learned. Machine learning usually refers to the changes in systems that perform tasks associated with artificial intelligence (AI). Such tasks involve recognition, diagnosis, planning, robot control, prediction, etc. The changes might be either enhancements to already performing systems or synthesis of new systems.

1.1 Wellsprings of Machine Learning

Work in machine learning is now converging from several sources. These different traditions each bring different methods and different vocabulary which are now being assimilated into a more unified discipline. Here is a brief listing of some of the separate disciplines that have contributed to machine learning. Statistics: A long-standing problem in statistics is how best to use samples drawn from unknown probability distributions to help decide from which distribution some new sample is drawn. A related problem is how to estimate the value of an unknown function at a new point given thevalues of this function at a set of sample points. Statistical methodsfor dealing with these problems can be considered instances of machine learning because the decision and estimation rules depend on a corpus of samples drawn from the problem environment. We use Fig. 1.2 to help define some of the terminology used in describing the problem of learning a function. Imagine that there is a function, f, and the task of the learner is to guess what it is. Our hypothesis about the function to be learned is denoted by h. Both f and h are functions of a vector-valued input X = (x1; x2; : : : ; xi; : : : ; xn) which has n components. We think of h as being implemented by a device that has X as input and h(X) as output. Both f and themselves may be vector-valued. We assume a priori that the hypothesized function, h, is selected from a class of functions H. Sometimes we know that false belongs to this class or to a subset of this class. We select h based on a training set, _, of m input vector examples. Many important details depend on the nature of the assumptions made about all of these entities.

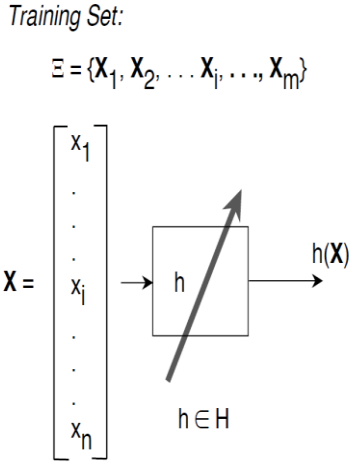
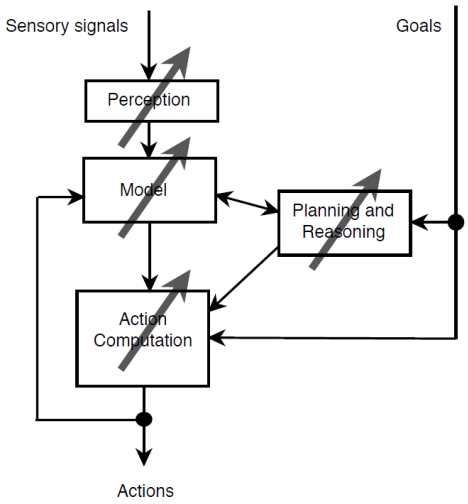


Figure 1.2: An Input-Output Function



Brain Models: Non-linear elements with weighted inputs have been suggested as simple models of biological neurons. Adaptive Control Theory: Control theorists study the problem of controlling a process having unknown parameters which must be estimated during operation. Often, the parameters change during operation, and the control process must track these changes. Psychological Models: Psychologists have studied the performance of humans in various learning tasks.

Evolutionary Models:

In nature, not only do individual animals learn to perform better, but species evolve to be better _t in their individual niches. Since the distinction between evolving and learning can be blurred in computer systems, techniques that model certain aspects of biological evolution have been proposed as learning methods to improve the performance of computer programs. Genetic algorithms [Holland, 1975] and genetic programming are the most prominent computational techniques for evolution.

1.2 Varieties of Machine Learning

Orthogonal to the question of the historical source of any learning technique is the more important question of what is to be learned. In this book, we take it that the thing to be learned is a computational structure of some sort. We will consider a variety of different computational structures: Functions Logic programs and rule sets Finite-state machines Grammars Problem solving systems We will present methods both for the synthesis of these structures from examples and for changing existing structures. In the latter case, the change to the existing structure might be simply to make it more computationally efficient rather than to increase the coverage of the situations it can handle.

II. Learning Requires Bias

To limit a priorities set of hypotheses to quadratic functions and then to insist that the one we choose passed through all four sample points. This kind of a prior information called bias, and useful learning without bias is impossible. We can gain more insight into the role of bias by considering the special case of learning a Boolean function of n dimensions. There are 2n different Boolean inputs possible. Suppose we had no bias; that is H is the set of all 22nBooleanfunctions, and we have no preference among those that the samples in the training set. In this case, after being presented with one member of the training set and its value we can rule out precisely one-half of the members of all those Boolean functions that would misclassify this labeled sample. The remaining functions constitute what is called a version space; As we present more members of the training set, the graph of the number of hypotheses not yet ruled out as a function of the number of different patterns presented is as shown in Fig. 1.4. At any stage of the process half of the remaining Boolean functions have value 1 and half have value 0 for any training pattern not yet seen. No generalization is possible in this case because the training patterns give no clue about the value of a pattern not yet seen. Only memorization is possible here, which is a trivial sort of learning.

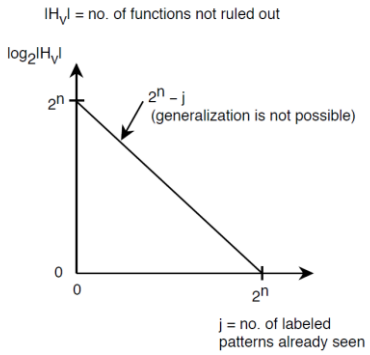


Figure 1.4: Hypotheses Remaining as a Function of Labeled Patterns Presented

III. SAMPLE APPLICATIONS

Rule discovery using a variant of ID3 for a printing industry problem:

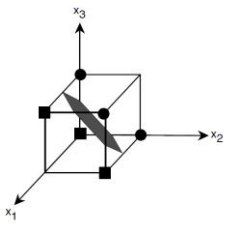


Figure 1.6: A Training Set That Completely Determines a Linearly Separable Function

Electric power load forecasting using a k-nearest-neighbour rule system Automatic “help desk" assistant using a nearest-neighbour system. Planning and scheduling for a steel mill using Expert Ease Classification of stars and galaxies

IV. CONCLUSION

AI research has been concerned with machine learning. Samuel developed a prominent early program that learned parameters of a function for evaluating board positions in the game of checkers. AI researchers have also explored the role of analogies in learning and how future actions and decisions can be based on previous exemplary cases.Recent work has been directed at discovering rules for expert systems using decision-tree methods and inductive logic programming 1991.Another theme has been saving and generalizing the results of problem solving using explanation-based learning.

REFERENCES

[1] Deo Brat Ojha, Ajay Sharma, AbhishekDwivedi, NitinPandey, Amit Kumar, “An Advanced machine leaningl”,International Journal on Advanced Networking and Applications ,vol. 02, Issue: 05, pp. 841-845,2011.

[2] Deo Brat Ojha et al , “A machine learning technique for playing ,International Journal of Computer applications, vol.12-no.9, pp. 22-26,2011.

[3] Nan-Ying Liang, Guang-Bin Huang, P.Saratchandran, and N. Sundararajan,“A fast and accurate online sequential learning algorithm for feed forward networks”,IEEE transactions on neural networks, vol. 17, no. 6,2006.

[4] Ramesha K et al, **“**machine learining”**,** International Journal on Computer Science and Engineering (IJCSE), vol. 02, no.01S, pp.14-23, 2010.

[5] Shermina J,“ machine learning using multilinearprincipal component analysis and locality preservation projection”, IEEE GCC conference and exhibition, Dubai, United Arab Emirates, 2011.

[6] SherminaJ ,“machine leariningbased on Discrete Transform and Principal Component Analysis”, International Conference on Emerging Trends in Electrical and Computer Technology (ICETECT),pp. 826-830, 2011.

❑❑❑

Content Based Image Retrieval: A Novel Approach for Image Recognition

Sarbajit Mukherjee[#1], Moloy Dhar[*2], Agnit Chatterjee[#3]

[#]Computer Science & Engineering, Computer Science & Engineering , Guru Nanak Institute of Technology

E-Mail : [1]mukherjee.sarbajit1990@gmail.com, [2]dhar.moloy@gmail.com & [3]agnit.chatterjee@gmail.com

Abstract - Semantic image analysis is an important component of modern technologies because human depends so much on the visual information than other creatures. This paper affords a method to extract information from input image and then use that information for further analysis. However it is relatively difficult to standardize the segmentation algorithm by considering the variability between images: a limit of segmentation performance. The main objective of our paper is to propose an algorithm on how to extract that relative information out of given images efficiently and then finally use that information to identify the nature of the images. For this purpose we propose the method of edge-based segmentation using the Reconstruction of image, Conversion to L*a*b* colour space, Intensity transformation of images, Sobel edge detection and then extracting the information using the eight-components connected method. Using this extracted information and finally matching it with our trained files in the database we now can identify the nature of the images.

Keywords— *Content-based image retrieval (CBIR), Image Reconstruction, L*a*b* color space, Intensity transformation of images, Image Segmentation, Sobel edge detection, trained database files.*

I. INTRODUCTION

Content-based image retrieval (CBIR), also known as query by image content (QBIC) and content-based visual information retrieval (CBVIR) is the application of computer vision techniques to the image retrieval problem, that is, the problem of searching for digital images in large databases.

There is a growing interest in CBIR because of the limitations inherent in metadata-based systems, as well as the large range of possible uses for efficient image retrieval. Textual information about images can be easily searched using existing technology, but requires humans to personally describe every image in the database. This is impractical for very large databases, or for images that are generated automatically, e.g. from surveillance cameras.

Potential uses for CBIR include:

- Art collections
- Photograph archives
- Retail catalogs
- Medical diagnosis
- Crime prevention
- The military
- Intellectual property
- Architectural and engineering design
- Geographical information and remote sensing systems

Several approaches have been proposed in the literature regarding the tasks of indexing, searching and retrieval of images. Segmentation is one of the first steps in image analysis. It refers to the process of partitioning a digital image into multiple regions (sets of pixels). Each of the pixels in a region is similar with respect to some characteristic or computed property, such as color, intensity, or texture. Many segmentation methods have been proposed in the literature. The choice of a segmentation technique over another and the level of segmentation are decided by the particular characteristics of the problem being considered. Image segmentation is further used in detecting the nature of the images in which the segmented image is matched with some trained files in the database and based upon the matching result the nature is determined.

II. MOTIVATION OF THE WORK

"Content-based" means that the search will analyze the actual contents of the image rather than the metadata such as keywords, tags, and/or descriptions associated with the image. The term 'content' in this context might refer to colors, shapes, textures, or any other information that can be derived from the image itself. CBIR is desirable because most web based image search engines rely purely on metadata and this produces a lot of

garbage in the results Also having humans manually enter keywords for images in a large database can be inefficient, expensive and may not capture every keyword that describes the image. Thus a system that can filter images based on their content would provide better indexing and return more accurate results.

Many CBIR systems have been developed, but the problem of retrieving images on the basis of their pixel content remains largely unsolved

III. THE REMEDIAL STRATEGY PROPOSED

- The new approach of image tagging and recognition is an amalgamation of the best features of both Content Based Image Retrieval and Context Based Image Retrieval techniques.
- It takes the test files and draws the hidden semantics from them and stores them along with the tag entered by the user.
- But the images are not stored as a whole, but are segmented.
- The individual segments of the images are stored along with their feature sets in the database.
- Later on the feature sets of all these indivdual segments are matched with the test image segments.
- The matched segments are then added together.
- The added up object is now serched for in the tagging database based on the cumulative feature sets of all the segments.

IV. IMAGE SEGMENTATION TECHNIQUES

A. Thresholding Methods

Thresholding is the operation of converting a multilevel image into a binary image Le., it assigns the value of 0 (background) or 1 (objects or foreground) to each pixel of an image based on a comparison with some threshold value T (intensity or color value). When T is constant, the approach is called global Thresholding; otherwise, it is called local thresholding. Global thresholding methods can fail when the background illumination is uneven. Multiple thresholds are used to compensate for uneven illumination. Threshold selection is typically done interactively; however, it is possible to derive automatic threshold selection algorithms.

B. Edge-Detection Methods

Edge detection methods locate the pixels in the image that correspond to the edges of the objects seen in the image. The result is a binary image with the detected edge pixels. Common algorithms used are Sobel, Prewitt and Laplacian operators. These algorithms are suitable for images that are simple and noise-free; and will often produce missing edges, or extra edges on complex and noisy images.

C. Region-Based Methods

The goal of region-based segmentation is to use image characteristics to map individual pixels in an input image to sets of pixels called regions that might correspond to an object or a meaningful part of one. The various techniques are: *Local techniques, Global techniques and Splitting and merging techniques.* The effectiveness of region growing algorithms depends on the application area and the input image. If the image is sufficiently simple, simple local techniques can be effective. However, on difficult scenes, even the most sophisticated techniques may not produce a satisfactory segmentation. Over-stringent criteria create fragmentation; lenient ones overlook blurred boundaries and over-merge. Hybrid techniques using a mix of the methods above are also popular.

V. IMAGE SEARCHING TECHNIQUES

Image segmentation can be further used to recognize and/or locate specific objects in an image and for identification of the nature of the images. The image is segmented into its constituent objects using an appropriate image segmentation technique. Then, the matching is performed for a particular part with the trained database files.

A. Methodology

There are two steps which are normally used regarding the searching of images:-

1) Query Builder: Query by example is a query technique that involves providing the CBIR system with an example image that it will then base its search upon. The underlying search algorithms may vary depending on the application, but result images should all share common elements with the provided example.

Options for providing example images to the system include:

- A preexisting image may be supplied by the user or chosen from a random set.
- The user draws a rough approximation of the image they are looking for, for example with blobs of color or general shapes.

This query technique removes the difficulties that can arise when trying to describe images with words.

2) *Information Retrieval*: The ideal CBIR system from a user perspective would involve what is referred to as

semantic or Information retrieval, where the user makes a request like "find pictures of humans" .This type of open-ended task is very difficult for computers to perform. Current CBIR systems therefore generally make use of lower-level features like texture, color, and shape. But not every CBIR system is generic.

Basically there are two approaches for information retrieval:-

1. Content Based image retrieval.
2. Context Based image retrieval

But both these methods are not fully sufficient regarding the extraction of information from the images.

- Difficulty of Content Based Image retrieval can be avoided if a fixed and viable set of features can be extracted.
- These features can then form the result set or the semantics based on which tagging and then searching can take place.
- The hidden semantics will be fairly constant and so tagging will be much more accurate.

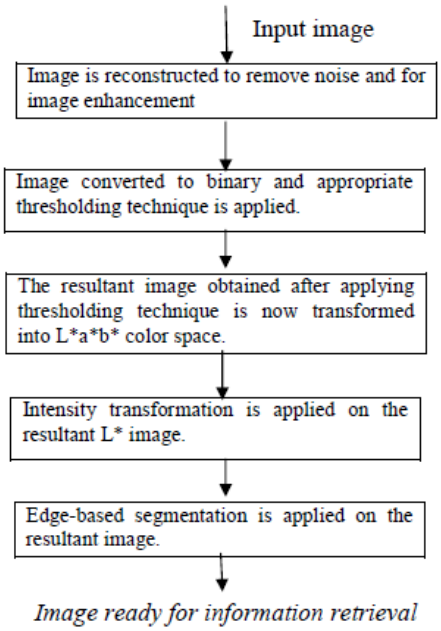
B. Features of an Image that can be used for forming the search semantics :

1) COLOR: Computing color similarity is achieved by computing a color histogram for each image that identifies the proportion of pixels within an image holding specific values. Current research is attempting to segment color proportion by region and by spatial relationship among several color regions.

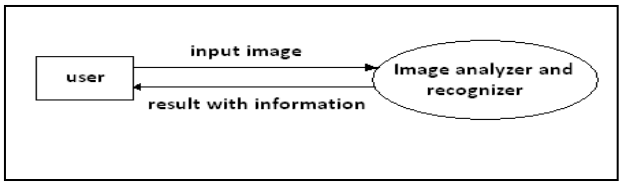
2) TEXTURE: Texture measures look for visual patterns in images and how they are spatially defined. The identification of specific textures in an image is achieved primarily by modeling texture as a two-dimensional gray level variation

3) PIXEL OCCUPANCY: It measures the number of black and number of white pixels in the image and based upon these results the search semantics are formulated.

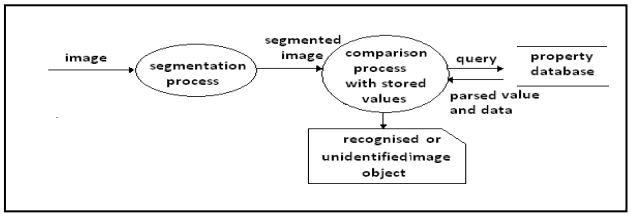
VI. The New Algorithm Proposed



Context Level DFD



Level 1 DFD



A. Image Enhancement and Reconstruction

Fig 1 Original Image

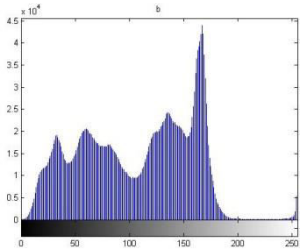


Fig 2 Original Histogram

Fig 3 Reconstructed Image

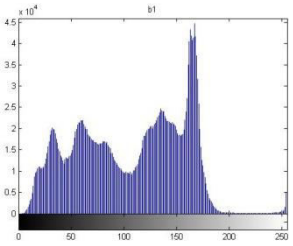


Fig 4 Reconstructed Histogram

*B. Transformation to L*a*b* color space*

Fig 5 L* color space

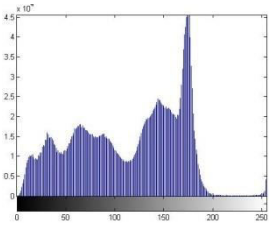


Fig 6 L* Histogram

Fig 7 a* color space

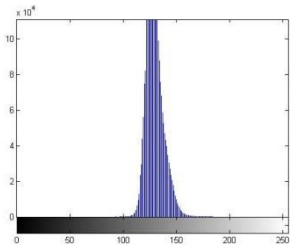


Fig 8 a* Histogram

Fig 9 b* color space

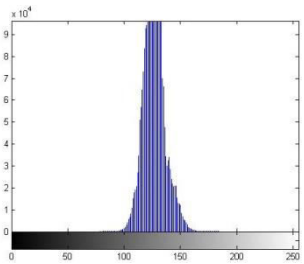


Fig 10 b* Histogram

C. Intensity transformation on the resultant L Image*

The intensity transformation is an important step towards edge-based image segmentation. So choosing appropriate values for the intensity levels becomes an important consideration.

Function *imadjust* is the basic Image Processing Toolbox function for intensity transformations of gray-scale images. The general syntax is :-g = imadjust (f, [low_in high_in], [low_out high_out], gamma)

1) low_in=0.1, low_out=0, high_in=0.85, high_out=0.9, gamma=2

Fig 11

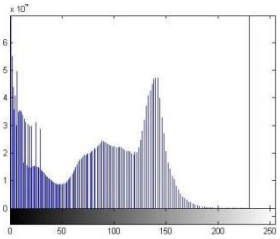
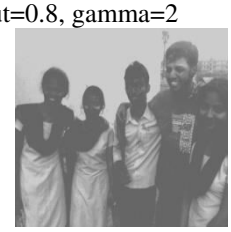


Fig 12

2) low_in=0.25, low_out=0.4, high_in=0.65, high_out=0.8, gamma=2



.Fig-13

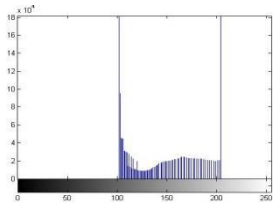


Fig 14

2) low_in=0.1, low_out=0.5, high_in=0.75, high_out=1, gamma=5

Fig 15

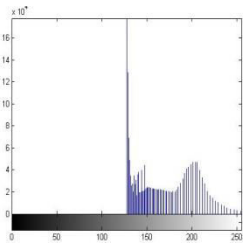


Fig 16

3) low_in=0.1, low_out=0.5, high_in=0.75, high_out=1, gamma=2

Fig 17

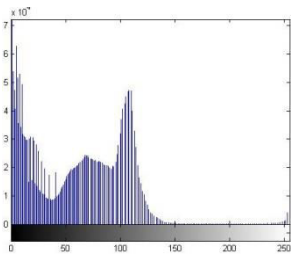


Fig 18

D. Edge based Segmentation using Median Filtering

After choosing the most feasible intensity values now the resultant image thus formed is to be segmented using the SOBEL Edge Detection technique. Now for segmentation an appropriate filtering technique need to be implemented. So for this purpose we have used median filtering.

1) *Median Filtering*

The median filter is an excellent rejecter of certain common kinds of noise, both random superimposed variations and "shot" or impulse noise in which individual pixels are corrupted or missing from the image. If a pixel contains an extreme value, it is replaced by a "reasonable" value, the median value in the neighborhood. This type of noise occurs in CMOS cameras with "dead" transistors that have no output or "locked" ones that always put out maximum signals, and in interference microscopes for points on a surface with a locally high slope that return no light, for example. Dust on scanned film negatives also creates this image defect.

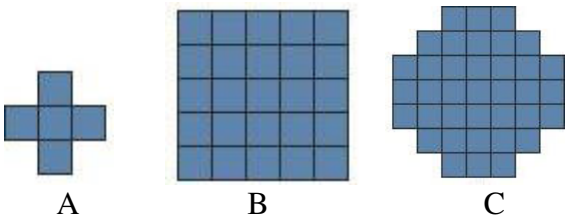
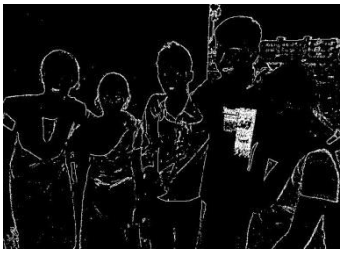
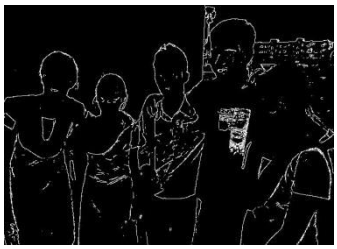


Fig 19: *Neighborhood patterns used for median filtering: (A) 4 nearest-neighbor cross; (B) 5 × 5 square containing 25 pixels; (C) 7 × 7 octagonal region containing 37 pixels.*

I. Using a 3 X 3 Filter



II. Using a 10 X 10 Filter



III. Using a 20 X 20 Filter

VII.SYSTEM TRAINING OR MODUS OPERANDI

STEP 1: The trained file is now segmented into a number of rectangular regions with each part containing a significant part of the image.

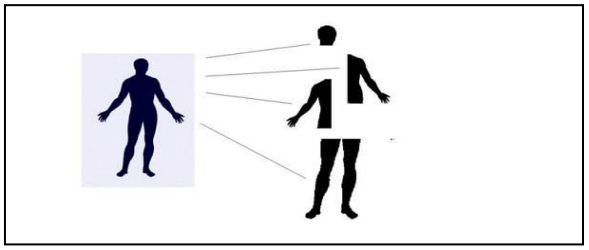


Fig 23: Trained File

STEP 2: The semantic information are extracted from the images (viz. pixel occupancy).

STEP 3: The information about each of these segments is now stored in a database table along with proper tags and a tag value.

STEP 4: The parsed up semantic value of the image (i.e. summed up occupancy value of whole image) is now stored along with proper tags in a second database file.

This completes our system training process.

VIII. EXTRACTING INFORMATION FROM IMAGES

The following steps are followed:-

1) We take the segments of the user provided image.
2) The next step in this approach is to create a new image having a name, one for each segment obtained after the use of the Sobel edge Detection technique.
3) Now, for each of the new images thus obtained from the segments, we find out the percentage of black pixels.
4) Having acquired the percentage of black pixels for each segmented image acquired we determine the sum of all percentage of black pixels.
5) After adding a further 10 to the summation of percentage of black pixels as allowance, we match this value with the values of the training images' values we have already established while creating the database.
6) If there is an exact match found or if the value obtained comes out to be multiple of the training images' values we conclude that the image

provided contains human/humans. Otherwise the assumption can be made that the user image does not contain human/humans.

IX. DATABASE SNAPSHOT

parts

Name	value	Occupancy
human head	1	13.9017
left_hand_wid_body	3	45.5135
right_hand_wid_body	4	39.0558
right_leg	2	19.5301
left_leg	5	18.8568
fig1_hed	1	24.6842
fig1_part1	4	74.3808
fig1_part2	3	74.8115
fig1_part3	2	40.9091
fig1_part4	5	42.4242
fig2_hed	1	20.1162
fig2_part1	4	59.3949
fig2_part2	3	60.0466
fig2_part3	2	26.4682
fig2_part4	5	26.1643

Fig 24: *The table ''parts'' stores the information about individual segments*

objects

picture_nam	value	Field1	Add New Field
Human Figure	15		

X. How the Entire System Works

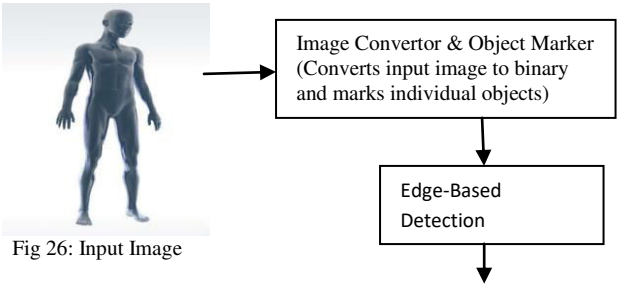


Fig 26: Input Image

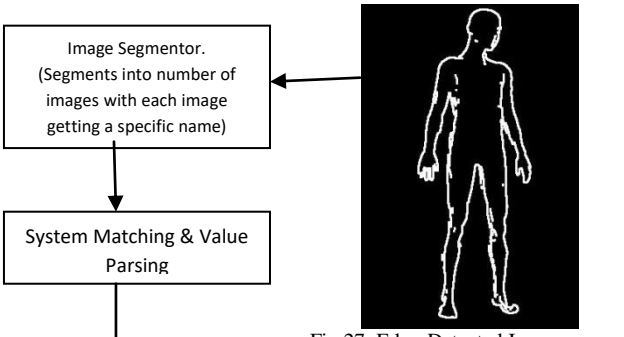


Fig 27: Edge-Detected Image

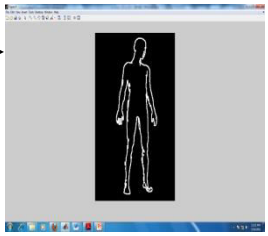
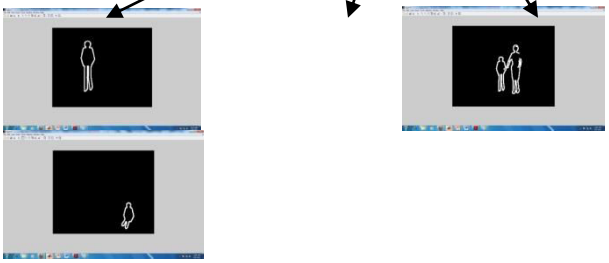


Fig 28: Human Image Detected

XI. EXPERIMENTAL RESULTS

Fig 29: Input Image

Fig 30: Edge-detected Image



a *b* *c*

Fig 31.a, 31.c: Human Image Identified
Fig 31.b: Human Image not identified

XII. SYSTEM ACCURACY

The images used for the testing purpose have been obtained on a random basis. So the accuracy of the system can vary when used on a different set of images.
Accuracy of recognition for first set of images:
Number of Input Images=675
Number of Images Recognized Correctly=581
Percentage Of accuracy=86.07%

XIII. CONCLUSION

The objective of our paper is to develop an acceptable and efficient Image Recognition algorithm to solve the challenge in Image Recognition technology under varying conditions. The object of our paper is to develop a system of identifying the object/s appearing in the image provided by the user. In our approach, we have first used the techniques of smoothing and removing noise from the images acquired after converting the user provided image to first gray-scale and then to binary image. Then the smoothed image has been passed through the process over edge detection using the Sobel edge detection operator. The 8 connected components of the image are thus obtained. The percentage of black pixels for each segment is calculated and these values summed up to match with the total percentage of black pixels for objects present in the database obtained during the testing phase.

XIV. FUTURE WORK

Since we are working on the field of image searching and recognition a hundred percent accurate output is not possible. So in our future work we plan to improve on this accuracy. In this improvement work we plan to implement some more advanced features such as the Watershed algorithm, the SUSAN operator technique etc. Furthermore the training has been done mainly on Human Being, so in our future work we plan to train our system more accurately on other living organisms and even plan to incorporate the training of inanimate objects in our system.

REFERENCES

[l] W. *Y.* Ma and B.**S.**Manjunath, "Edge Flow: **A** Technique for Boundary Detection and Image Segmentation" IEEE Trans.Image Processing, Vol. 9, **pp. 1375-1388, August** 2000.

[2] R. C. Gonzales, R. E. Woods, and S. L. Eddins, "Digital Image Processing using MATLAB", TMH, 2010.

[3] R. C. Gonzales, R. E. Woods, "Digital Image Processing ", PHI, 2006.

[4] Video Lectures on Digital Image Processing from NPTEL (National Programme on Technology Enhanced Learning) by Prof.P.K.Biswas,IITKgp.

[5] N. Otsu, "A Threshold Method from Gray-Level Histogram s", IEEE Trans. on Systems, Man and Cybernetics, vol. SMC-9, no.l, 1979, pp. 62-66. [6] http://ordination.okstate.edulPCA.html, Principal Component Analysis.

[7] http://icg.cityu.edu.hklprivateIPowerPointl PCA. ppt, Principal Component Analysis and Applications in Image Analysis.

❑❑❑

Admonishing Conservative Blinding For Wireless Sensor Networks

Swarna Surekha & C.Nagesh
INTELL ENGINEERING COLLEGE,JNTU ANANTAPUR-A.P.INDIA
E-mail : swarnas.623@gmail.com, nagesh.pandu@gmail.com

Abstract - Giving privacy utilizing and location monitoring services. Server poses threats to monitor individuals while monitoring personal locations. So, we propose Admonishing Conservative Blinding For Wireless Sensor Networks which gives alerting and hiding the information when unauthorized entrusted person access server in our system, we use two existing in network location anonymization algorithms, namely, *resource-* and *quality-aware* algorithms, that aim to enable the system to provide high quality location monitoring services for system users, while preserving personal location privacy. Both algorithms depends on the well established k-anonymity privacy concept, that is, a person is indistinguishable among k persons, to enable trusted sensor nodes to provide the aggregate location information of monitored persons for our system. Each aggregate location is in a form of a monitored area A along with the number of monitored persons residing in A, where A contains at least k persons. The resource-aware algorithm aims to minimize communication and computational cost, while the quality-aware algorithm aims to maximize the accuracy of the aggregate locations by minimizing their monitored areas. To utilize the aggregate location information to provide location monitoring services, we use a spatial histogram approach that estimates the distribution of the monitored persons based on the gathered aggregate location information. Then the estimated distribution is used to provide location monitoring services through answering range queries. We evaluate our system through simulated experiments. The results show that our system provides high quality location monitoring services for system users and guarantees the location privacy of the monitored persons.

Keywords - *Location privacy, location monitoring system, aggregate query processing, spatial histogram.*

I. INTRODUCTION

Now-a-day's technology improved and wireless sensors developed in many new applications for military, civilian and so on purposes. Many applications mainly concentrate on personal location i.e., to find particular location. There are so many sensors we use identity sensors to find out exact location and find particular object or particular person. While taking counting sensors such as photoelectric and thermal sensors used to report number of persons located in sensing area to server. Unknown person who is having privacy threat going to monitor personal information which may harm to the person who is under sensing area or it may be confidential information. It is better to use counting sensors rather than identity sensors because identity sensors give exact location information of monitoring persons to server whereas counting sensors gives only number of objects or persons exactly in its location. Counting sensors provides aggregate location information which also poses threats. By using identity sensors also poses privacy breaches. If there are few persons in particular small clocked sensing area it is very easy to detect particular person by using counting sensor. So we propose for small clocked area combining sensor information with more than one sensor nearby information and answering range queries is better solution rather than giving information regarding clocked area. If more small clocked areas are present then generating sensor information by collecting all sensor information is done. Each sensor stores information related to its sensing area. Whenever the sensor detected itself as small clocked sensing area then sensor will intimate neighbor sensors by updating its status and one of the neighbor sensor will collect the information from the present sensor and gives information to the sensor. When server came to know that the accessing person is unauthorized person then person's identity will be removed which means it will display that the person exist but not in exact location. For example, if we consider a building then when Alice is a person moving from Room1 to Room3 and then to Corridor. This information should not be revealed to entrusted person. If the intruder gets these information this may cause or lead to so many problems to the Alice. For this problem we propose Admonishing Conservative Blinding for Wireless Sensor Networks. If there are K-Persons in a clocked area then it is difficult to detect one individual person among K-Persons. But if we consider in Alice case it is very easy to know her movements. So, if the any unique person is present when server detects that the entered person is untrusted person and if untrusted person access any small clocked area then duplication of information should be present by hiding the actual information which means instead of giving

information about Alice it will give details of nearby neighbor's information. Thus, we propose for small clocked sensing area instead of taking large clocked area.

II. SYSTEM ARCHITECTURE

The architecture of our system, where there are three major entities, *sensor nodes*, *server*, and *system users*. We will define the problem addressed by our system, and then describe the detail of each entity and the privacy model of our system.

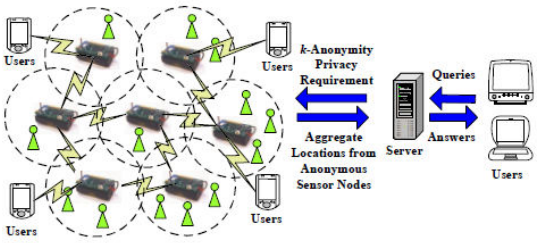


Fig 1: System Architecture

The objective is to guarantee that each sensor node knows an adequate number of objects to compute a cloaked area. To reduce communication cost, this step relies on a heuristic that a sensor node only forwards its received messages to its neighbors when some of them have not yet found an adequate number of objects. The basic idea of this step is that each sensor node blurs its sensing area into a cloaked area that includes at least k objects, in order to satisfy the k-anonymity privacy requirement. To minimize computational cost, this step uses a greedy approach to find a cloaked area based on the information stored in *Peer List*. An MBR is a rectangle with the minimum area (which is parallel to the axes) that completely contains all desired regions, where the dotted rectangle is the MBR of the sensing area of sensor nodes A and B. The major reasons of our algorithms aligning with MBRs rather than other polygons are that the concept of MBRs have been widely adopted by existing query processing algorithms and most database management systems have the ability to manipulate MBRs efficiently.

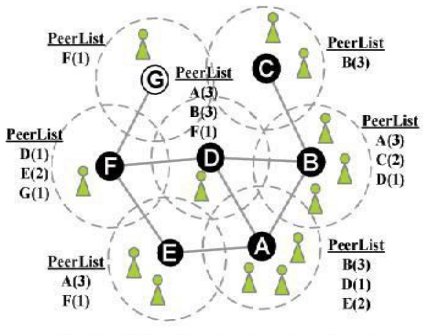


Fig2 Peerlist Information

It takes a set of peers residing in the search space, S, as an input and computes the minimal cloaked area for the sensor node m. Although the search space step already prunes the entire system space into S, exhaustively searching the minimal cloaked area among the peers residing in S, which needs to search all the possible combinations of these peers, could still be costly. Thus we propose two optimization techniques to reduce computational cost. The basic idea of the first optimization technique is that we do not need to examine all the combinations of the peers in S; instead, we only need to consider the combinations of at most four peers. The rationale behind this optimization is that an MBR is defined by almost four sensor nodes because at most two sensor nodes define the width of the MBR (parallel to the x-axis) while at most two other sensor nodes define the height of the MBR(parallel to the y-axis). Thus, this optimization mainly reduces computational cost by reducing the number of MBR computations among the peers in S.

2.1Spatial Histogram: we present a *spatial histogram* that is embedded inside the server to estimate the distribution of the monitored objects based on the aggregate locations reported from the sensor nodes. Our spatial histogram is represented by a two-dimensional array that models a grid structure G of NR rows and NC columns; hence, the system space is divided into NRxNC disjoint equalized grid cells. In each grid cell G(I, j), we maintain a float value that acts as an estimator H[I, j] (1<=i<=NC,1<= j <=NR) of the number of objects within its area. We assume that the system has the ability to know the total number of moving objects M in the system. The value of M will be used to initialize the spatial histogram. In practice, M can be computed online for both indoor and outdoor dynamic environments. For the indoor environment, the sensor nodes can be deployed at each entrance and exit to count the number of users entering or leaving the system. For the outdoor environment, the sensor nodes have been already used to count the number of people in a predefined area. We use the spatial histogram to provide approximate location monitoring services. The accuracy of the spatial histogram that indicates the utility of our privacy preserving location monitoring system will be evaluated.

III. EXISTING SYSTEM

In existing system, the there are multiple sensors, users and server. As sensor is a node having sensing area so that it can detect objects, persons etc and gives the information to the server. While User will going to communicate with servers in the form of queries in order to access the information from the sensor. User cannot access the sensor directly. So with the use of

server user can access the sensors. Server can communicate with each and every individual sensor and collects the information regarding its sensing area and the objects or persons that are present under it. If server access each and every individual sensor node and collects the information then the time taken for accessing will be more instead of collecting information. So server will communicate with nearby sensor and then access the information by communicating with the neighbor sensors. Sensors only will going to collect each and every information regarding total number of persons or objects etc., under its sensing area and gives the information to nearby sensors also known as Neighbor Sensors. Each sensor automatically updates when any new object or person moves from one sensing area to another sensing area. Thus, the information will automatically update to each and every sensor. When server wants any information regarding one particular person or object then it will approach a nearby sensor then sensors will communicate among themselves in the form of message by using the concept interprocess communication among sensors gives required information to the server and this process is done by Resource-Aware-Algorithm. The collection of information regarding user is given in the form of Spatial Histogram which gives the status and movements of particular person or object done from one sensing area to another sensing area by the server in the form of answering range queries. By giving information regarding the person or object results in security issues. So an alternative way has been proposed giving aggregate location information results in overcoming of above issues which is proposed by Quality-Aware-Algorithm. In this algorithm if any user requested regarding particular object then the server will go directly to particular sensor and access the sensing area by blurring the clocked area such that it will count the number of objects or persons and gives the aggregate information regarding that particular sensor not regarding individual known as Minimum Bounding Rectangle(MBR). Blurring the sensing area in order to collect individual's information is known as MBR. Thus, it is gives blinding (privacy) for an individual.

Even though giving aggregate location information from individual sensor arises some problems. When there are few objects or persons under sensor in its sensing area it is very easy to find an individual. If small clocked sensing area is present then it is very easy to find an individual. This is the major problem raised. If the MBR has very small sensing area then it is very easy to detect an individual by the intruder or untrusted person.

IV. PROPOSED SYSTEM

To evaluate the privacy protection of our system, we simulate an attacker attempting to infer the number of objects residing in a sensor node's sensing area. We will analyze the evaluation. The key idea of the attacker is that if the attacker cannot infer the exact object count of the sensor node from our system output, the attacker cannot infer the location information corresponding to an individual object. We consider the worst-case scenario where the attacker has the background knowledge about the system, i.e., the map layout of the system, the location of each sensor node, the sensing area of each sensor node, the total number of objects currently residing in the system, and the aggregate locations reported from the sensor nodes. By using a *brute-force* approach of finding the minimal cloaked area of a sensor node has to examine all the combinations of its peers. Let N be the number of sensor nodes in the system. Since each sensor node has N-1 peers, we have to consider and to find the minimal cloaked area.

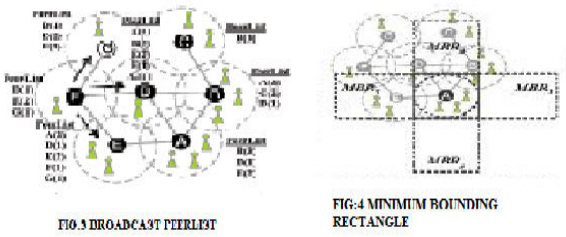


FIG 4:REBROADCAST OF PEERLIST AND MBR

In this paper, the search space step determines a search space, S, and prunes the peers outside S. Let M be the number of peers in S, where M<=N-1. Thus the computational cost is reduced. In the minimal cloaked area step, the first optimization technique indicates that an MBR can be defined by at most four peers. As we need to consider the combinations of almost four peers, the computational cost is reduced to O(M4).Furthermore, the second optimization technique uses the monotonicity property to prune the combinations, which cannot give the minimal cloaked area. When their small clocked area which means when there are few persons or objects which can be identified uniquely then the sensor node will display the information of its neighbor sensor node by invoking requesting and receiving response from its neighbor nodes by using false location technique. By using interprocess communication concept communication between two sensors can be done and access information. If the neighbor sensor nodes has < K Persons or objects then aggregation of multiple sensor nodes information can be given to the server at this

situation space transformation is used. At this situation aggregate of information is given in the form of spatial histogram.

V. RELATED WORK

Straightforward approaches for preserving users' location privacy include enforcing privacy policies to restrict the use of collected location information and anonymizing the stored data before any disclosure However, these approaches fail to prevent internal data thefts or inadvertent disclosure. Recently, location anonymization techniques have been widely used to anonymize personal location information before any server gathers the location information, in order to utilize personal location privacy in location-based services. These techniques are based on one of the three concepts.

5.1False locations: Instead of reporting the monitored object's exact location, the object reports n different locations, where only one of them is the object's actual location while the rest are false locations. By using this solution we can reduce our problem somehow. By collecting the information if the number of objects or number of persons is K-objects or persons then the information has been gathered from neighbor sensor nodes by invoking request through messages and receiving respond message gathering the information regarding neighbor sensor nodes and sending the information to the server reduces the problem complication.

5.2Spatial cloaking: The spatial cloaking technique blurs a user's location into a cloaked spatial area that satisfy the user's specified privacy requirements.MBR when blur's the information it will be redirected to another sensor where K-Anatomy persons or objects that are present so that intruder or untrusted person cannot access the sensor node so that individual will be in safe state.

5.3Space transformation: This technique transforms the location information of queries and data into another space, where the spatial relationship among the query and data are encoded. Server will go to respond in the form of answering range queries.

. Among these three privacy concepts, only the spatial cloaking technique can be applied to our problem:

(a) The false location techniques cannot provide high quality monitoring services but gives solution to our problem due to a large amount of false location information results in blinding of information. So we use technique for small clocked areas.

(b) The space transformation techniques cannot provide blinding-conservative monitoring services as it reveals the monitored object's exact location information to the query issues and

(c) The spatial cloaking techniques can provide aggregate location information to the server and balance a trade-off between privacy protection and the quality of services by tuning the specified privacy requirements, for example, k-anonymity and minimum area privacy requirements.

Thus we adopt the false locations, spatial cloaking and space transformation technique to preserve the monitored object's location privacy in our location monitoring system. In terms of system architecture, we can use these techniques that can be categorized into *centralized, distributed*, and *peer-to-peer* approaches. In general, the centralized approach suffers from the mentioned internal attacks, while the distributed approach assumes that mobile users communicate with each other through base stations is not applicable to the wireless sensor network. Although the peer-to-peer approach can be applied to the wireless sensor network, the previous work using this approach only focuses on hiding a single user location among K-individuals with no direct applicability to sensor-based location monitoring. Also, the previous peer-to-peer approaches do not consider the quality of cloaked areas and discuss how to provide location monitoring services based on the gathered aggregate location information. In proposed system it not only applicable for small area networks but also for large area networks when aggregate location information has to be blinded then it can be redirected and applied to aggregate information also. In the wireless sensor network, Military equipment detection is one of the applications used by our technique so that missile should not be detected then diverting the intruder's concentration to another area so that missile is not at all exist providing some wrong information. We can also provide, when many users decide not to reveal their locations, the location monitoring system can provide useful services. This is the advantage to our system that aims to enable the sensor nodes to provide the blinding-conservative aggregate location information of the monitored objects. Our work distinguishes itself from this work, as (1) we do not assume any hierarchical structures, so it can be applied to all kinds of environments, and (2) we consider the problem of how to utilize the anonym zed location data to provide blinding-conservative location monitoring services. Other privacy related works include: anonymous communication that provides anonymous routing between the sender and the receiver , source location privacy that hides the sender's location and identity , aggregate data privacy that preserves the privacy of the sensor node's aggregate readings during transmission , data storage privacy that hides the data storage location , and query privacy that avoids

disclosing the personal interests are not considered to our problem.

VI. CONCLUSION

In this paper, we propose we used two in-network location anonymization algorithms, namely, *resource-* and *quality-aware* algorithms that preserve personal location privacy, while enabling the system to provide location monitoring services. The resource-aware algorithm aims to minimize communication and computational cost, while the quality-aware algorithm aims to minimize the size of cloaked areas in order to generate more accurate aggregate locations. To provide location monitoring services based on the aggregate location information, we propose a *spatial histogram* approach that analyzes the aggregate locations reported from the sensor nodes to estimate the distribution of the monitored objects. The estimated distribution is used to provide location monitoring services through answering range queries such that providing security when an small clocked sensing area is present if it is very confidential area then it is better to redirect the intruder or untrusted so that individual object or person cannot be recognized regarding location monitoring when there are K-Anatomized Persons or objects which gives high quality of security to the information so that individual cannot monitor the blinding area.

REFERENCES

[1] A. Harter, A. Hopper, P. Steggles, A. Ward, and P. Webster, .The anatomy of a context-aware application,. in Proc. of MobiCom, 1999.

[2] N. B. Priyantha, A. Chakraborty, and H. Balakrishnan, .The cricket location-support system,. in Proc. of MobiCom, 2000.

[3] B. Son, S. Shin, J. Kim, and Y. Her, .Implementation of the realtime people counting system using wireless sensor networks, IJMUE, vol. 2, no. 2, pp. 63.80, 2007.

[4] Onesystems Technologies, .Counting people in buildings. ttp://www.onesystemstech.com.sg/index.php?option=comcontent&task=view%&id=10..

[5] Traf-Sys Inc., .People counting systems. http://www.trafsys.com/products/people-counters/thermal-sensor.aspx..

[6] M. Gruteser, G. Schelle, A. Jain, R. Han, and D. Grunwald,.Privacy-aware location sensor networks,. in Proc. of HotOS, 2003.

[7] G. Kaupins and R. Minch, .Legal and ethical implications of employee location monitoring,. in Proc. of HICSS, 2005.

[8] .Location Privacy Protection Act of 2001,http://www.techlawjournal.com/cong107/privacy/location/s1164is.asp..

[9] Title 47 United States Code Section 222 (h) (2),http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=browse usc&do%cid=Cite:+47USC222..[10] D. Culler and M. S. Deborah Estrin, .Overview of sensor networks,. IEEE Computer, vol. 37, no. 8, pp. 41.49, 2004.

[10] A. Perrig, R. Szewczyk, V. Wen, D. E. Culler, and J. D. Tygar,.SPINS: Security protocols for sensor netowrks,. in Proc. of MobiCom,2001.

[11] J. Kong and X. Hong, .ANODR: Anonymous on demand routingwith untraceable routes for mobile adhoc networks,. in Proc. ofMobiHoc, 2003.

[12] P. Kamat, Y. Zhang,W. Trappe, and C. Ozturk, .Enhancing source location privacy in sensor network routing,. in Proc. of ICDCS,2005.

❑❑❑

Design And Development of Plug-in in Virtual Network For DataCenter Analysis

Yashaswini. S

M.S.Ramaiah Institute Of Technology,Bangalore
E-mail : yash.sridhar8@gmail.com

Abstract - The performance data is collected on each Hypervisors, VMs and application on memory,CPU and storage, network traffic, user access, user executions, peak utilizations every configurable interval. The data should be refreshed at regular intervals. The VM's of both Windows and Linux should be included .The performance data should be gathered in a well-known format. It should be able to act upon the performance data collected and should be able to see the changes graphically in different parameters overtime.

Keywords - *virtualization, Datacenter, Hypervisors, Virtual Machine.*

I. INTRODUCTION

Virtualization Improves the efficiency and availability of IT resources and applications. It eliminates the old "one server, one application" model and run multiple virtual machines on each physical machine.

The VMware vSphere transforms or "virtualizes" the hardware resources of an x86-based computer—including the CPU, RAM, hard disk and network controller—to create a fully functional virtual machine that can run its own operating system and applications just like a "real" computer.

Each virtual machine contains a complete system, eliminating potential conflicts. VMware virtualization works by inserting a thin layer of software directly on the computer hardware or on a host operating system. This contains a virtual machine monitor or "hypervisor" that allocates hardware resources dynamically and transparently. Multiple operating systems run concurrently on a single physical computer and share hardware resources with each other. By encapsulating an entire machine, including CPU, memory, operating system, and network devices, a virtual machine is completely compatible with all standard x86 operating systems, applications, and device drivers.

Virtualizing your IT infrastructure lets you reduce IT costs while increasing the efficiency, utilization, and flexibility of your existing assets.

A data center is a centralized repository, either physical or virtual, for the storage, management, and dissemination of data and information organized around a particular body of knowledge or pertaining to a particular business.

A hypervisor, also called a virtual machine manager, is a program that allows multiple operating systems to share a single hardware host. Each operating system appears to have the host's processor, memory, and other resources all to itself. However, the hypervisor is actually controlling the host processor and resources, allocating what is needed to each operating system in turn and making sure that the guest operating systems (called virtual machines) cannot disrupt each other.

A virtual machine (VM) is a software implementation of a computing environment in which an operating system (OS) or program can be installed and run.

The virtual machine typically emulates a physical computing environment, but requests for CPU, memory, hard disk, network and other hardware resources are managed by a virtualization layer which translates these requests to the underlying physical hardware.

VMs are created within a virtualization layer, such as a hypervisor or a virtualization platform that runs on top of a client or server operating system. This operating system is known as the host OS. The virtualization layer can be used to create many individual, isolated VM environments.

Typically, guest operating systems and programs are not aware that they are running on a virtual platform and, as long as the VM's virtual platform is supported,

this software can be installed in the same way it would be deployed to physical server hardware. For example, the guest OS might appear to have a physical hard disk attached to it, but actual I/O requests are translated by the virtualization layer so they actually occur against a file that is accessible by the host OS.

Virtual machines can provide numerous advantages over the installation of OS's and software directly on physical hardware. Isolation ensures that applications and services that run within a VM cannot interfere with the host OS or other VMs. VMs can also be easily moved, copied, and reassigned between host servers to optimize hardware resource utilization. Administrators can also take advantage of virtual environments to simply backups, disaster recovery, new deployments and basic system administration tasks. The use of virtual machines also comes with several important management considerations, many of which can be addressed through general systems administration best practices and tools that are designed to managed VMs.

The virtualization enables you to get more from existing resources. It reduces the datacenter cost by reducing physical infrastructure, increase availability of hardware and applications for improved businesscontinuity.Virtualization enables to Gain operational flexibility and Improve desktop manageability and security.

The Benefits of Virtualization are as follows:

- *Compatibility:*

The virtual machine hosts its own guest operating system and applications, and has all the components found in a physical computer (motherboard, VGA card, network card controller, etc). As a result, virtual machines are completely compatible with all standard x86 operating systems, applications and device drivers, so you can use a virtual machine to run all the same software that you would run on a physical x86 computer.

- *Isolation:*

The virtual machines can share the physical resources of a single computer, they remain completely isolated from each other as if they were separate physical machines. If, for example, there are four virtual machines on a single physical server and one of the virtual machines crashes, the other three virtual machines remain available.

- *Encapsulation:*

A virtual machine is essentially a software container that bundles or “encapsulates” a complete set of virtual hardware resources, as well as an operating system and all its applications, inside a software package. Encapsulation makes virtual machines incredibly portable and easy to manage.

- *Hardware Independence:*

Virtual machines are completely independent from their underlying physical hardware. For example, you can configure a virtual machine with virtual components (eg, CPU, network card, SCSI controller) that are completely different from the physical components that are present on the underlying hardware. Virtual machines on the same physical server can even run different kinds of operating systems (Windows, Linux, etc). Hardware independence also means that you can run a heterogeneous mixture of operating systems and applications on a single physical computer.

II . RELATED WORK

There are some tools which monitorsdatacenter analytics and measures performance data in virtual environment,they are as follows:

1. Vision Core:

It is a performance monitoring and management tool that provide solutions to improve user satisfaction and ensure that applications meets the needs of the organization. It Monitor service levels , resolve performance bottlenecks, Deliver role-based views for domain admins, operations management, and the business and Consolidate tools for your physical, virtual, and cloud environments.

2. Akkori

Akkori optimizes servers and storage by virtualization. It helps to identify the interdependencies between virtualized servers and storage system. It eliminates the virtualization relationships problems between physical server, network, and storage components and makes the process of diagnose and address operational found in traditional softwaretools.

3. Dynamic Ops:

DynamicOps’ Operations Virtualization™ platform enables enterprise IT to rapidly create on-demand private and public cloud services from existing systems in days, imprinting current business processes on the cloud and achieving unparalleled time-to-cloud value, while providing a development path for a controlled evolution to building next-generation cloud services.

4. Scalent:

Scalent, a private company that provides software that makes data center infrastructure dynamic, easily scalable and highly efficient. Its acquired by Dell. It simplifies data center management by enabling a single administrator to dynamically allocate compute, storage and network resources for physical and virtual application workloads.

It enables administrators to make changes to infrastructure without the need for physical server, along with industry-standard servers, Ethernet switches and Fibre Channel switches, allowing customers to transit quickly to a highly-dynamic data center using existing infrastructure investments.

5. Cirba:

CIRBA is based on experience in integrating and deploying technology in heterogeneous data centers by virtualization and consolidation . CiRBA provides best practices and guidance on how to exploit the benefits of analytics in the data center. CiRBA covers data collection, administration, template creation and analytics in the planning, configuration, test deployment, and production deployment phases and provides a full set of services from assessment to detailed design and actual implementation.

6. CA

Over-provisioning IT resources is a common problem that often leads to excessive spending on application/infrastructure capacity needs. CA Technologies helps existing physical and virtual infrastructure to meet computing needs cost-effectively by providing automated capacity management capabilities for high-volume physical, virtual, and cloud environments.

It distributes workload and ensure service levels of existing systems by using data center planning tools, it analyzes capacity utilization, ensures service levels, and re-allocate or consolidate resources as needed by automating and managing data center capacity, it reduces costs and maintains the availability and quality of IT services.

7. Up.time Software tool:

Up.time is complete, yet easy to use IT systems management software for deeply monitoring, reporting and alerting on the performance, availability and capacity of your virtual, physical and cloud datacenters, applications and IT services. up.time can monitor services, monitor applications, monitor servers, and monitor platforms from a unified dashboard, even across multiple datacenters.

Even though the existing system for Data Center Workload Monitoring, Analysis, Emulation identifies location, environment,service performance, and includes collecting,analyzing facilities on performance data with focus on boundary, data analysis and workload methods. The above tools provides consolidated service capabilities of performance data by analysing datacenter analytics most of them are commercial and not cost effective to implement on larger cloud infrastructure.

Hence the system proposed in the paper collects all performance data and consolidates them into single monitoring application at different levels of datacenter analytics by extracting data from datacenters, hypervisiors, VM through a lightweight process. The collected data is in well known format and allows user to act upon and collects the accurate data by refreshing and represents only requested data in graphs which provides good understanding to user .

III . VIRTUALIZATION INFRASTRUCTURE AND ARCHITECTURE

The Virtual machines are a fundamental building block of the virtual infrastructure. While a virtual machine represents the hardware resources of an entire computer, a virtual infrastructure represents the interconnected hardware resources of an entire IT infrastructure—including computers, network devices and shared storage resources. Organizations of all sizes use VMware solutions to build virtual server and desktop infrastructures that improve the availability, security and manageability of mission-critical applications

The virtual infrastructure lowers capital and operational costs and improve operational efficiency and flexibility. It does server consolidation and deploy a standard virtualization platform to automate your entire IT infrastructure. VMware customers have harnessed the power of virtualization to better manage IT capacity, provide better service levels, and streamline IT processes. We coined a term for virtualizing the IT infrastructure.

A virtual infrastructure helps to share physical resources of multiple machines across your entire infrastructure. Resources are shared across multiple virtual machines and application depending upon business needs they can be dynamically mapped with the physical resources of your infrastructure to applications.This resource optimization drives greater flexibility in the organization and results in lower capital and operational costs.

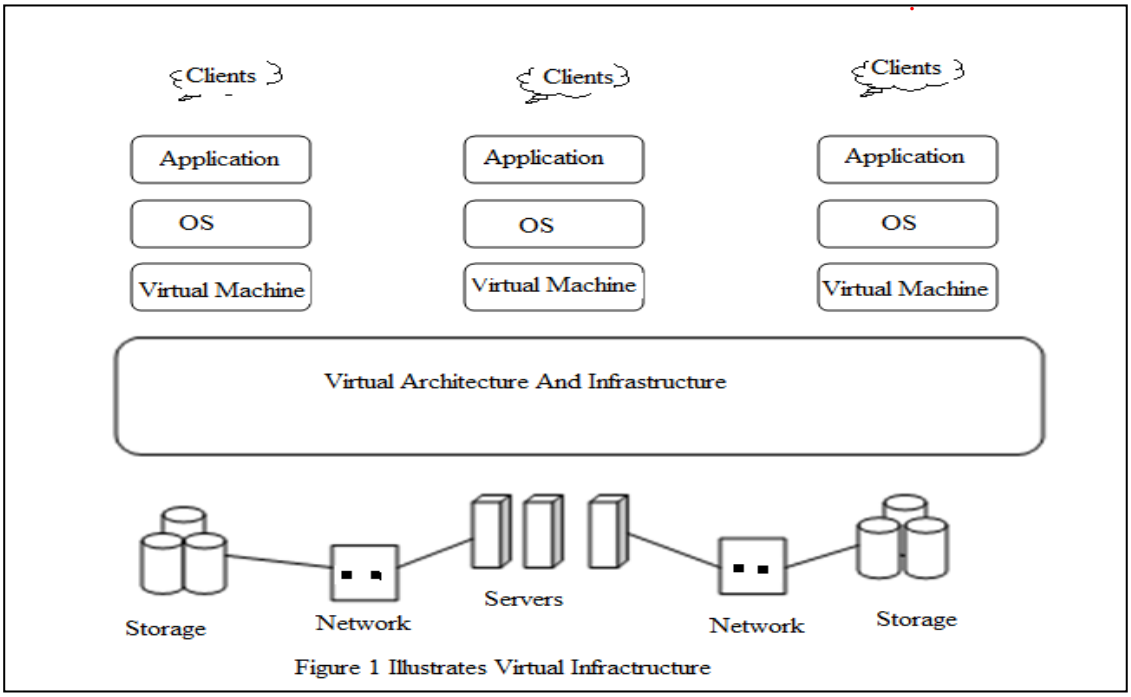


Figure 1 Illustrates Virtual Infractructure

As shown in Figure 1 the virtual infrastructure builds virtualization platform from VMware. VMware Infrastructure provides hardware resources to create a shared dynamic platform, while delivering built–in availability, security and scalability to applications. It supports a wide range of operating system and application environments, as well as networking and storage infrastructure. It provides solution for key integration for hardware and infrastructure management vendors and partners to deliver differentiated value that can be applied uniformly across all application and operating system environments.

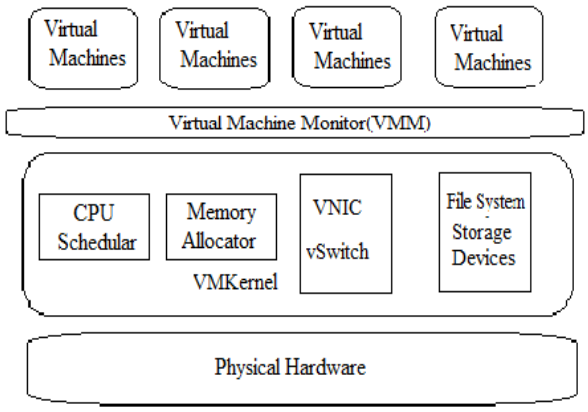


Figure 2 Illustrates VMware Architecture

As shown in the Figure 2 the VMware virtualization architecture includes physical hardware which act as an underlying support to VMkernel. The VMkernel includes a CPU Schedular to schedule the tasks and memory allocator to provision memory allocation for VMs .The VNIC and vSwitch specifies the port and all network related information followed by the file system used for mounted ,the type of storage used and devices supported by the kernel.

The thin candy layer called Virtual Machine Monitor(VMM) or hypervisor is inserted to provision virtualization and it inturn allocates the required virtual machine for application depending upon the availability of memory.

A virtual machine is a tightly isolated software container that can run its own operating systems and applications as if it were a physical computer. A virtual machine behaves exactly like a physical computer and contains it own virtual (ie, software-based) CPU, RAM hard disk and the details like router, switches, bridges, hubs, terminals, network interface card (NIC).

An operating system can't tell the difference between a virtual machine and a physical machine, nor can applications or other computers on a network. A virtual machine is composed entirely of software and contains no hardware components. As a result, virtual machines offer a number of distinct advantages over physical hardware cost.

IV APPROACH

The Performance data includes CPU ,storage, network traffic, user access, user executions, drivers ,applications and services.The peak utilizations is configured at regular interval (like 30mins) by using a refresh rate which schedules the java classes.

The gathered performance data is graphically displayed by using Flot.The output consist of detail information of performance data, collected from VM, hypervisor, datacentersand applications in terms of charts and graphs.

The safe VM, hypervisor, datacenters are indicated by GREEN color and unsafe are indicated by RED. The unsafe systems has to be handaled at earliest to handle workload and improve performance of datacenters.

A. VIJava API

The VI Java API developed by Steve Jen and VIX Disk lib which provides services of Vmachines are used to collect the performance data on each datacenter, Hypervisor, VMs and applications.

The API has created a full set of managed objects on the client side so that you can take fulladvantage of object-oriented programming and compile time–type checking. As a result, youhave more readable and shorter code. Based on the observation of converting samples usingWeb Services in the VI SDK, the average reduction of code is about 70 percent. This boostsproductivity for your development, meaning less investment for the product and shorter time tomarket.

The API has been open sourced at sourceforge.net (http://vijava.sf.net) under BSD license,which is lenient. Anyone can use it as it is or modify it as needed as long as they meet thelicense conditions.

B. Algorithms

The connection algorithm specifies the connection set up applicable through service instances, the service instance requires vclientip address, username and password once they are valid connection is set up.

The entity algorthim specifies which entity is to be monitored .The options for entity are datacenter, host system and virtual machine. Depending on selected entity its characteristics are displayed.

The datacenter algorithm specifies the root traversals required and collects data at different levels of datacenter analytics like datacenter, host system and virtual machines.

Algorithm Connection(Si)

```
Input : Service Instance(Si)
Vclient IP : 172.182.16.53\SDK
Username
Password
 Si= getServiceInstance(Vclient IP,Username,Password)
if (Si == null)
connection Failed
else
connected to Vclient
```

Algorithm Entity(Managed object)

```
Input :: Managed Object,Root Folder

If(Root Folder == Datacenter folder)
 managed object = Datacenter;
else is (Root folder == Hostsystem folder)
managed object =  hostsystem;
else
managed object =Virtual machine;

if(entity == managed object )
connection() == true;
else
connection() == false;
```

Algorithm for Datacenter Analysis

```
Input:: Si,Rootfolder,Managed entity

if (Si == null)
connection failed;
else
connection Successfull;

 if (rootfolder == datacenterfolder)
 managed enttity = datacenter;
 display datacenter();

display datacenter()
{
display(no of datacenter,datacenter name)
if(datacenter name == valid)
managed entity == datacenter;
display(datacentercharacteristics)
display hostsystem()
else
return invalid datacenter name;
}
```

```
if(Rootfolder == hostsystemfolder)
managed entity == hostsytem ;
display hostsystem()


display hostsystem()
{
display(no of hostsystem, hostsytem name)
if(hostsystem name == valid)
managed entity == Hostsystem;
display(hostsystem characteristics)
display virtualmachine()
else
return invalid hostsystem name;
}

if(Rootfolder == virtualmachinefolder)
managed entity == virtualmachine ;
display virtualmachine()

display virtualmachine()
{
display(no of virtual machine,virtualmachine name)
if(virtualmachine name == valid)
managed entity == virtualmachine;
display(virtualmachinecharacteristics)
else
return invalid virtualmachine name;
}
```

The performance algorithm collects the performance characteristics like CPU, memory disk RAM for virtual machine and hypervisors depending on sub-entity like percounter, perfmetric id, historical data. The collected is refreshed through an api the default refresh time is 20mins.It collects the performance data along with units and using flot it represents the collected data graphically in piecharts which give deeper insight and understanding.

Algorithm for Datacenter Analysis

```
Input :: Entity,Performance Manager
Output :: Performance Characteristics
 Entity == Hostsystem || Virtual Machine
perfmgr == Si.getperformancemanager();
if(perfmgr == null)
performance characteristics cannot be retrived
select subentity
subentity == perfmetric id || perfcounter || historicaldata
retrive graph values;
Set refreshrate;
collect all performance parameters in collections with units
use flot and get values;
using collected performance draw pie charts for specific entity
```

A. Eclipse

Eclipse is a professional, integrated development environment (IDE) for software developers [7]. It is an open source project, and freely available versions are easy to install in university laboratories and on students' home computers. Eclipse is used by students in their programming assignments to provide a uniform platform to plug-in different software quality tools.

The Eclipse Java perspective provides context dependent help for Java and its libraries, offering compiler warnings and errors, and support for managing project files.

The Eclipse formatter corrects code layout automatically to satisfy standard Java conventions.The vijavaapi is configured in eclipse to provide support and even flot consisting of Jquery.

B. Flot

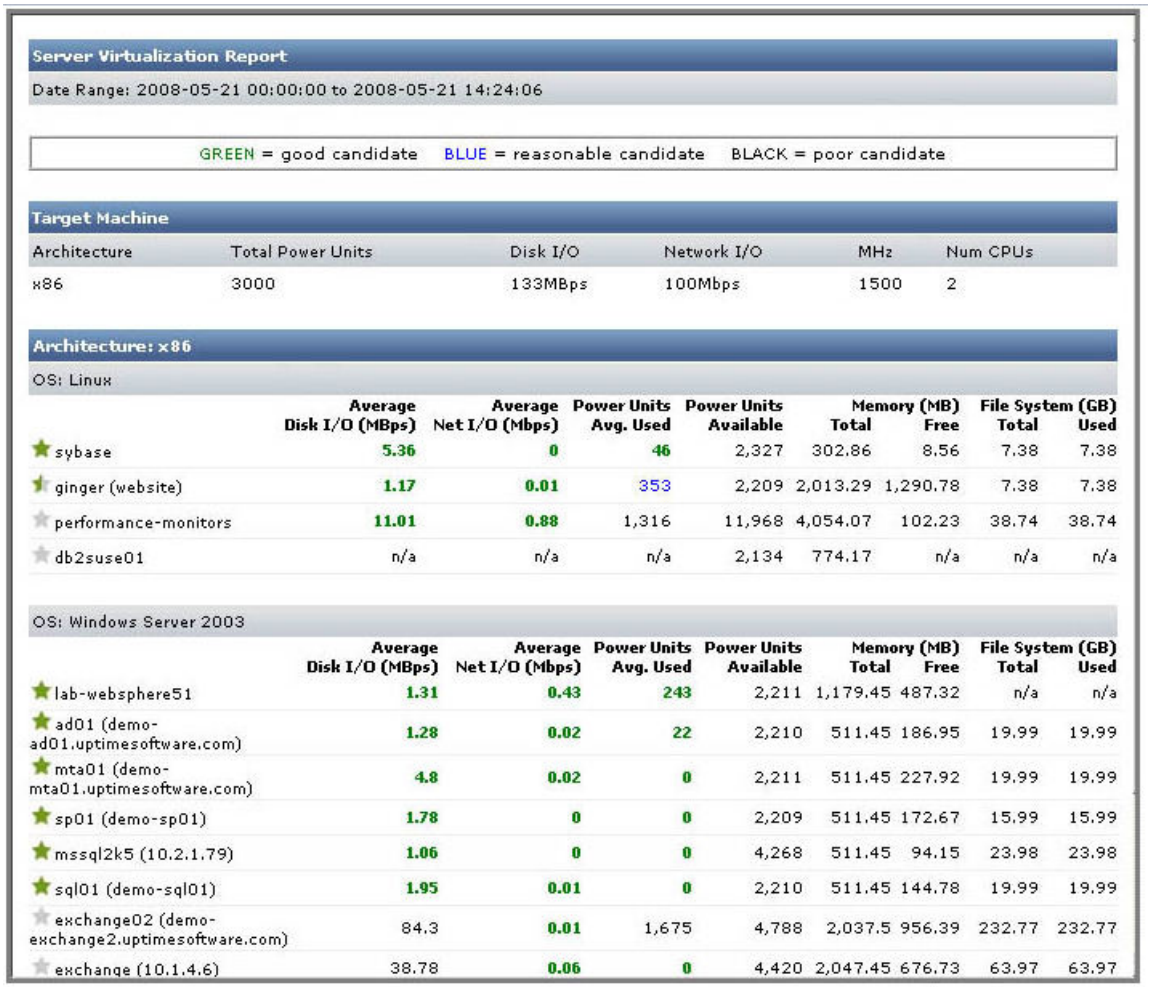
Flot is a pure Javascript plotting library for jQuery. It produces graphical **plots** of arbitrary datasets on-the-fly client-side. The focus is on **simple** usage (all settings are optional), **attractive** looks and **interactive** features like zooming and mouse tracking.

The plugin works with Internet Explorer 6+, Firefox 2.x+, Safari 3.0+, Opera 9.5+ and Konqueror 4.x+ with the HTML canvas tag (the excanvasJavascript emulation helper is used for IE < 9).

V . RESULTS

VI. GRAPHS

The tools specified will provide the information for datacenter as a whole and provides all the information of virtual machine like average disk I/O, net I/O memory ,filesystem utilization in a single page which will be tedious to monitor and retrieve specific value in no of virtual machine provisioned is invariably high.



Server Virtualization Report

Date Range: 2008-05-21 00:00:00 to 2008-05-21 14:24:06

GREEN = good candidate BLUE = reasonable candidate BLACK = poor candidate

Target Machine

Architecture	Total Power Units	Disk I/O	Network I/O	MHz	Num CPUs
x86	3000	133MBps	100Mbps	1500	2

Architecture: x86

OS: Linux

	Average Disk I/O (MBps)	Average Net I/O (Mbps)	Power Units Avg. Used	Power Units Available	Memory (MB) Total	Memory (MB) Free	File System (GB) Total	File System (GB) Used
sybase	5.36	0	46	2,327	302.86	8.56	7.38	7.38
ginger (website)	1.17	0.01	353	2,209	2,013.29	1,290.78	7.38	7.38
performance-monitors	11.01	0.88	1,316	11,968	4,054.07	102.23	38.74	38.74
db2suse01	n/a	n/a	n/a	2,134	774.17	n/a	n/a	n/a

OS: Windows Server 2003

	Average Disk I/O (MBps)	Average Net I/O (Mbps)	Power Units Avg. Used	Power Units Available	Memory (MB) Total	Memory (MB) Free	File System (GB) Total	File System (GB) Used
lab-websphere51	1.31	0.43	243	2,211	1,179.45	487.32	n/a	n/a
ad01 (demo-ad01.uptimesoftware.com)	1.28	0.02	22	2,210	511.45	186.95	19.99	19.99
mta01 (demo-mta01.uptimesoftware.com)	4.8	0.02	0	2,211	511.45	227.92	19.99	19.99
sp01 (demo-sp01)	1.78	0	0	2,209	511.45	172.67	15.99	15.99
mssql2k5 (10.2.1.79)	1.06	0	0	4,268	511.45	94.15	23.98	23.98
sql01 (demo-sql01)	1.95	0.01	0	2,210	511.45	144.78	19.99	19.99
exchange02 (demo-exchange2.uptimesoftware.com)	84.3	0.01	1,675	4,788	2,037.5	956.39	232.77	232.77
exchange (10.1.4.6)	38.78	0.06	0	4,420	2,047.45	676.73	63.97	63.97

The performance data collected from VIjavaapi is particular to datacenter ,hypervisor,virtual machine and it represented in charts to provide good understanding of data pictorically its more attractive and interactive by using flot.

VII. CONCLUSION

The proposed system collects all performance data and consolidates them into single monitoring application by extracting data from datacenters, hypervisiors, VM through a lightweight process.

It uses Sqlite database which is lightweighted and integrates virtual environment and increaces performance.

It is affordable to implement on large cloud infrastructure and results are graphical which provides deeper understanding on virtualization performance parameters through datacenter analytics.

REFERENCES

[1] http://pubs.vmware.com/vsphere50/topic/com.vmware.ICbase/PDF/vsdk_progguide.pdf

[2] https://optimize.vmware.com/support/CP-DataCollectionGD.pdf

[3] http://www.vmware.com/support/developer/vcsdk/visdk400pubs/sdk40programmingguide.pdf

[4] http://www.vmware.com/files/pdf/vmi_cisco_network_environment.pdf

[5] http://www.vmware.com/files/pdf/VMware_NFS_BestPractices_WP_EN.pdf

[6] http://www.vmware.com/files/pdf/partners/hp/hp-vc-vmware-infrastructure3-wp.pdf

[7] http://www.vmware.com/files/pdf/virtual_networking_concepts.pdf

[8] http://code.google.com/p/flot/

Detection of Leukemia Using Image Processing (OpenCV)

Hema Malini. S, Ishwarya Bhaskaran & P. Neelamegam

Dept. of Electronics & Instrumentation Engineering, SASTRA University, Thanjavur, India
E-mail : {hema.malini44, aishwarya.bhaskaran78}@gmail.com, neelkeer@eie.sastra.edu

Abstract - Leukemia is a rapidly spreading disease that calls for a very efficient, rapid and cost-effective method of analysis. Though conventional methods like laboratory tests, physical examination and biopsy prevail, they are either very costly or more prone to human errors. To address to this problem, we need a quick and cost-effective technique that detects the disease. In this paper, two image processing techniques have been proposed that detect leukemia using blood cell count. To implement them, OpenCV2.0 library has been used. These proposed methods use certain pre-processing and post processing techniques which yield a cleaner and clearer image of the blood cells. The number of blood cells is counted and ratio of the white blood cells(WBC) count to the red blood cells(RBC) count is found out that detects the presence of leukemia. The results show an accuracy of 92.1% for the second method which is better when compared to the first method with an accuracy of 82.9% for detection of leukemia.

Keywords - Leukemia, image processing, OpenCV2.0, segmentation, counting, ratio calculation.

I. INTRODUCTION

Image processing is an emerging field that finds application in industries, medical field, security systems etc. Apart from these, Google maps, Image retrieval, Robotics and Machine vision also depend on image processing extensively. Medical imaging plays an important role in detecting diseases, finding out faulty tissues and bones etc. Computed Tomography, Magnetic Resonance Imaging, Electro cardiogram are all examples of medical imaging[1].

Leukemia is a disease that affects blood forming cells in the body. Its cancerous condition is characterized by an abundance of abnormal white blood cells in the body. In a healthy body, bone marrow makes white blood cells to help the body fight an infection. When a person has leukemia, the bone marrow starts to build a lot of abnormal white blood cells called leukemia cells. They grow faster than normal cells and they do not stop growing when they should[2]. In leukemia, the white blood cells become abnormal, divide and grow in an uncontrolled way. These cells start in the soft, inside part of the bones called the bone marrow. After they start building up, leukemia cells often shift quickly into the blood where they can reach other parts of the body such as the lymph nodes, spleen, liver, central nervous system (brain and spinal cord) and other organs[3]. There are two major types of leukemia namely, Acute and Chronic. Acute leukemia is characterized by a rapid increase in the number of immature blood cells which make the bone marrow unable to produce healthy blood cells. It is usually common in children and immediate treatment is required. Chronic leukemia is characterized by excessive build up of relatively mature but still abnormal white blood cells. It takes months or years to progress and the cells are produced at much higher rate than normal thereby increasing the count of abnormal white blood cells. It is usually common in older people but can occur in any age group. Leukemia is further classified into two types according to which type of blood cell is affected. They are: Myeloid and Lymphocytic. In the former one, the cancerous change takes place in a type of marrow cell that normally goes on to form red blood cell, some other types white cells and platelets. In the latter one, the cancerous change takes place in the type of marrow cell that goes on to form lymphocytes which are white blood cells that are infection fighting immune system cells. Most of this type leukemia involve a specific type of cell called the B-cell[1]. The four major types of leukemia are Acute Myelogenous Leukemia (AML), Acute Lymphoblastic Leukemia (ALL), Chronic Myelogenous Leukemia (CML) and Chronic Lymphocytic Leukemia (CLL). According to statistics, 196,000 cases of ALL, 200,000 cases of AML have been reported.[4]

The early and fast identification of the leukemia type, greatly aids in providing the appropriate treatment for the particular type. Its detection starts with a complete blood count (CBC). The patient should undergo bone marrow biopsy if there are abnormalities in this count. Therefore, to confirm the presence of leukemic cells, a study of morphological bone marrow and peripheral blood slide analysis is done. In order to classify the abnormal cells in their particular types and

subtype of leukemia, a hematologist will observe some cells under a light microscopy looking for the abnormalities presented in the nucleus or cytoplasm of the cells. This classification is very important in predicting the clinical behavior of the disease and the prognosis in order to determine which treatment should be given to the patient. The conventional method of Leukemia detection is by counting WBC and RBC cells in blood sample by humans. It starts with a complete blood count (CBC). Manual counting done under the microscope was performed in order to count the white blood cells in leukemia slides. This way is troublesome and time consuming if the counting process is interrupted; it has to be started all over again. Thus, the traditional method of manual counting under the microscope is susceptible to error and puts an intolerable amount of stress on the medical laboratory technicians. Although there are hardware solutions such as the Automated Hematology Counter to perform counting, certain developing countries are not capable to deploy such an expensive machine in every hospital laboratory in the country[5].Furthermore, hematologists still carry out the manual counting based on slide of blood and bone marrow samples to confirm the case. Therefore, this paper aims at providing an alternative solution where the number of cells is counted automatically and the presence of leukemia is confirmed.

II. IMPLEMENTATION

The main objective of this study is to design and develop an image processing system for leukemia detection using the blood cell count. Normally, the number of white blood cells in patients with positive cases of leukemia will increase. The increasing number of white blood cell will increase the ratio of white blood cells (WBC) to red blood cells (RBC). Thus, it is important to have a cost effective image processing system which will assist hematologists to determine the ratio of white blood cells to red blood cells for leukemia detection. The methodology used to develop the image processing system is described in the following sections.

A. Development of Image Processing System for Ratio Calculation:

OpenCV 2.0 library has been used in this study to develop a system for blood cell ratio calculation. The main objective of using Eclipse for this project is to provide a software solution which is cost effective as well as efficient for countries like India to be widely utilized in the healthcare industry. The development of this system involved several stages. These include image pre-processing techniques which were conducted before the calculation of the blood cells ratio could be implemented on the blood cells image. Examples of image pre-processing techniques include conversion to grayscale image, to binary image and image contrast enhancement. In this project, the method used to determine the ratio of blood cells is by counting the number of white blood cells (WBC) to red blood cells (RBC).

In this study, an image processing system for blood cells calculation has been developed using two methods. The first method employs image enhancement technique on binary image while in the second method, the enhanced image is converted to binary. In the first technique, the original blood cell image will be converted into grayscale image. Then, based on the grayscale image, the threshold values for the WBC and RBC will be determined manually. These threshold values will be used to segment area of WBC and RBC. The image obtained from the segmentation process will be converted into binary image. If the result of these preprocessing techniques is satisfactory, the binary image will be implemented with image enhancement techniques to produce cleaner and clearer image to ease blood cells ratio calculation.

The first method is implemented in the following steps:

Step 1: Input the original blood cell image.

Step 2 : Convert the colour image into grayscale image.

Step 3: Develop a histogram to obtain the threshold value.

Step 4: Segment the image to separate the WBC's using the threshold value.

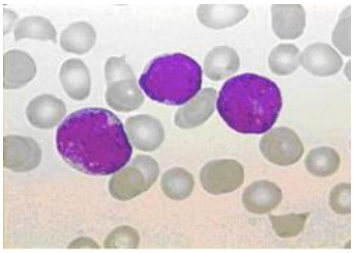
Step 5: If the binary image obtained in the previous step contains only WBC's, then enhance the image. If not, repeat step3.

Step 6: Calculate the ratio by counting the respective number of cells, namely the WBC's and the RBC's.

The implementation of the second technique, which is represented as a flowchart, is as follows. The image is converted to grayscale and then pre-processing techniques are applied. The image is enhanced using the smoothing operation and the histogram equalization method. In the next step, the histogram of the image is taken. Values from the histogram are used to threshold the image and therefore segment the WBC's separately. After segmentation, the edges are detected and contours are found which helps us to count the cells.

B. Image Acquisition

A total of 25 data images were collected from the database. Among the images analysed, 10 were of Acute Lymphoblastic Leukemia (ALL) type, 10 belonged to Acute Myelogenous Leukemia (AML) and 5 images were of normal blood cells.



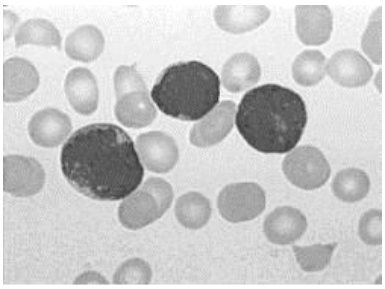
(a) Original image

C. Image Pre-processing

Converting the image to grayscale, binary and contrast enhancement are among the pre-processing techniques involved in the development of this image processing system. For contrast enhancement, histogram equalization method has been used that stretches the histogram over a wide scale for increased sharpness.

D. Grayscale Image

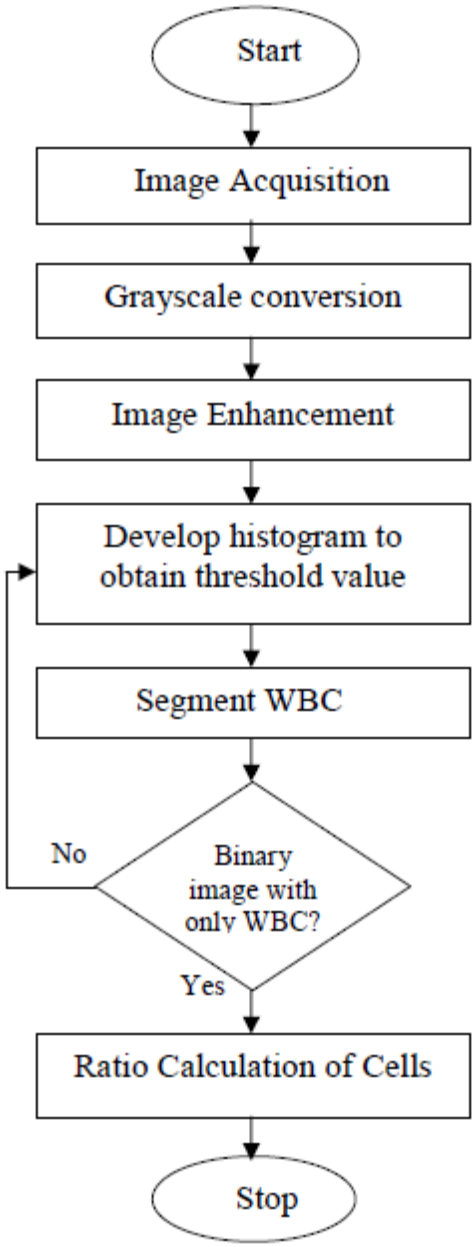
Original blood cells' images are in colour. To ease the process of ratio determination, the original images will be converted into grayscale. Grayscale represents the intensity of the image. In OpenCV 2.0, the image is converted into grayscale with the help of the function cvCvtColor( )[6] or while loading the image using cvLoadImage function, CV_LOAD_IMAGE_GRAYSCALE is specified that will automatically convert the image into a gray one.



(b) Grayscale image

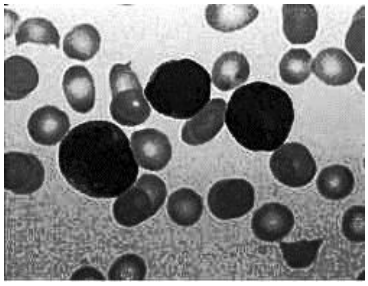
E. Image Enhancement

In this method, the image enhancement technique is applied after the image is converted into grayscale. Normally, the original image consists of small spots within the image. These small spots are considered as noise and need to be removed from the image to facilitate accuracy. Hence, image enhancement technique is used to remove the noise. The cvSmooth( ) function is used to remove the noise using the median filter. For increasing the clarity of the finer details, histogram equalization is done. Histogram equalization is a process of contrast adjustment by which pixel values are redistributed over a wide range. The function cvEqualizeHist( )[6] is used to stretch the histogram over a wide scale which results in increased contrast at peaks and lessened contrast at tails.

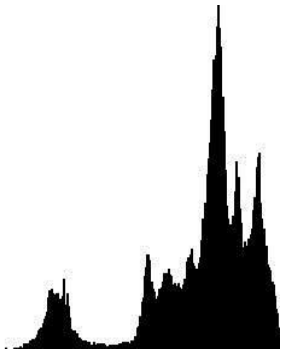


F. Image Segmentation:

Image segmentation is the process that subdivides an image into its constituent parts or objects. The level to which this subdivision is carried out depends on the problem being solved. Histogram is the graphical representation of the tonal distribution of the image. It plots the intensity on the x-axis to the number of pixels on the y-axis. After the image enhancement techniques are



(c) Image after histogram equalization



(d) Histogram of the image

performed on the grayscale image, the intensity distribution of that image can be presented through the gray level histogram. The frequencies of all the intensity levels can be seen and the image is analyzed based on the gray level histogram [7]. In this study, the gray level histogram is important to distinguish between RBC, WBC and background areas. A threshold value in an image normally lies in the valley between the two peaks. In Eclipse 2.0, the development of the histogram can be done by using the cvCreateHist( ) function and the same is displayed using cvDrawHist( )[6] function. Thresholding is a method of converting a grayscale image to a binary image so that the objects (WBC and RBC) are separated from the background [7]. Threshold value is applied on each image in order to obtain image with either RBC or WBC. Thresholding is implemented in OpenCV2.0 using cvThreshold()[6] function with the threshold type CV_THRESH _BINARY.

G (a) Edge Detection

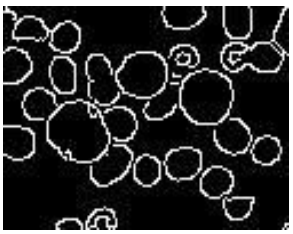
Edge detection is a fundamental process in image processing which identifies the points in the image at which brightness changes sharply. Some features like corners, lines, curves can be extracted from the edges of an image. There are different methods by which edges can be detected. Some of them are Sobel edge detector, Laplacian edge detector, Scharr edge detector and Canny edge detector. The Canny edge detector, known as the optimal edge detector is used in this project. It is implemented in OpenCV2.0 using the function cvCanny( )[5]. The cvCanny( ) function expects an input image,

(e) Image after thresholding

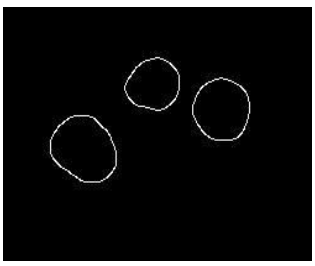
which must be grayscale, and produces a grayscale output image.

G(b) Cell Counting

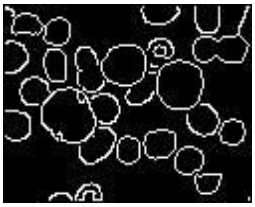
The next step is to assemble these edge pixels into contours. A contour is a closed curve that defines any object or shape. The total blood cell count is found out by finding the contours on the edge detected image. Based on the threshold value obtained from the histogram, the white blood cells were separated and their contours were detected to find their count. Once the WBC count and the total blood cell count is known, the red blood cell count is also found. Next, the ratio of WBC to RBC is found out. Contours are very helpful in finding and counting the number of cells, objects etc. These are detected in OpenCV2.0 using cvFindContours( ). The contours that are detected are drawn using the cvDrawContours( )[6] function. The contours are then counted to find the number of cells in the image.



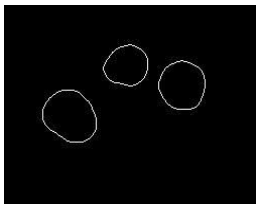
(f) Edge detected image



(g) Edge detected image for WBC



(h) Contour detection



(i) Contours of WBC

III. RESULTS AND DISCUSSION

The efficiency of the ratio method is discussed here. OpenCV2.0 library has been used to develop this method and it has several stages. The stages are: image acquisition, pre-processing, enhancement, image segmentation and counting. 25 blood cell images were obtained from the database. For each and every sample, the two techniques mentioned above were followed and the accuracy was tested. The results are as shown in the figure.

In the first method, since enhancement was done only after conversion to binary image, the images lacked clarity and the edges were not detected properly. Therefore, the count was not accurate when compared to the second method where the image was enhanced before converting to binary. The average accuracy of the first method was found to be 82.9% while it was 92.1% for the second one.

To obtain fully segmented image, the threshold mode is maintained at binary. In a binary image, object pixels have the value of 1 and background pixels have zero value. The binary image containing only the WBC will still have some noise which has to be removed to enhance the quality of the image. For this purpose, Median filter is applied on the image. This filter gave the best results for noise removal. The WBC is segmented by fixing the threshold value at 150 for ALL and 160 for AML. The binary images after thresholding some sample images are shown in the figure. Twenty five sample images were used to test the accuracy of the two methods. The testing procedure was started by counting the number of abnormal white blood cells(blast cells). Then the total blood count was found to obtain the RBC count. The manual count and the count obtained from the technique was compared in order to find the accuracy of both the methods. The details are given in TABLE1 and TABLE2.

$$\text{Accuracy} = \frac{(\text{Auto count}) \times 100}{(\text{Manual count})}$$

$$\text{Average Accuracy} = \frac{(\text{Total Accuracy})}{(\text{Total Images})}$$

For normal blood cell images, the ratio range of WBC's to RBC's is 0 to 0.1 which means that the RBC's outnumber the WBC's. For abnormal images i.e. those containing leukemic cells, the ratio is higher which may range from 0.2 to 2.5 for ALL and 0 to 10 for AML. The results obtained from this method also show that the sample images taken for study contain leukemic cells.

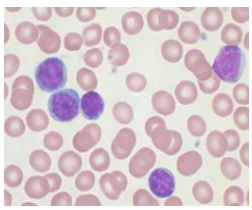
In the proposed method, the overlapped cells might give rise to incorrect count in the number of cells. So, different techniques like Watershed algorithm,

TABLE 1: FIRST METHOD

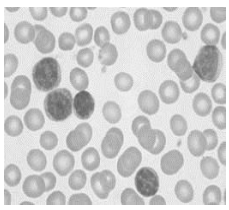
Image	**Expected count(manual)**		**Obtained count(auto)**		**Accuracy(%)**	
	WBC	**RBC**	**WBC**	**RBC**	**WBC**	**RBC**
Image1	3	26	3	21	100.0	80.8
Image2	5	46	4	39	80.0	84.8
Image3	7	16	5	11	71.4	68.8
Image4	1	5	1	4	100.0	80.0

TABLE2: SECOND METHOD

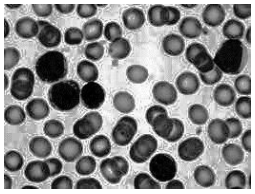
Image	**Expected count(manual)**		**Obtained count(auto)**		**Accuracy(%)**	
	WBC	**RBC**	**WBC**	**RBC**	**WBC**	**RBC**
Image1	3	26	3	23	100.0	88.5
Image2	5	46	5	41	100.0	89.1
Image3	7	16	6	12	85.7	75.0
Image4	1	5	1	5	100.0	100.0



(a)

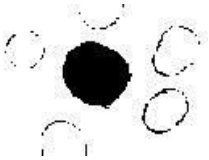


(b)



(c)

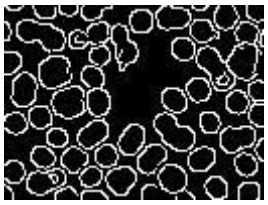
(d)



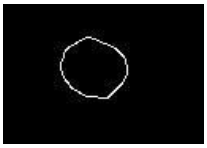
(e)

(f)

(e)

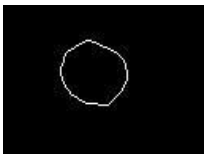


(f)

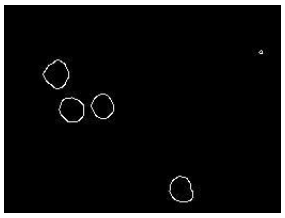


(g)

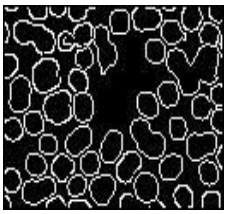
(h)



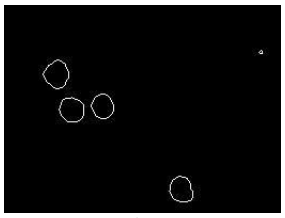
(i)



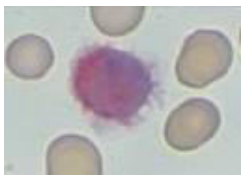
(g)



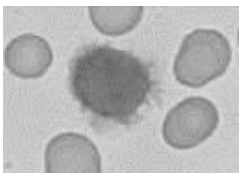
(h)



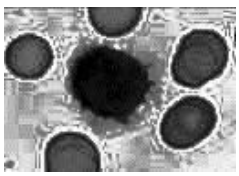
(i)



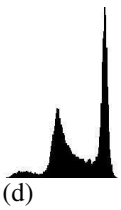
(a)



(b)



(c)



(d)

(a) Original image (b) Grayscale image

(c) Equalized image (d) Histogram of the image

(e) Thresholded image (f) Edge detected image

(g) Edge detection of WBC's (h) Contour of the cells (i) Contour of WBC's

edge separation based on centroid are being tried out to separate out the overlapping cells in order to obtain a perfect count. But the method is still reliable as the difference in count due to the overlapping cells is negligible. Thus, the error is low and acceptable and the system is efficient in achieving its objective.

IV. CONCLUSION

Out of the two proposed techniques, the first one has an average accuracy of 82.9% whereas the second one provides 92.1% accuracy. This proves that the second method is reliable enough and can assist hematologists in finding out the ratio and confirm the presence of leukemia at an early stage. The early detection will prove to be of great help to the patients to seek further treatment and cure the disease. This will reduce the errors due to the manual counting. Since this method makes use of open source software, it is rapid and cost-effective which can be employed even in laboratories with less facility. This will also help in reducing the leukemic related deaths due to in efficient detection.

REFERENCES:

[1] Leukemia Disease, http://en.wikipedia.org/wiki/ Leukemia, retrieved on 1 June 2011.

[2] Abdul Nasir et al, Application of Thresholding Technique in Determining Ratio of Blood Cells for Leukemia Detection, Malaysia, 2009.

[3] Nor Hazlyna Harun , Mohd Yusoff Mashor and Rosline Hassan, Automated Blasts Segmentation Techniques Based on Clustering Algorithm for Acute Leukemia Blood Samples, Malaysia, December2011.

[4] Harendra Modak, Suyamindra S Kulkarni, Kadakol.G.S, Hiremath.S.V, Patil.B.R, Umesh Hallikeri, Pramod B Gai, "Prevalence and Risk of Leukemia in the Multi-ethnic Population of North Karnataka" in Asian Pacific Journal of Cancer Prevention, Vol 12, 2011.

[5] Nurul Hazwani Abd Halim, Mohd Yusoff Mashor, and Rosline Hassan**,** "Automatic Blasts Counting for Acute Leukemia Based on Blood Samples" in International Journal of Research and Reviews in Computer Science (IJRRCS),Vol. 2, No. 4, August 2011.

[6] Gary Bradski, Adrian Kaehler, Learning OpenCV, O'Reilly publications, California, 2008.

[7] Jain. R, Kasturi. R and Schunck. B.G , Machine Vision. International Edition 1995, McGraw Hill, Inc, 1995.

❑❑❑

Statistical Analysis of WSN based Indoor Positioning Localization Schemes with Kalman Filtering

A.Mohamed Rias, R.Sambath Kumar, G.Sathishkumar & A. Sivagami
Electronics and Communication Engineering, Sri Manakula Vinayagar Engineering College, Puducherry.
E-mail : mohamedrias1103@gmail.com

Abstract - Wireless Sensor Network (WSN) is used for determining the Indoor Positioning of objects and persons since recent years. WSN has been implemented in indoor positioning applications such as real time tracking of humans/objects, patient monitoring in health care, navigation, warehouses for inventory monitoring, shopping malls, etc. But one of the problems while implementing WSN in Indoor positioning system is to ensure more coverage large number of sensors must be deployed which increases the installation cost. So in this paper, we have used MATLAB GUI named Sensor Network Localization Explorer to analyze the impact of node density on indoor positioning localization schemes. Later we have integrated the Kalman filter with the indoor positioning system to increase the reliability and reduce the localization error of the system with lesser number of nodes.

Keywords- *Kalman Filter, Indoor Positioning, Wireless Sensor Networks, Time of Arrival, Angle of Arrival, Node density*

I. INTRODUCTION

Global Positioning System (GPS) plays a dominant role in localization of objects or persons in outdoor environments. Even though lots of GPS devices are developed to provide sufficient precision for outdoor use, GPS is not efficient for localization in indoor environment because in indoor environment the GPS signal can't penetrate most of the building materials and also the signal gets weakened due to obstacles. Since people spend most of their time in indoor environments, indoor positioning and tracking is in great demand. Hence in order to enable localization in indoor environments, development of special indoor localization techniques were needed. Several indoor positioning localization technologies have been developed based on Infrared, ultrasonic, RFID, Wireless Sensor Network (WSN), Wi-Fi, WLAN, etc. [1] The proliferation of wireless localization technologies offers large number of applications in indoor environments including patient monitoring, health care, navigation, real-time tracking of persons or objects, rescue purposes in fire extinguishers, monitoring elderly persons, etc.

Wireless Sensor Networks (WSN) is used for indoor positioning operations since recent years. The deployment of tiny, cheap, low power sensor nodes which are capable of sensing, processing and wireless communication has found many applications in the field of agriculture for irrigation purposes, surveillance, military purposes, etc. [2] Each sensor node consists of a processing unit such CPU or processor, a memory unit to store program and data, a radio transceiver for communicating with base station and other nodes, sensing unit for monitoring the given physical environment i.e. pressure, temperature, moisture, etc. and a power source.

The sensor networks, the nodes can be deployed either in location aware infrastructure or into an unplanned infrastructure where there is no a priori knowledge about location[3].

The rest of this paper is organized as follows. Section II will give information regarding the steps involved in indoor positioning localization. Section III explains the signal measurement phase of indoor positioning system. Section IV and V discusses the problem statement and the simulation environment. Section VI shows the outputs obtained using the senelex tool without Kalman filter. Section VII explains application of Kalman filter in indoor positioning system. Section VIII and IX concludes the paper with a discussion on open issues.

II. INDOOR POSITIONING SYSTEM

Dempsey [4] has defined indoor positioning system is a system that is capable of determining the position of an object or person in a physical environment and in real time.

In any indoor positioning system, at first the reference nodes are placed in the indoor environment. The reference nodes may be either aware of their location or in some cases they may be placed in an unknown infrastructure.

Now let us consider a typical indoor positioning scenario in which the reference nodes are placed. The reference sensor node sends out beacon signals at particular interval of time. When any unknown node i.e. target comes under the range of a reference node, the reference node sends out a request signal to the unknown sensor node. This unknown sensor node will perceive the incoming request signals and issues a ranging reply to the sensor node. By this time, the reference node would have calculated the transmission time between the reference node and the unknown node i.e. target. Then the reference node forwards the calculated time to base station where the original position of the target will be calculated based on the various position calculation schemes such as trilateration, triangulation, etc.

Thus in any indoor positioning system, in order to determine the position of a target, there are two important steps. First one is the signal measurement phase and second one is position calculation phase. In the signal measurement phase, some signals are transmitted between a number of reference nodes and the target node. During this process, some of the signal parameters such as Time of Arrival (TOA), Received Signal Strength Indicator (RSSI) and Angle of Arrival (AoA) are measured.

The second phase is the position calculation. In this phase, the physical position of the target node will be determined based on the signal parameters obtained in the first phase. Trilateration and triangulation are two most popular geometric approaches which are used for range based localization schemes position calculation. However the measured signal parameters in real time are prone to indoor noise, hence the accuracy is only up to a certain extent. So we need optimization techniques such as filters which are often used to suppress the indoor positioning measurement noise and increase the accuracy of the output.

III. LOCALIZATION SCHEMES

The problem of estimating the spatial coordinates of an unknown node (target) is known as localization. Broadly localization techniques can be classified in two main categories i.e. Fine-grained (range-based) and Coarse-grained (range-free). In range-based localization scheme distance, time of flight, angle information is noted to determine the position of target from the sensor node. Range-based localization schemes require more sophisticated hardware to measure the signal parameters such as Time of Arrival (TOA), Angle of Arrival (AOA) and Received Signal Strength Indicator (RSSI).[6] The accuracy of such estimation, however, is subject to the transmission medium and surrounding environment. On the other hand, the Range-free localization uses only proximity (connectivity) information to measure the distance of the target from reference node. [7] Now let us see the two phases of indoor positioning system with various range based localization schemes.

A. Time of Arrival (TOA)

Time-of-Arrival (TOA) is the time measured at the receiver end at which it receives the signal. The measured TOA is actually the time taken for the transmission plus the time delay. Thus the distance between the receiver node and a reference node is determined by time of flight of the transmitting signal. In TOA measurement, the speed of the transmitted signal is known. At the receiver end, on receiving the signal, in turn, each receiver node will send a signal back to transmitting node which is the reference node.

Once the time of flight of the signal is calculated, the distance between the nodes can be determined using the formula:

$$R = \text{time} \times \text{speed} \quad (1)$$

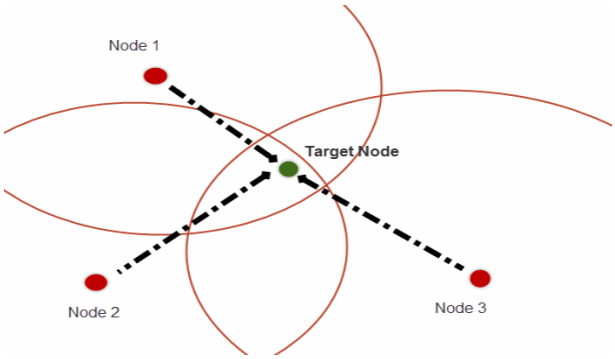


Fig.1 Time of arrival method[9]

After measuring the distance the usual method of trilateration is used for finding the position of the sensor.

A. Angle of arrival (AOA)

The Angle of Arrival (AoA) technique is another range-based localization scheme which requires directional antennas with rotating capability. It estimates relative or absolute angles between the reference nodes and the target node. AoA is defined as the angle between the propagation direction of an incident wave and some reference direction, which is known as orientation. Usually directional antennas or array of antennas are used for measuring the AoA. For proper AoA measurement, the array geometry must be known. With AOA, no time synchronization between nodes is required. But AoA requires directional antennas

with rotation capabilities which make the hardware complex.

However, If the AoA signal parameter is available, triangulation can be used to determine the position of the target node. Unlike trilateration method, in triangulation only two reference nodes are enough to predict the position of the target. Thus it reduces number of reference nodes required to detect a target

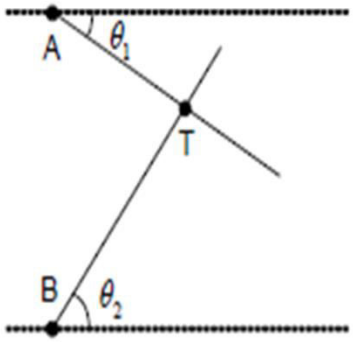


Fig.2. Angle of Arrival

As shown in Fig. 2, the reference nodes are represented by A and B. Once the angles $\theta 1$ and $\theta 2$ between the reference nodes and the target node is known, the physical position of Target T can be calculated based on the predetermined co-ordinates of the reference nodes.

C. Received Signal Strength Indicator (RSSI)

In RSSI, the distance is measured based on the attenuation introduced by the propagation of signal from the transmitting node (reference node) to the receiving node (target node). [8]The basic principle in RSSI measurement is that the signal strength is inversely proportional to distance travelled by the signal. That means the signal strength decreases as the signal travels greater distance, this decrease in signal strength is inversely proportional to the square of the distance travelled. It is given by

$$\text{Signal Strength} \propto \frac{1}{d^2} \qquad (2)$$

The main advantage of RSSI localization scheme is its lower configuration cost than the other range-based localization schemes. At the same time, RSSI measurement has larger error because of the variation of RSSI by the environment (Radio interference, Obstacles (persons, walls), Individual differences of transmitters and receivers (antenna type, transmission power etc.). Multi-path fading, background interference, irregular signal propagation makes estimates inaccurate.

IV. PROBLEM STATEMENT

If we take a closer look at the localization schemes, each one of them have their own advantages as well drawbacks. Either the hardware complexity increases or the accuracy gets reduced. So to maintain accuracy, the node density needs to be increased. So we have tried to analyze the node density effect on the localization schemes such as TOA, AOA and RSSI. Then we applied the obtained estimated position of the target by each localization scheme to the Kalman filter to improve the accuracy of lesser node density network up to the level of higher node density network.

V. SIMULATION ENVIRONMENT

We have used a MATLAB GUI called Senelex i.e. The Sensor Network Localization Explorer which is provided by OHIO STATE University [9].The Localization GUI requires MATLAB version 7.x and greater and the Optimization Toolbox to run properly. The sensor network self-localization GUI enables the user to determine the localization of arbitrary sensor networks through simulation. We kept the network size to be constant as 300x200 m^2 and array node density to be 18. At first the localization error is calculated for all signal parameters such as TOA, AOA and RSSI. Then the array node density is increased to 36 keeping the network size to be constant. Now again the simulation is run and the localization error parameter is calculated for all signal parameters.

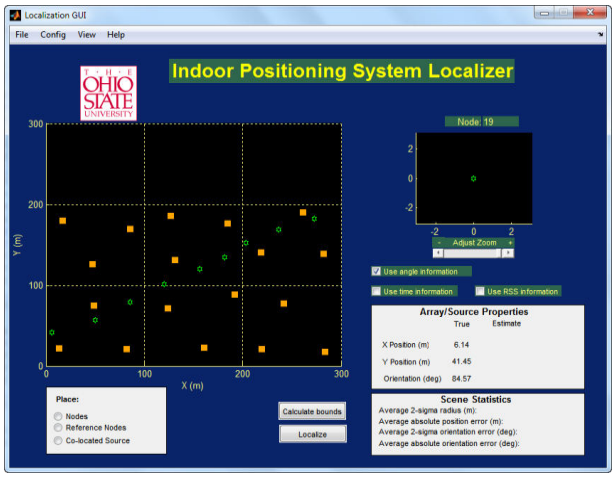


Fig.3. Sensor Network before Localization

Fig. 3 shows a network of sensor node in which 18 anchor nodes representing the orange boxes and rest other are target node position are placed within the area 300m x 200m.

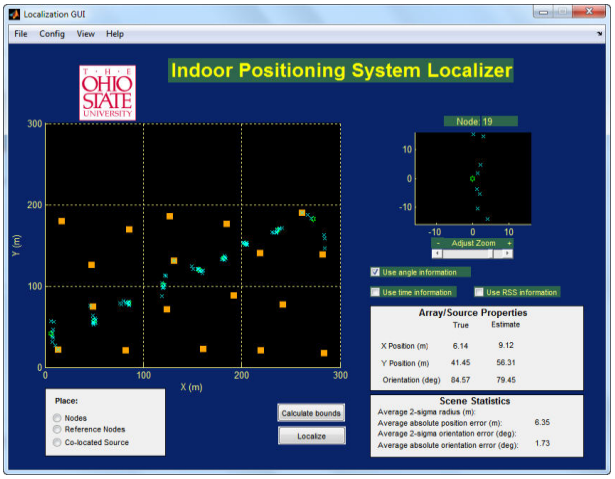


Fig.4. Sensor Network after Localization

Fig. 4 shows the localized result of the same network after applying range-based RSS scheme.

The simulations of each range-based scheme are done on each network parameters. The output of each simulation is stored into a MATLAB .m file. Then on each .m file the performance metrics is applied and the result is calculated.

The standard deviation is calculated using the following procedure:

$$LE(X) = (X - X_{est}) \quad (3)$$

$$LE(Y) = (Y - Y_{est}) \quad (4)$$

$$Mean(X) = \sum_{i=1}^{N} \frac{LE(X)}{N} \quad (5)$$

$$Mean(Y) = \sum_{j=1}^{N} \frac{LE(X)}{N} \quad (6)$$

$$\Delta X = LE(X) - Mean(X) \quad (7)$$

$$\Delta Y = LE(Y) - Mean(Y) \quad (8)$$

$$\sigma^2_{Xk} = (\Delta X)^2 \quad (9)$$

$$\sigma^2_{Yk} = (\Delta Y)^2 \quad (10)$$

VI. RESULTS

Keeping the network size constant, the network is simulated with each signal parameter such AOA, TOA and RSSI one by one. The following represents the results of the simulations.

From the exported Matlab file, the performance metrics are applied and the results are plotted versus the original position of the target node.

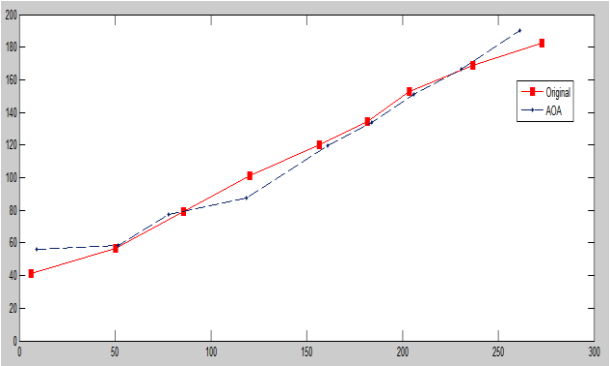


Fig.5. Angle of Arrival Estimated Position Vs Original Position

In figure 5, we can notice that the original position of the target and the estimated position of the target are not the same. The localization error between the original position and the estimated position using the Angle of Arrival parameter is found to be 14.6 and 8.3

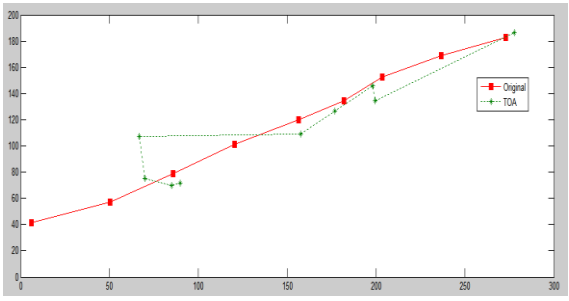


Fig.6. RSSI estimated Position vs. Original Position

In figure 6, we can notice that there is large difference between the original position of the target and the estimated position of the target.

The localization error between the original position and the estimated position using the Angle of Arrival parameter is found to be 23.6 and 16.2 respectively for two different node densities.

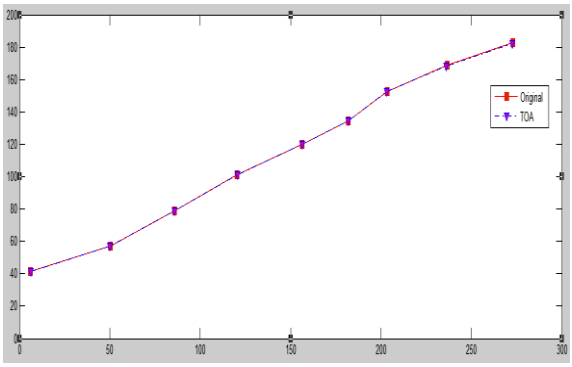


Fig.7. TOA Estimated Position vs. Original Position

In figure 7, we can notice that there is only small difference between the original position of the target and the estimated position of the target.

The localization error between the original position and the estimated position using the Angle of Arrival parameter is found to be 3.6 and 1.2 respectively for two different node densities.

VII. KALMAN FILTER

Kalman filter is a parametric filter which is used to suppress the indoor noise from the estimated position and to predict the future position. In this paper, we have considered only the noise suppression phase of the Kalman filter[10].

Kalman filter is used for filtering the measurement noise, and predict the next position of the person using system model. The KF uses the current position of the person to predict his next position for a uniform sampling period. We have assumed that the target is moving with constant velocity of .5m/s.

A. System model:

This model provides the present state of the system at any time step,

$$X_k = A^* X_{k-1} + w_k \qquad (3)$$

Where A- Represents the state transition matrix

$$\begin{pmatrix} x_p \\ y_p \\ z_p \\ x_v \\ y_v \\ z_v \end{pmatrix}_k = \begin{pmatrix} 1\,0\,0\,T\,0\,0 \\ 0\,1\,0\,0\,T\,0 \\ 0\,0\,1\,0\,0\,T \\ 0\,0\,0\,1\,0\,0 \\ 0\,0\,0\,0\,1\,0 \\ 0\,0\,0\,0\,0\,1 \end{pmatrix} * \begin{pmatrix} x_p \\ y_p \\ z_p \\ x_v \\ y_v \\ z_v \end{pmatrix}_{k-1} + W_k$$

The state vector X_k has positional components in x, y & z coordinates represented as x_p, y_p & z_p and their velocity counterparts, represented as x_v, y_v & z_v respectively.

The initial estimates are passed to the Kalman filter and the Kalman filter suppresses the noise caused to multi path and additive white Gaussian noise[11]. Thus the measurement noise is reduced in the Kalman filter.

Now again the localization error is calculated for all localization schemes such as TOA, AOA and RSSI. This time it is found that, the standard deviation in estimated position and the original position of the target is lesser.

The respective outputs for TOA, AOA and RSSI for network size with 18 nodes are found to be

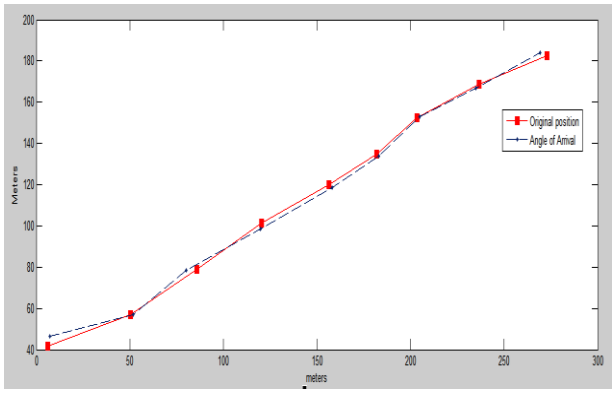


Fig.8. Angle of Arrival with Kalman Filter

Figure 8 shows that, the estimated position obtained after integrating Kalman filter is better than before. And also the localization error i.e. the standard deviation now is found to be 9.3 which are closer to network with higher node density.

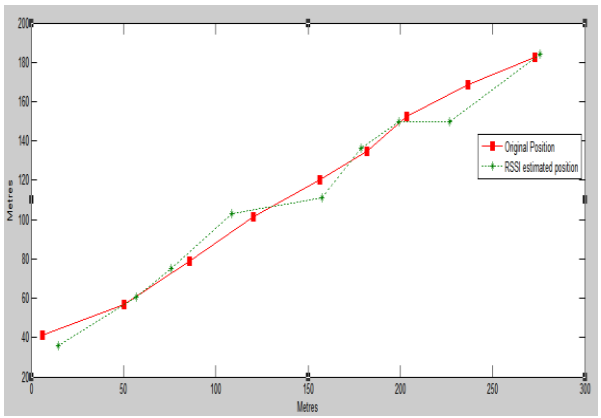


Fig.9. RSSI with Kalman Filter

Figure 9 shows that, the estimated position obtained from RSSI after integrating Kalman filter is better than before. And also the localization error i.e the standard deviation now is found to be 18.6 which is closer to network with higher node density.

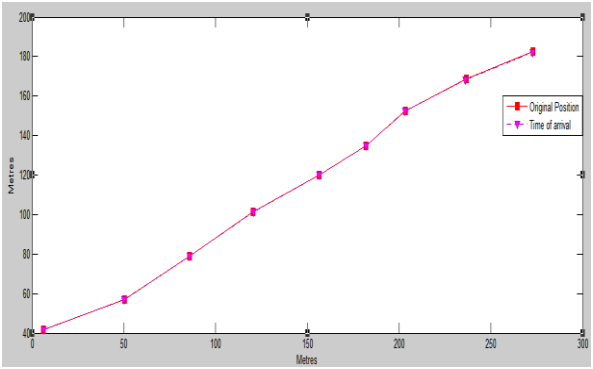


Fig.10. TOA with Kalman Filter

Figure 10 shows that, the estimated position obtained from TOA after integrating Kalman filter is better than before. And also the localization error i.e the standard deviation now is found to be 2.3 which is closer to network with higher node density.

VIII. CONCLUSION

Sensor networks are a collection of large number of low-cost, low-power, multifunctional, and small sensors and Localization is a fundamental problem of deploying wireless sensor networks for many applications. The localization can be mainly range-based or range-free according to the mechanism used for determination of location.

Simulations and experiments show the relationship between original position and the estimated position of target determined for each localization scheme. At last we would like to conclude that the range based Time Algorithm provides the lowest deviation from the mean localization error. This means lower the SD better the accuracy. So in comparison to RSS and Angle one should use Time Algorithm for localization purpose.

Similarly, with the help of Kalman Filter, the localization error of the indoor positioning system can be further reduced and also the accuracy of higher node density system can be obtained in the system of same network size but with lesser node density. Thus by integrating Kalman filter with exiting indoor positioning system, we can reduce the cost of node deployment and can improve the accuracy.

IX. FUTURE WORK

We are looking forward to implement Particle filter in indoor positioning system to track more than one target at the same time. And also Particle filter uses iterative prediction method in which we can define a preset threshold for any environment based on the noise present there.

REFERENCES

[1] Jinhong Xiao, Zhi Liu, Yang Yang, Dan Liu, Xu Han "Comparison and analysis of indoor wireless positioning techniques" Computer Science and Service System (CSSS), page 236-296, June 2011.

[2] K. Muthukrishnan, M. E. Lijding, and P. J. M. Havinga, "Towards Smart Surroundings: Enabling Techniques and Technologies for Localization", Proc. International Workshop on Location-and Context-Awareness, Berlin, Germany, 2005.

[3] I.F.Akyildiz, W.Su, Y. Sankarasubramaninam, and E. Cayirci,"A survey on sensor networks", IEEE Commun. Mag., vol 40,no. 8,pp. 102-114,Aug. 2002.

[4] M. Depsey, "Indoor Positioning Systems in Healthcare", Radianse Inc.White Paper, 2003.

[5] J. Yick,B. Mukherjee,and D. Ghosal, "Wireless sensor network survey", Computer Networks J., vol 52 , pp. 2292-2330,Apr. 2008

[6] N. Patwari, A. O. Hero III , M. Perkins, N. S.Correal, and R. J. O'Dea, "Relative location estimation in wireless sensor networks", IEEE Trans. Signal Processing, vol. 51,no. 8,pp 2137-2148, Aug.2003.

[7] K. Langendoen and N. Reijers, "Distributed localization in wireless sensor networks: A quantitative comparison",Computer Networks J.,vol 43,pp. 499-518, 2003.

[8] J. N. Ash and L. C. Potter, "Sensor network localization via received signal strength measurements with directional antennas," in Proceedings of the 2004 Allerton Conference on Communication, Control, and Computing, 2004.

[9] J. N. Ash. SeNeLEx: The Sensor Network Localization Explorer. [Online]. Available:

http://www.ece.osu.edu/ ~ashj/localization/

[10] Greg Welch and Gary Bishop, "An Introduction to the Kalman Filter", TR 95-041, http://www.cs.unc.edu/ ~welch/media/pdf/kalman_i ntro.pdf

[11] A.S. Paul and E. A. Wan, "WI-FI based indoor localization and tracking using sigma-point Kalman filtering methods," in Proceedings of PLANS 2008 IEEE/ION Position Location and Navigation Symposium, 2008.

❑❑❑

An Efficient Privacy Management Technique in Cloud Environment - SHES

.

Design of Circular Polarized Microstrip Patch Antenna for L band

Jolly Rajendran, Rakesh Peter & KP Soman

Amrita Vishwa Vidyapeetham, Coimbatore, India

Abstract - In this paper, we share our experience of designing a circularly polarized square patch antenna at L band. The antenna is designed using a relatively cheap substrate FR-4 with permittivity ε_r = 4:4 and loss tangent tanδ = 0:02. The antenna has a gain of 5dB. Simulated response shows that the designed antenna has an input impedance(Z_{in}) of 50Ω approximately. An efficiency of 65% is obtained for a single patch. It has a narrow bandwidth and a high Q factor. The design procedure, feed mechanism and simulation results are presented in this paper.

Keywords - *Dielectric substrates, L-band, Microstrip antennas, Patch antennas, Polarization, Circularly polarized square patch antenna.Keywords - Precision farming, attribute oriented induction, data generalization.*

I. INTRODUCTION

L-band frequencies are used in mobile satellite, cellular and personal communication systems. Circular polarized antennas are used for satellite communication between base station and a mobile unit [1][2]. Compact, directive antennas are required for the same. Microstrip patch antennas are compact, conformal to both planar and non-planar surfaces, have good efficiency and are easy to produce as arrays. They are cheaper and easy to install. These characteristics make them an ideal candidate for the communication applications. Radiation properties of microstrip structures has been known since mid 1950s. A microstrip patch antenna consists of a radiating patch which is made up of a conducting material like copper or gold on one side of a dielectric substrate and ground plane on the other side. The patch could be of different shapes viz. square, rectangular, circular, triangular or elliptical[3]. Usually rectangular and circular microstrip resonant patches are used in array configurations due to their simple geometry and ease of design. Microstrip patch antennas support both linear as well as circular polarization and capable of dual and triple frequencies. Circularly polarized antennas have been developed with single and dual feed arrangement. In this paper design of a circularly polarized rectangular patch with dual feed is proposed. Dual feed excites two orthogonal field components with equal amplitudes but a 90^0 phase difference.

II. ANTENNA CONFIGURATION AND DESIGN PROCEDURE

The geometry of circulary polarized antenna is shown in Figure 1. The antenna consists of a rectangular patch etched on a 60 mil thick FR-4 substrate. The patch and ground plane are made of a high conductivity metal, copper and is of thickness 't'. The patch is of length 'L' and width 'W' and is etched on a dielectric substrate of thickness 'h' and permittivity ε_r.

2.1 Substrate

The dielectric constant of substrates used for microstrip patch antennas are typically in the range 2:2 $\ll \varepsilon_r \ll$ 12. Lower the permittivity of the substrate, wider is the fringing field and better is the radiation. With the decrease of permittivity antenna bandwidth and efficiency increases. But lowering the permittivity decreases the input impedance and increases the size of the antenna. FR-4 substrate with ε_r = 4:4 is chosen for the design of the proposed antenna. Thickness of substrate is chosen such that

$$h > 0.06\lambda_g \tag{1}$$

where λ_g is the guided wavelength given by Equation (2).

$$\lambda_g = \frac{\lambda_0}{\sqrt{\epsilon}} \tag{2}$$

A tradeoff has to be made while selecting the substrate thickness. As thickness of substrate increases, surface waves are induced within the substrate. Surface waves results in undesired radiation, decreases antenna efficiency and introduces spurious coupling between different circuits or antenna elements. Also surface waves reaching the outer boundaries of an open microstrip structure are reflected and diffracted by the edges. These diffracted waves provide an additional contribution to radiation, degrading the antenna pattern by increasing the side lobe and cross polarization levels. Thus thickness should be chosen such that surface waves are suppressed. A thick substrate with low dielectric constant yeilds better efficiency, larger bandwidth and better radiation, where as a thin substrate with higher dielectric constant yeilds compact antenna, with less efficiency and narrower bandwidth. Thus a compromise has to be made between the antenna dimensions and antenna performance. A 60 mil FR-4 substrate is used in the proposed design.

2.2 Patch Dimension

A square patch is chosen for symmetry.

2.2.1 Patch thickness

The patch is selected to be very thin such that $t \ll \lambda_0$ where λ_0 is the free space wavelength given by Equation (3). The patch thickeness is chosen to be 0.1 mm.

$$\lambda_0 = \frac{c}{f_0} \tag{3}$$

In Equation (1) 'c' is the velocity of light known as 3x108m/s and f_0 is the resonant frequency of patch which is chosen as 1GHz.

2.2.2 Design Equations

The effective permittivity of the FR-4 substrate (ε_r = 4:4) is found using Hammerstad and Jensen model[4] as follows.

$$\epsilon eff = \frac{\epsilon_r + 1}{2} + \frac{\epsilon_r - 1}{2} \times (1 + \frac{10h}{W})^{-ab} \tag{4}$$

with

$$a = 1 + \frac{1}{49} \ln[\frac{(u^4 + (\frac{u}{52})^2)}{u^4 + 0.432}] \tag{5}$$

$$b = 0.564[\frac{\epsilon_r - 0.9}{\epsilon_r + 3}]^{0.093} \tag{6}$$

$$W$$

$$u = \frac{W}{h} \tag{7}$$

Effective length is given by [3]

$$Leff = \frac{c}{2f0} \times \sqrt{\frac{1}{(\epsilon_{eff})}} \tag{8}$$

Scattering length Δ

$$\Delta = 0.412h \frac{\epsilon eff + 0.3}{\epsilon eff - 0.258} \times \frac{u + 0.264}{u + 0.8} \tag{9}$$

Real Patch Length L is given by

$$L = Leff - \Delta \tag{10}$$

For a rectangular patch, the length of the patch L controls the resonant frequency and width W controls the input impedance and radiation pattern. The wider the patch, the larger is the input impedance. The nearly square patch (L=W) is used for the proposed antenna. Length is chosen as 59.08 mm as calculated from the above design equations.

2.3 Feed

The feedlines are directly coupled to the resonant patch. Critical coupling is achieved at resonant frequency via a quarter wave transmission line section of characteristic impedance Z_T given by

$$Z_T = \sqrt{Z_f R_r} \tag{11}$$

where *Rr* is the input impedance of the resonant patch and Z_f is the characteristic impedance of transmission line feed which is 50 Ohms (width = 2.892 mm). The width and length of the quarter wave transmission line section (Z_T = 89.744 ohms) was found out using LineCalc tool in ADS for resonant frequency 1.147GHz and was found to be 0.1438 mm and 36.77 mm respectively. The position of the feed controls the input impedance.

The resonant patch is fed via a 90^0 branch line coupler. The branch line coupler divides the power equally into the two output ports. The signal is fed via one of the ports, while the other port is grounded through a 50Ω resistor. The signal arriving at the two output ports of the branch line coupler are 90^0 out of phase. The feed lines are extended further and bend such that the total delay produced in the two feed lines are the same. The resonant patch is thus fed at two points as shown in Figure 1 such that the signals have a 90^0 phase difference. This dual feed arrangement excites two

orthogonal field components with equal amplitude but 90^0 phase difference resulting in circular polarization.

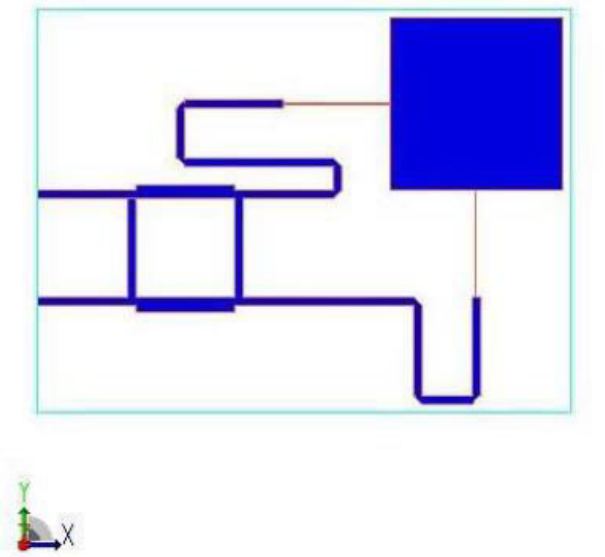


Fig. 1: Geometry of Circular polarized patch antenna

III. SIMULATION RESULTS

The antenna is modelled and simulated using Momentum. Figure 2.a and 2.b gives the magnitude and phase of S_{11} vs frequency. The resonant frequency f_0 of the antenna is 1.14 GHz. The fractional bandwidth is given by

$$BW = \frac{f_2 - f_1}{f_0} \qquad (12)$$

The antenna has a very narrow bandwidth, approximately 0.9% and has a high Q factor. Q factor is given by

$$Q = \frac{f_0}{BW} \qquad (13)$$

Q factor was found to be 111. Figure 2.c shows the antenna has an input impedance(Z_{in}) of 56:25 + j12:2Ω. Thus the designed antenna is almost matched to the characteristic impedance Z_0 which is assumed to be 50 ohms. The reactive part +j12:2Ω could be cancelled out by adding a series capacitor of 39pF during fabrication. From the simulation results shown in Figure 3.a and Figure 3.c, the antenna has a gain of 5 dB and efficiency of 65%. Figure 4.a and Figure 4.c shows the magnitude and phase of electric field for various values of θ. The antenna is right circular polarized. The two orthogonal components which are same in magnitude and in phase quadrature results in circular polarization. These components could be described by the Equation(14)(15) and the circularly polarized wave by (16).

$$\mathbf{E_{right}} = E_0 sin(\omega t - \beta z)\mathbf{a_x} \qquad (14)$$

$$\mathbf{E_{left}} = E_0 cos(\omega t - \beta z)\mathbf{a_y} \qquad (15)$$

$$\mathbf{E} = \mathbf{E_{right}} + \mathbf{E_{left}} \qquad (16)$$

The 3-D radiation pattern is shown in Figure 5. Figure 4.b and Figure 4.d shows the magnitude and phase of axial ratio for different values of θ.

IV. CONCLUSION

Finally we complete our discussion with the fundamental issues that need to be addressed in future. Though compact when compared to conventional antennas, the antenna has a very low efficiency and narrow bandwidth. The bandwidth could be improved by incorporating lossy material or resistors. Also slots could be introduced to improve bandwidth. Furthermore the antenna could be formed into arrays to get better directivity.

REFERENCES

[1] Wu, W. W., E. F. Miller, W. L. Pritchard, and R. L. Pickholtz, "Mobile satellite communications," Proc. IEEE, vol. 82, 1431-1448, 1997.

[2] Miller, "Satellite free the mobile phone," IEEE Spectrum, vol. 35, 26-35, 1998.

[3] I.J.Bahl and P.Bhartia, "Microstrip Antennas," Dedham, MA: Artech House, 1980.

[4] E. Hammerstad and Jensen, "Accurate Models for Microstrip Computer-Aided Design," Symposium on Microwave Theory and Techniques, pp. 407-409, June 1980.

[5] J R James and P. S. Hall, "Handbook of Microstrip Antennas," vol.1, IEE Electromagnetic Waves Series 28, 1989.

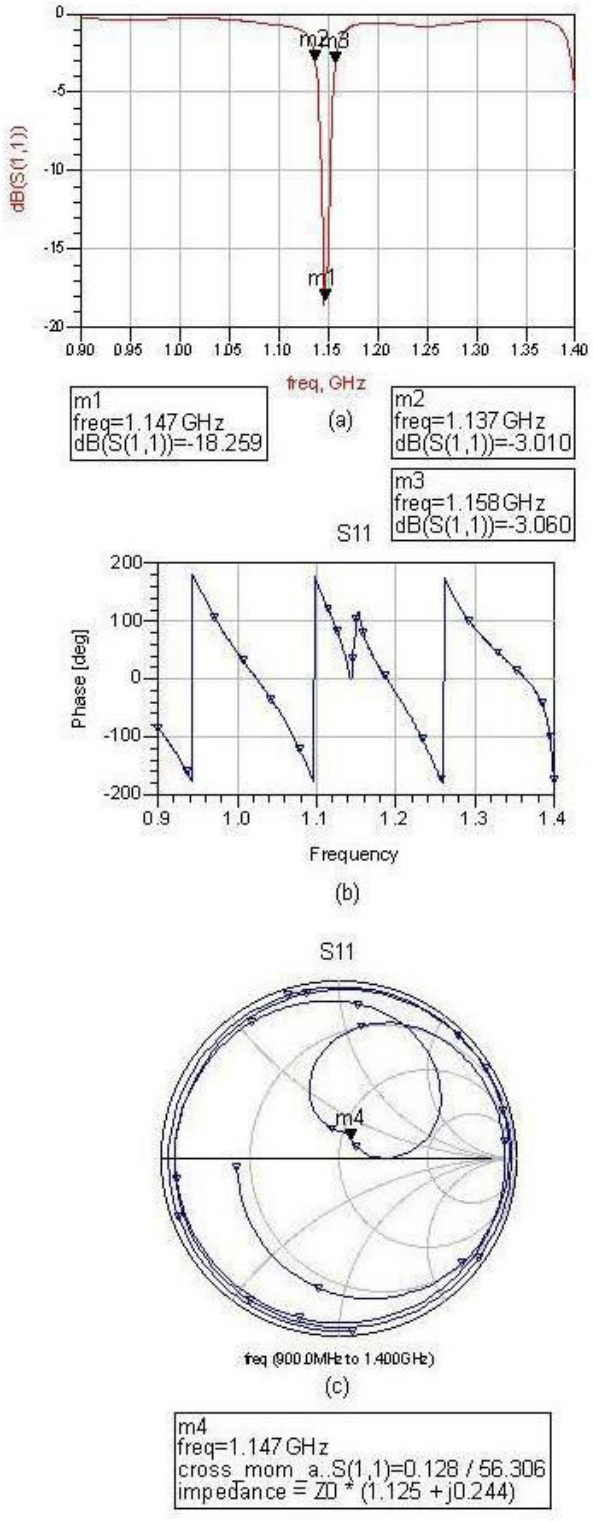


Fig. 2 : (a) Return loss vs. frequency(magnitude plot) (b) Return loss vs. frequency(phase plot) (c) S11 plot on Smith Chart

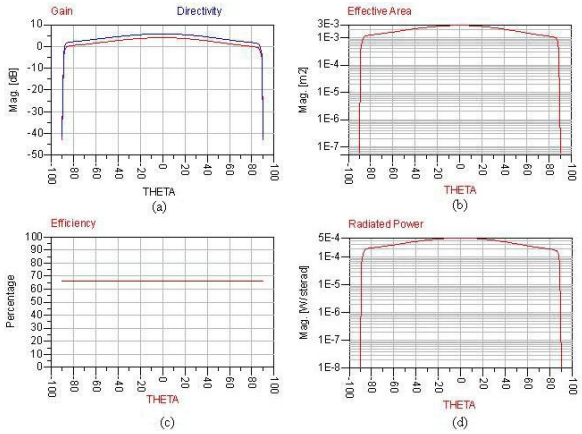


Fig. 3 : (a) Gain and Directivity vs. Theta (b) Effective Area vs. Theta (c) Efficiency vs. Theta (d) Radiated Power vs. Theta

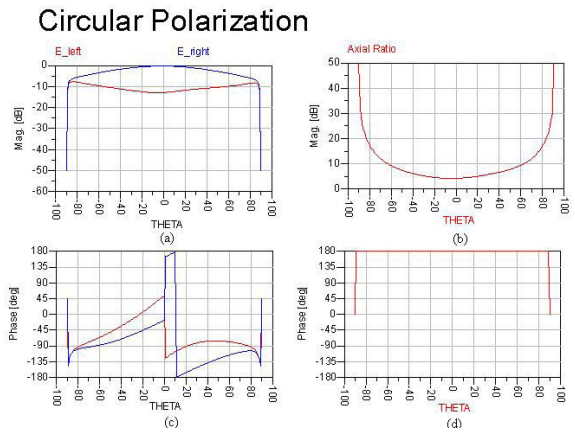


Fig. 4 : (a) Electric Field vs. Theta(magnitude plot) (c) Axial Ratio vs. Theta(magnitude plot) (c) Electric Field vs. Theta(phase plot) (d)Axial Ratio vs. Theta(phase plot)

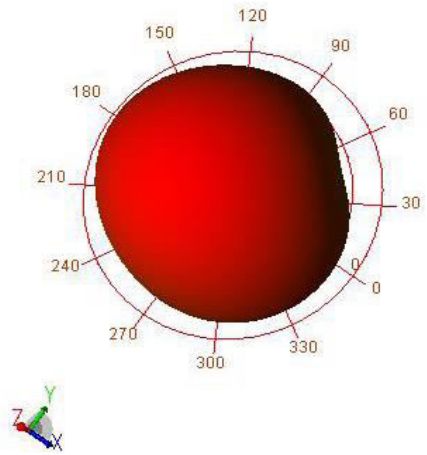


Fig. 5 : Three dimensional radiation pattern

❑❑❑