Global Journal of Computer Science and Technology

discovering thoughts and inventing future

Volume 10 Issue 8 Version 1.0 Online ISSN: 0975-4172 Print ISSN: 0975-4350

highlights

- Hybrid Algorithm Approach
- Implementing Graphical Passwords
- Cognitive Radio Networks
- Critical Node Test Mechanism

20 Technology Reforming Ideas

September 2010

ENG

Global Journal of Computer Science and Technology

Global Journal of Computer Science and Technology

Volume 10 Issue 8 (Ver. 1.0)

Global Academy of Research and Development

Incorporation No.: 0423089
License No.: 42125/022010/1186
Registration No.: 430374
Import-Export Code: 1109007027
Employer Identification Number (EIN):
USA Tax ID: 98-0673427

Global Journals Inc.

*(A Delaware USA Incorporation with "Good Standing"; **Reg. Number: 0423089**)*

Sponsors: Global Association of Research
Open Scientific Standards

Publisher's Headquarters office

Global Journals Inc., Headquarters Corporate Office, Cambridge Office Center, II Canal Park, Floor No. 5th, ***Cambridge (Massachusetts)***, Pin: MA 02141 United States
USA Toll Free: +001-888-839-7392
USA Toll Free Fax: +001-888-839-7392

Offset Typesetting

Global Journals Inc., City Center Office, 25200 Carlos Bee Blvd. #495, Hayward Pin: CA 94542 United States

Packaging & Continental Dispatching

Global Journals, India

Find a correspondence nodal officer near you

To find nodal officer of your country, please email us at *local@globaljournals.org*

eContacts

Press Inquiries: *press@globaljournals.org*
Investor Inquiries: *investers@globaljournals.org*
Technical Support: *technology@globaljournals.org*
Media & Releases: *media@globaljournals.org*

Pricing (Including by Air Parcel Charges):

For Authors:
22 USD (B/W) & 50 USD (Color)
Yearly Subscription (Personal & Institutional):
200 USD (B/W) & 500 USD (Color)

Editorial Board Members

Dr. Bart Lambrecht
Director of Research in Accounting and Finance Professor of Finance
Lancaster University Management School
BA (Antwerp); MPhil, MA, PhD (Cambridge)

Dr. Carlos García Pont
Associate Professor of Marketing
IESE Business School, University of Navarra
Doctor of Philosophy (Management), Massachusetts Institute of Technology (MIT)
Master in Business Administration, IESE, University of Navarra
Degree in Industrial Engineering, Universitat Politècnica de Catalunya

Dr. Fotini Labropulu
Mathematics - Luther College
University of ReginaPh.D., M.Sc. in Mathematics
B.A. (Honors) in Mathematics
University of Windso

Dr. Lynn Lim
Reader in Business and Marketing
Roehampton University, London
BCom, PGDip, MBA (Distinction), PhD, FHEA

Dr. Mihaly Mezei
ASSOCIATE PROFESSOR
Department of Structural and Chemical Biology
Mount Sinai School of Medical Center
Ph.D., Etvs Lornd University
Postdoctoral Training, New York University

Dr. Söhnke M. Bartram
Department of Accounting and FinanceLancaster University Management School Ph.D. (WHU Koblenz)
MBA/BBA (University of Saarbrücken)

Dr. Miguel Angel Ariño
Professor of Decision Sciences
IESE Business School
Barcelona, Spain (Universidad de Navarra)
CEIBS (China Europe International Business School).
Beijing, Shanghai and Shenzhen
Ph.D. in Mathematics
University of Barcelona
BA in Mathematics (Licenciatura)
University of Barcelona

Philip G. Moscoso
Technology and Operations Management
IESE Business School, University of Navarra
Ph.D in Industrial Engineering and Management, ETH Zurich
M.Sc. in Chemical Engineering, ETH Zurich

Dr. Sanjay Dixit, M.D.
Director, EP Laboratories, Philadelphia VA Medical Center
Cardiovascular Medicine - Cardiac Arrhythmia
Univ of Penn School of Medicine

Dr. Han-Xiang Deng
MD., Ph.D
Associate Professor and Research
Department Division of Neuromuscular Medicine
Davee Department of Neurology and Clinical Neurosciences
Northwestern University Feinberg School of Medicine

Dr. Pina C. Sanelli
Associate Professor of Public Health
Weill Cornell Medical College
Associate Attending Radiologist
New York-Presbyterian Hospital
MRI, MRA, CT, and CTA
Neuroradiology and Diagnostic Radiology
M.D., State University of New York at Buffalo, School of Medicine and Biomedical Sciences

Dr. Roberto Sanchez
Associate Professor
Department of Structural and Chemical Biology
Mount Sinai School of Medicine
Ph.D., The Rockefeller University

Dr. Wen-Yih Sun
Professor of Earth and Atmospheric SciencesPurdue University Director
National Center for Typhoon and Flooding Research, Taiwan
University Chair Professor
Department of Atmospheric Sciences, National Central University, Chung-Li, Taiwan University Chair Professor
Institute of Environmental Engineering, National Chiao Tung University, Hsin-chu, Taiwan.Ph.D., MS The University of Chicago, Geophysical Sciences
BS National Taiwan University, Atmospheric Sciences
Associate Professor of Radiology

Dr. Michael R. Rudnick
M.D., FACP
Associate Professor of Medicine
Chief, Renal Electrolyte and Hypertension Division (PMC)
Penn Medicine, University of Pennsylvania
Presbyterian Medical Center, Philadelphia
Nephrology and Internal Medicine
Certified by the American Board of Internal Medicine

Dr. Bassey Benjamin Esu
B.Sc. Marketing; MBA Marketing; Ph.D Marketing
Lecturer, Department of Marketing, University of Calabar
Tourism Consultant, Cross River State Tourism Development Department
Co-ordinator , Sustainable Tourism Initiative, Calabar, Nigeria

Dr. Aziz M. Barbar, Ph.D.
IEEE Senior Member
Chairperson, Department of Computer Science
AUST - American University of Science & Technology
Alfred Naccash Avenue – Ashrafieh

Chief Author

Dr. R.K. Dixit (HON.)
M.Sc., Ph.D., FICCT
Chief Author, India
Email: authorind@computerresearch.org

Dean & Editor-in-Chief (HON.)

Vivek Dubey(HON.)
MS (Industrial Engineering),
MS (Mechanical Engineering)
University of Wisconsin
FICCT
Editor-in-Chief, USA
editorusa@computerresearch.org

Er. Suyog Dixit
BE (HONS. in Computer Science), FICCT
SAP Certified Consultant
Technical Dean, India
Website: www.suyogdixit.com
Email:suyog@suyogdixit.com,
dean@computerresearch.org

Sangita Dixit
M.Sc., FICCT
Dean and Publisher, India
deanind@computerresearch.org

Contents of the Volume

From the Chief Author's Desk

We see a drastic momentum everywhere in all fields now a day. Which in turns, say a lot to everyone to excel with all possible way. The need of the hour is to pick the right key at the right time with all extras. Citing the computer versions, any automobile models, infrastructures, etc. It is not the result of any preplanning but the implementations of planning.

With these, we are constantly seeking to establish more formal links with researchers, scientists, engineers, specialists, technical experts, etc., associations, or other entities, particularly those who are active in the field of research, articles, research paper, etc. by inviting them to become affiliated with the Global Journals.

This Global Journal is like a banyan tree whose branches are many and each branch acts like a strong root itself.

Intentions are very clear to do best in all possible way with all care.

Dr. R. K. Dixit
Chief Author
chiefauthor@globaljournals.org

III. RESEARCH PROBLEM AND HYPOTHESIS

There is no direct method to run aggregate function of SQL on the encrypted data. Hypothesis of the proposed solution is to keep sensitive data column in unencrypted form in another table. This will resolve the above mentioned problem.

IV. PROPOSED METHOD AND ITS WORKING METHODOLOGY

This paper proposes a new method for directly running the aggregate function of SQL on encrypted data column. In this method two tables are used for that table which have encrypted data column. One table is the actual table and other one is just a dummy table. The dummy table will contain the encrypted data column of the actual table in the unencrypted form and hash values of that column which is used in the WHERE clause. The order of the rows will be shuffled in the dummy table in order to provide security even it is accessed by unauthorized person. There is no direct link between the actual table and this dummy table. The dummy table will be stored in secured schema. The dummy table will only be used for the aggregate function's queries.

The working methodology will be follows

When user performing query to the table having encrypted data column, so its nature will be checked. If the query having aggregate function on the encrypted data then it will be transformed to the dummy table to solve the aggregate function. The dummy table can only be accessed by thoseusers who have clearance to the encrypted data. In this method there is no need to decrypt any value.

Table 4.1: Actual_Table

Name	Salary	Job Title	Company Name
Ikram	Encrypted	Manager	Stop-Loss 200
Umar	Encrypted	Assist manager	Atlanta Medical Services
Shahid	Encrypted	N/A admin	First Midwest Financial

TABLE 4.2 Dummy_table

XYZ (Salary column of Actual_Table)	Hash Values of company name
12000	41789000916342
10000	41789000916346
9000	14146267157396
13000	41789040916342

EXAMPLE

Reference to Table 4.1, consider the user's following query over the Actual_Table.

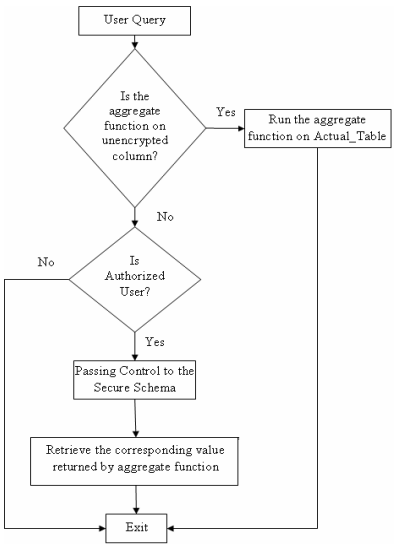
SELECT Emp_Name, SUM(Salary)
FROM Actual_Table
WHERE [Company Name] = _Stop-Loss 200'
GROUP BY Emp_Name

The algorithm interprets the above query and transform as follow:

SELECT Emp_Name, (SELECT SUM(Salary) FROM Dummy_table WHERE [Hash Values of company name] =HashvalueGerateFunction(Stop-Loss 200))
FROM Actual_Table
GROUP BY Emp_Name

Here, in the first query if user wants to find sum of the salaries of all employees in a particular company, so he/she must decrypt that values and then retrieves the required aggregated value of sum function. In case of proposed approach the query is intercepted into the form as shown in example. In the case of second query there is no need to decrypt the values for finding the sum of salaries of employees. The inner query calculates the required aggregate function value directly from the dummy table which increases system performance.

V. FLOW CHART OF THE PROPOSED SYSTEM3



V. ALGORITHM

Following are the algorithmic steps of the proposed algorithm

1. [User Query]
   User poses query
2. [Check the aggregation Column]
   If (aggregation function is not on encrypted column)
   Goto step 3
   Else if (Authorized User)
   Goto step 4
   Else
   Goto step 5
3. [Perform aggregate function on Data]
   Run the aggregate function on Actual_Table
   Goto step 5
4. [Passing Control to the Secure Schema]
   [Run aggregate function on column in secure schema]
   Retrieve the corresponding value returned by aggregate function
5. Exit

VI. SECURITY IN THE PROPOSED SYSTEM

Sensitive data column in database can be categorized in to the following two types:
i. Independent data column
ii. Dependent data column

A. Independent data column

The data column which can be used independently for some information leakness for example the prepaid cards number of a telecom company. If the prepaid card number is stolen by someone so he/she will simply use it without any extra information.

B. Dependent data column

The dependent data columns are those whose information can not be used independently. Its data can be informative when the data of some other column is combined with it. For example salary in the employee table of anorganizational database. Salary information is sensitivewhen the employee record is available and if the employee
record does not exist then the salary information ismeaningless. similarly passwords column which needs user
name to get information from it.An organization has a lot of data in which some is verysensitive and important for that organization. All of the datain organization may not be as much sensitive but some maybe sensitive. Similarly in a table all the columns may not beimportant for the organization security point of view. Inproposed technique security is proposed at column level asall the columns may not be sensitive. Sensitive column is encrypted in the actual table and a copy of the same columnis stored in another dummy table which only used for the aggregate type queries on the encrypted column. First security layer is that the dummy table is stored in a secure schema. Only those users will have access to secure schema that have clearness to the encrypted data. The proposedsystem is very secure in the case of Dependent data columnas there is no direct relationship between the actual table anddummy table. If the secure schema layer is broken by hackerstill no information can be extracted from data in the case of
dependent data.

VII. EXPERIMENTAL RESULTS

Proposed algorithm has been tested on TPC (Transaction Processing Performance Council) [14] schema and data. A table of TPC-E schema named Cash_transaction is used for testing purposes. It has total 133152 records. Different amount of data has been retrieved for different queries having aggregate function.

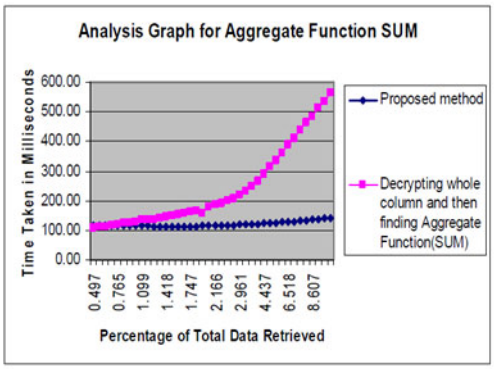


Figure 7.1: analysis graph of SUM aggregate function
The figure 7.1 shows the analysis graph of SUM aggregate function. It is shown in graph that if the queried rows are less than the 0.7 % of total rows, retrieved from table then the state of art technique is better than ours, but greater than 0.7 % gives efficient results in the proposed technique.

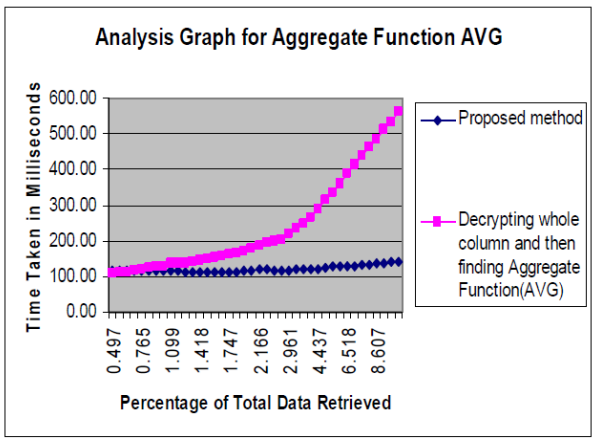


Figure 7.2: Analysis graph of average (AVG) aggregate function

The graph (Figure 7.2) is the experimental results of aggregate function AVG (average). Here, again the results of the state of art technique is better in the case of less data retrieval upto 0.7 % of total rows but expensive performance wise when selected rows in the SELECT query is more than the 0.7 % of total rows of table.

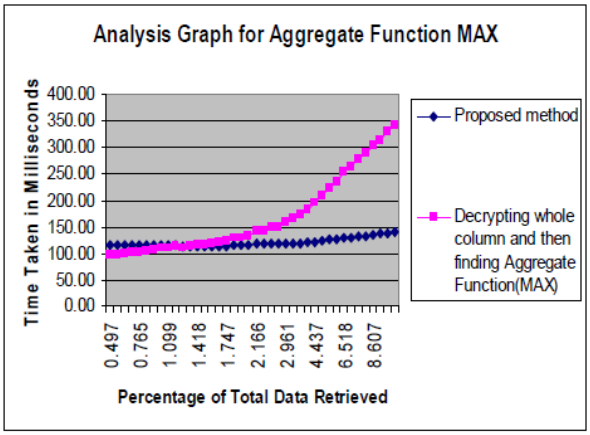


Figure 7.3: Analysis graph of MAX (maximum) aggregate

Function

The graph (figure 7.3) is the experimental results of the aggregate function MAX‘s query. It is obvious from the graph that the proposed system is better when we find the maximum value in more than the 1.5% of total rows in table.

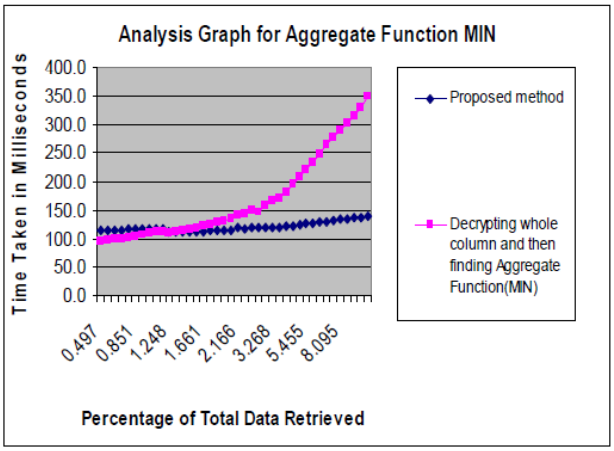


Figure 7.4: Analysis graph of MIN (minimum) aggregate Function

Figure 7.4 shows the graph of experimental results of aggregate function MIN (minimum) performance forproposed and state of arts technique. Again like the MAX, the MIN aggregate function is also better in the case of rows affected by query is more than 1.5 % of total rows in the table.

If we look to all the four graphs so the results is better in the case of proposed technique over the state of art technique. We used that state of art technique in which the total effected rows are decrypted and then the aggregate function is run on it. All the results for the proposed technique are better when the total effected rows of a table are more than 1% of total rows in that table. In the typical environment the aggregate function is run on the data in which at least more than 1% rows are selected. For example in a company there are ten different groups of worker and manager of thecompany is interested to find the minimum, maximum,average, or sum of salaries of all workers in a particulargroup then the probability of rows to be affected, in the table

of workers, is 10% of total rows. It means that in the typical environment the rows affection is more than 1% of the total.

VIII. CONCLUSION

This work proposes an efficient technique for handling aggregate function‘s query over encrypted data. All tests conducted on the TPC schema and data. Results of the experiments are satisfactory. The proposed technique is efficient when the rows affection in the SELECT query having an aggregate function is more than 1% of the total rows.

IX. REFERENCES

1) Ambhore, P.B. Meshram, B.B. and Waghmare, V.B. (2007). A implementation of object oriented database security, in Fifth International Conference on Software Engineering Research, Management and Applications. 359 – 365.
2) Bertino, E. Betini, C. Ferrari, E. Samarati, P.(1996). Supporting periodic authorization andtemporal reasoning in data base access control, in 22nd Intl. Conf. On very Large Data bases.Bombay (India). 472-483.
3) Bertino, E. Samarti, P. Jajodia, S. (1997). An extended authorization mode, in IEEE Trans. On knowledge and data Engineering. 85-101.
4) Sloan, J.A., and Sloan, R.H. (2004). A layered design of discretionary access controls with decidable properties, in IEEE Symp.Security and Privacy. 56–67.
5) Kiely, D., (2006). Protect Sensitive Data Using Encryption in SQL Server 2005..
6) Agrawal R., Kiernan, J. Srikant, R. Xu,Y. (2004). Order Preserving Encryption for Numeric Data, in SIGMOD 2004. ACM New York, NY, USA Paris, France. 563 - 574.
7) Huang, Q., (2009). Research on ciphertext index method for relational database, in 2009 2nd IEEE International Conference on Computer Science and Information Technology. Beijing, China. 445-449.
8) Sesay, Z.Y., Chen, J. and Xu, D. (2004). A Secure Database Encryption Scheme, IEEE. 49-53.
9) Sion, R., (2005). Query Execution Assurance for Outsourced Databases, in 31st VLDB Conference. Trondheim, Norway. 601-612.
10) Wang, Z. Wang, W. Shi, B.L. (2005). Storage and Query over Encrypted Character and Numerical Data in Database in Computer and Information Technology. 77-81.
11) Zhang, Y. Wang.-X.L., Niu, Z.M. (2008). A Secure Cipher Index over Encrypted Character Data in Database, in Seventh International Conference on Machine Learning and Cybernetics. IEEE: Kunming. 1111-1116.
12) Hacigumus, H. Iyer, B. Li, C. and Mehrotra, S. (2002). Executing SQL over encrypted data in the database-service-provider model, in SIGMOD02. ACM. 216–227.
13) Tang, Y. and Zhang, L. (2005). Adaptive Bucket Formation in Encrypted Databases, in IEEE International Conference on e-Technology, e-Commerce and e-Service on e-Technology, e-Commerce and e-Service. IEEE Computer Society Washington, DC, USA. 116 - 119.
14) TPC Benchmark Specification, http://www.tpc.org/

Employing Artificial Intelligence to eCommerce Web service

GJCST Classification
I.2.1,H.3.5

R. Vadivel[1] Dr. K. Baskaran[2]

***Abstract*-In recent years, web services have played a major role in computer applications. Web services are essential, as the design model of applications are dedicated to electronic businesses. This model aims to become one of the major formalisms for the design of distributed and cooperative applications in an open environment (the Internet). A main objective of this paper is application of techniques from the field of artificial intelligence (AI) to the field of web services (WS). Current commercial and research-based efforts are reviewed and positioned within these two fields. Particular attention is given to the application of AI techniques to the important issue of WS composition. Within the range of AI technologies considered, we focus on the work of the Semantic Web and Agent-based communities to provide web services with semantic descriptions and intelligent behavior and reasoning capabilities. Re-composition of web services is also considered and a number of adaptive agent approaches are introduced and implemented in publication domain and one of the areas of work is eCommerce.**

Keywords-Web Services, Semantic Web, eCommerce, Artificial intelligence, Publication Domain, Dynamic Web

I. Introduction

Currently, Web services give place to active research and this is due both to industrial and theoretical factors. On one hand, Web services are essential as the design model of applications dedicated to the electronic business. On the other hand, this model aims to become one of the major formalisms for the design of distributed and cooperative applications in an open environment (the Internet). Research in the field of semantic web / web service (WS) and artificial intelligence (AI) communities are coming together to develop solutions that will take us to the next and more mature generation of the web application. The composition of web services to create a value-chain greater than the sum of the parts is a key part of what can be expected. The fulfilment of the vision of the web as an information-providing and world-altering provider of servicesis not far away. More futuristic is the notion of serendipitous. In both visions the services and outcomes may be the same.

However, the difference between the two visions is that the first can be achieved through static and manual solutions and the second requires dynamic and automated solutions. While helpful for the first, the addition of semantic content on the web is essential to enable automatic discovery and composition of multiple services. It is natural that earlier work in the field of AI will assist in realization of the (artificially) intelligent web. The work on the Web Services Modelling Framework(WSMF) is an example of AI being applied to this field. WSMF offers the combined use of ontology, goal (problem-type) repositories, web service descriptions and mediators to handle interoperability issues. The agent community, which is primarily AI-based, has also been actively conducting WS related research.

Our own distributed agent-based work and the AgentFactory, originates from our earlier AI research intocomplex knowledge based systems and generic task basedconfiguration. On the one hand, our work on planning andautomated configuration offers a way of composing eCommercewebservices. On the other hand, WSs potentially provide uswith components needed to achieve an implementation ofour design. Through the addition of techniques from theSemantic Web community, the benefits of combining ouragent technology with WSs has been mutual.

This paper offers a review of research that overlaps thefields of WS and AI. In the following section we describeweb services and the need for semantics to be added. In*section B* we look at how the Semantic Web communities, within the field of AI, are offering semantics. In *section C*we present AI-based research to address the discovery of

WSs. In *section D* we consider both commercial and AIbasedtechniques for WS composition. In *section E*, thenotion of re-composition of WS is considered and howadaptive agent technology, including our own, can addressthis problem. We conclude with future directions for therole of AI in the web services field.

II. Related Works

A. Web Services

Web services are typically application programming interfaces (API) or web APIs that can be accessed over a network, such as the Internet, and executed on a remote system hosting the requested services.

Web services are a new way of connecting business. Web services are platform-neutral and vendor-independent protocols that enable any form of distributed processing to be performed using XML and Web-based technologies.

1) Just-in-time integration

The Web Services architecture describes the principles behind the next generation of e-business architectures, presenting a logical evolution from object-oriented systems to systems of services. Web Services systems promote

About-[1]Computer Science, Karpagam University Pollachi Road, Eachanari, Coimbatore, Tamilnadu India 641 024 (e-mail-vadivel.rangasamy@gmail.com)
About-[2]Asst. Professor (RD), Dept. of CSE and IT, Govt. College of Technology, Coimbatore – 641 006

significant decoupling and dynamic binding of components: All components in a system are services, in that they encapsulate behavior and publish a messaging API to other collaborating components on the network. Services are marshaled by applications using service discovery for dynamic binding of collaborations. Web Services reflect a new service-oriented architectural approach, based on the notion of building applications by discovering and orchestrating network-available services, or just-in-time integration of applications.

B. *Semantic description of Web Services*

WSDL, SOAP and UDDI are seen as steps in the right direction but ones that will fail to achieve the goals of improved automation and interoperability, because they rely on a priori standardizations and require humans in the loop. To support automated reasoning, knowledge representations (such as markup languages) will be needed that express both data and rules for reasoning. The ability to dynamically locate and compose web services based on their semantic description will rely on the richness of the description and the robustness of the matching techniques used. Ontology will be used to enable definition and comprehension of meaningful content. These are the concerns of the Semantic Web community. Additionally, agents will be needed to interpret the content and transform user requests into optimized delivered solutions. The Intelligent Brokering Service for Knowledge-Component Reuse on the WWW (IBROW)4can be seen as a forerunner of the Semantic Web. In IBROW problem solving methods (PSMs) and ontologies were the components being configured, the current focus is on WS configuration. PSMs and ontologies when used together are also capable of delivering services. The most significant work that has been done to describe web services has been conducted by the DAML-S coalition. The matching of service providers and service requesters via semantic descriptions of the services are key goals of this work. DAML-S uses the DAML+OIL specification language (which extends the weak semantics of RDF(S)) to define a number of ontologies that can be specifically used to describe web services. DAML-S is built on the AI-based action metaphor where each service is either an atomic/primitive or composite/complex action. Knowledge preconditions and knowledge effects are handled via the inputs and outputs of the web service. The DAML-S coalitions are providing solutions to work with current WS standards. For example, a DAML-S service grounding definition can be mapped to a WSDL definition of the service. A number of approaches to service discovery and compositionthat we discuss in the following sections use or extend the DAML-S web service ontology.

C. *Discovering Web Services*

Discovery involves locating and/or matchmaking against some selection criteria. An earlier AI system, Lark, which involved annotation of agent capabilities to enable them to be located and brokered, clearly solved a problem similar to the discovery of WS by a middle agent. This work has developed into the DAML-S Matchmaker[5]. To support matchmaking a number of filters may be configured by the user to achieve the desired tradeoff between performance and matching quality. These filters include: word frequency comparison, ontology similarity matching, ontology subsumption matching, and constraint matching.

Offer an alternative to sequential searching when matchmaking an agent with a service request. They point out that finding possible partners via matching of service advertisements with requests is not enough. To support runtime interactions we need smarter behavior to handle components that are not quite what was requested and combining several partial components to meet the original request. The solution to overcome sequential searching is the conversion of the concepts into number intervals and the use inheritance hierarchies to determine subclass and equality relations. A generalized search tree is used to handle partial matches.

The feasibility of matchmaking largely depends on the annotation of web services. AI can also be applied to this problem. A number of markup tools have been developed for document markup and these could be applied to the semantic description of WSs. The SHOE Knowledge Annotator [19] uses ontologies to guide knowledge annotation. To produce RDF-based markup, COHSE or AeroDAMLcan be used. These approaches start with descriptions in DAML+OIL and DAML, respectively. These approaches support automatic conversion of markup languages but do not support information extraction or automatic mark-up. OntoMat does support some form of automated extraction of semantics. OntoMat combines the resource with its DAML-S markup. The MnM approach additionally stores the annotations in a knowledge base. Automated markup in MnM is achieved using techniques from knowledge engineering; machine learning and natural language processing have developed a query language that is used to find services.

The solution to finding services is to first describe the service using the process ontology with the assistance of the MIT Process Handbook. The Handbook is large and allows reuse to assist in ontology definition. Next, the ontology is indexed by breaking it down into its components such as attributes, ports, dependencies, subtasks and exceptions. The requester can form a query in the query language that will use the index to find matches.

Clearly AI is already contributing solutions for locating, matchmaking, querying and annotation of WS to facilitate their discovery. Discovery of web services is an important issue as it is a prerequisite to their use. However, the real value of web services lies in their composition.

D. *Composing Web Services*

Web service composition can be simply defined as: —the problem of composing autonomous services to achieve newfunctionality". WS composition is not just analternative to application development but a means ofreducing the application backlog problem because: manyservices are moving online; integration is easier since WSsconform to the HTTP protocol and many independentproviders have related services that need to be combined tosatisfy user

requirements. The rigidity and lack ofintelligence of current solutions has spawned a number ofresearch projects from a number of other research fields.

The work by has arisen from experience in thedistributed systems and networking fields. They havedeveloped the Infrastructure for Composability at Runtimeof Internet Services (ICARIS). They have extended WSDLto develop the Web Services Offerings Language (WSOL).They offer flexibility and adaptability but their approach isvery alternative. Instead of trying to solve the problem ofhow to find services dynamically and combine them, theyfocus on the situation where providers and requestors arealready matched but will at times either make changes totheir services or requests. A service is seen to havenumerous offerings. The functionality will be the same butthe constraints will differ such as authorization rights andQoS. They suggest that a limited number of classes ofservices be offered and described. Then using WSOL they are able to specialize the classes into offerings. Theirsolution offers dynamic switching between offerings. Froma commercial point of view the notion of offerings makessense as customers probably prefer to do business withcompanies they already know and businesses want tomaintain their existing client base.

The work at Hewlett Packard laboratories on *eFlow*is similar in that dynamiccomposition involves automaticadaptation of the configuration at runtime according to therequests of the individual customer. The approach is drivenby the view that composition adds value but to staycompetitive, composition needs to be dynamic as servicesoffered need to adapt to stay competitive. Their goal is toallow dynamic change in service processes with no orminimal human intervention. While they take a businessprocess perspective they point out that web services are less static, predictable or repetitive compared to —traditional"business processes. Similar to most current commercialsolutions, dynamic composition is made possible due to theuse of a central repository that has clients and providersalready attached to it.

The notion of generic solutions that are customizedaccording to user constraints is a recurring theme in much of the literature. Also look at composition as theselection of possible services based on user specifiedcriteria. They offer a centralized, pipes and filtersarchitecture with two main components: a composer (userinterface) and an inference engine (IE) component (whichincludes a knowledge base of known services). Theinference engine is an OWL reasoner and includes axiomsto find all relevant entailments, such as the inheritancerelation between two classes which may not have beenmade explicit. The user identifies some criteria that theservice must satisfy. The matchmaker (IE) selects servicesthat might be suitable based on those criteria and thecomposer shows them to the user. Suitable services forcomposition are ones whose output can be an input to aselected service. While execution of WS may be performedautomatically, the actual task of composition is performedby a human using the services suggested by the system.

Model-based reasoning is a common techniqueemployed in AI approaches. In SWORD entity relationshipmodelling of services is performed by —baseservice modellers" to produce a —worldmodel". Afterbuilding a world model for each service, a compositionmodel is developed that models each service as an action.An expert system is used to automatically determine if thecomposite service can be created with existing services and if so aplan of execution is generated.

In summary, a number of solutions are offered to provide webservice composition. The approaches described in this sectionshow that composition can be assisted through the use of classdefinitions, inheritance hierarchies and model and rule-basedreasoning. In many cases, decision making is left to humans. Theonly automated composition offered is in limited situations wherea central repository is used and the requestor and provider are partof the same system. However, the web is distributed in nature.Intelligent reasoning and collaboration between services is neededto handle this complexity. Agents are capable of both.

E. Agents and Web Services

The autonomous and reasoning capabilities of agents make them well suited for handling cross-organizational decision making. For example, agents can be used to (re)negotiate contracts which would then require: determination of which processes are needed to fulfil the contract; creation of new business processes; and adaptation of existing business processes. Two main agent-oriented approaches exist: use wrappers to make WS behave like agents and; using agents to orchestrate WS.

1) Adding Behaviour to WS via Agents Wrappers

WS are componential, independent, software applications similar to agents. However, agents are also reactive, social and capable of reasoning. If we wish web services to work together, we need to give them social and reasoning capabilities. This can be achieved by wrapping a service in an agent. In the work of, a composition language is used to create an agent wrapper which allows services to collaborate. The created agent has first–order reasoning abilities that have been derived from the DAML-S description of the service. This then allows one agent wrapped service to know what other agent-wrapped services are capable of doing and whether they can assist in the service/agent meeting its goals. Also offer an agent-based wrapper approach to web services. They have developed a tool for creating wrappers so that web sources can be queried in a similar manner to databases. They then use an interactive, hierarchical constraint propagation system to perform integration. As in, the end user interacts via a GUI to manage the orchestration. The Racing project6 offers amediator architecture also using agent wrappers that are structured into a hierarchy. A number of different agent wrappers are supported: user, query translation, query planning, resource wrapper, ontology, matchmaking, and cloning and coordination agents. The use of agent wrappers is a way of allowing multi-agent system technology to be applied to web services

2) Composing Web Services using Agents

The work of combines ideas from the Semantic Web, Knowledge Representation and Agent communities to allow WSs to be composed. Their goal is to —onstruct reusable, high-level generic procedures, and to archive them in shareable (DAML-S) generic-procedures ontologies so that multiple users can access them". In the approach, WSs and user constraints are marked up in DAML-S. A generic task procedure is selected by the user and given to the DAML(-S) enabled agent, who customizes the procedure according to the user specific constraints. The generic procedures are written in an extended version of ConGolog, a situation calculus agent programming language, and executed using a Prolog inference engine. Others provide agent-oriented languages for web service description. Propose an Agent Service Description Language (ASDL) and Agent Service Composition Language (ASCL). ASDL is an extension to WSDL and captures external behaviour via a finite state machine. Their work is based on the argument that composition requires more than description of the data, but also requires a strong representation of actions and processes. A number of approaches are focused on the design of agent systems with web services as the components have developed WARP (Workflow Automation through Agent-based Reflective Processes) that uses the XML and WSDL standards. The goal is automatic configuration and management of low-level services (components). The software engineering development process that has been developed is semi-automatic involving multiple software agents and a human workflow designer. They support visualization of the process based on activity diagrams in UML.

3) (Re-)composition and Adaptable Agents

The ability of agents to adapt according to changes in system requirements and the environment is important to enable dynamic and reactive behaviour.

Agents may be adapted in a number of different ways. The knowledge and facts that an agent uses may be adapted for example the agent may use a client profile that changes according to the clients activities (e.g. this type of adaptation typically involves machine learning, e.g. An agent may also adapt its interface according to the platform on which it is being used (e.g.[brand]. A third type of adaptation, and the type of adaptation we are concerned with, is adaptation of the agent's functionality. There is limited work in this area. Semi-automatic agent creation tools such as AGENTBUILDER, D'AGENTS/ AGENT/TCL, ZEUS and PARADE could possibly be extended to support agent adaptation.

Following the use of compositionality in the major softwareengineering paradigms (e.g. functional programming, object-orientedprogramming, component-based programmingand the Factory design pattern, we have developed an AgentFactory. The approach is based on the use of components, thegeneral agent model (GAM) and the DESIRE formal knowledge levelmodelling and specification frameworkfor multi-agentsystems. Our agent (re-)structuring approach allows an agentto automatically adapt by reusing existing components. Ourapproach is a combination of process-oriented and object-orientedapproaches by treating processes as the 'active' parts of our agent,which are our agent components and classes as the 'passive' partof our agent, which are the data types used in the agentcomponents. We are currently exploring whether DAML-Sdescriptions of web services are adequate for automatedconfiguration of web services by the Agent Factory.the Agent Factory andbased on the notion of design patterns, assists human designers infunctional design, and the configuration of software componentsto fulfil the conceptual design specified by the designers,depending on the agent platform that is to be used. Our approachdoes more: it automates the creation and redesign of both theconceptual and operational design based on the requirements onfunction, behavior and state of an agent. Our use of web servicesas components is a further distinguishing feature.

While not currently working in the WS area, the Adapt agent approach, bring together adaptive workflow and agentresearch. They consider how agents can be used to collaborate toperform a workflow and make workflow more intelligent andhow workflow can be used to organize a set of agents andcoordinate interaction between people and agents.

The reuse of knowledge has also been a widely researchedtopic and the creation of libraries of problem solving methodsand generic task modelsoffer a similar idea to the functionalcomponents in our agent factory. The IBROW project, mentionedearlier, has even more in common with our approach by semi automaticallyconfiguring intelligent problem solvers usingproblem solving methods as building blocks. They use mappingsto act as glue between the components which are modelled asCORBA objects. Unlike our approach, their architecture isrestricted to specific languages and architectures, they onlysupport semi-automation and they do not distinguish betweenconceptual and implementation level designs.

III. Experimental Results

In this section we evaluate the performance of the proposed artificial intelligence to eCommerce web service agent. We have created common web service application to integrate the all web and windows application who want to integrate eCommerce application to their application. Refer Fig 1 – 4 work flow of AI based eCommerce web service.

A. Application Overview

The Order Management System (eCommerce) has been written to provide a common means to create simple orders and process credit card transactions. The first version works only with PayPal's PayFlowProw service but can be updated to work with other online merchant services (e.g. Authorize). When the need to use an alternative provide comes up we'll code the core library accordingly. Any changes here will not affect the way you use the service.

1) Not a User Management System

The system doesn't offer any user management capabilities like sign in. It assumes the calling application knows who the user is let's it take care of any user authentication required. When you're coding your shopping carts you need primary means of identification and is required before you can process any payments.

2) Typical Lifecycle / Process Flow

It's important to understand how the Order Management System (OMS) works so you can make use of the methods in the most efficient way.

The first thing you'll need to do is to create a Processing Session in the OMS. This is done by calling the **GetSessionForKnownUser()** method and passing in the email address of the current user. The OMS will create a session and a shopping cart for the user. It's recommended that you store the ID of the session in your application cookie or in your database so it can be reused. It's not efficient to create a session every time!

To retrieve the shopping cart you simply call the **GetShoppingCart()** method. To add an item to the shopping cart simply call the **AddItemToShoppingCart()** method passing in a properly constructed ShoppingCartItem object. To remove an item from the shopping cart simply call the **RemoveItemFromShoppingCart()** method passing in the item to remove. You can also empty the shopping cart by calling the **EmptyShoppingCart()** method.

3) Ready to Checkout

Once you've populated the shopping cart, authenticated your user you're ready to process the transaction and turn the Shopping Cart into an Order. To do this you must create a **PaymentProcessingKey**. Think of this is a temporary key allowing you to make a credit card transaction. To create one you call the **GeneratePaymentProcessingKet()** method passing in the session. It will configure it with the session and the associated shopping cart ready for processing.

4) Payment Information Page

This page is the one responsible for taking the credit card information and processing the payment through the online payment gateway (e.g. PayFlowPro). The Order summary is displayed at the top of the page so the user can make sure they're purchasing the correct item(s). The next section prompts for the credit card information including the CVV2 security code location on the credit card.

to handle all of this. The Order Management System simply provides the relevant methods to create Processing Sessions, Shopping Carts etc you just need to implement them.

The Order Management System does keep track of "users" (customers) through the use of an email address. This is the

The last section prompts the user for the billing address that's associated with the credit card they're using. If the user is purchasing physical goods they should also populate a shipping address. If the order consists of only electronic items the shipping address can be left blank.

5) Processing the Payment

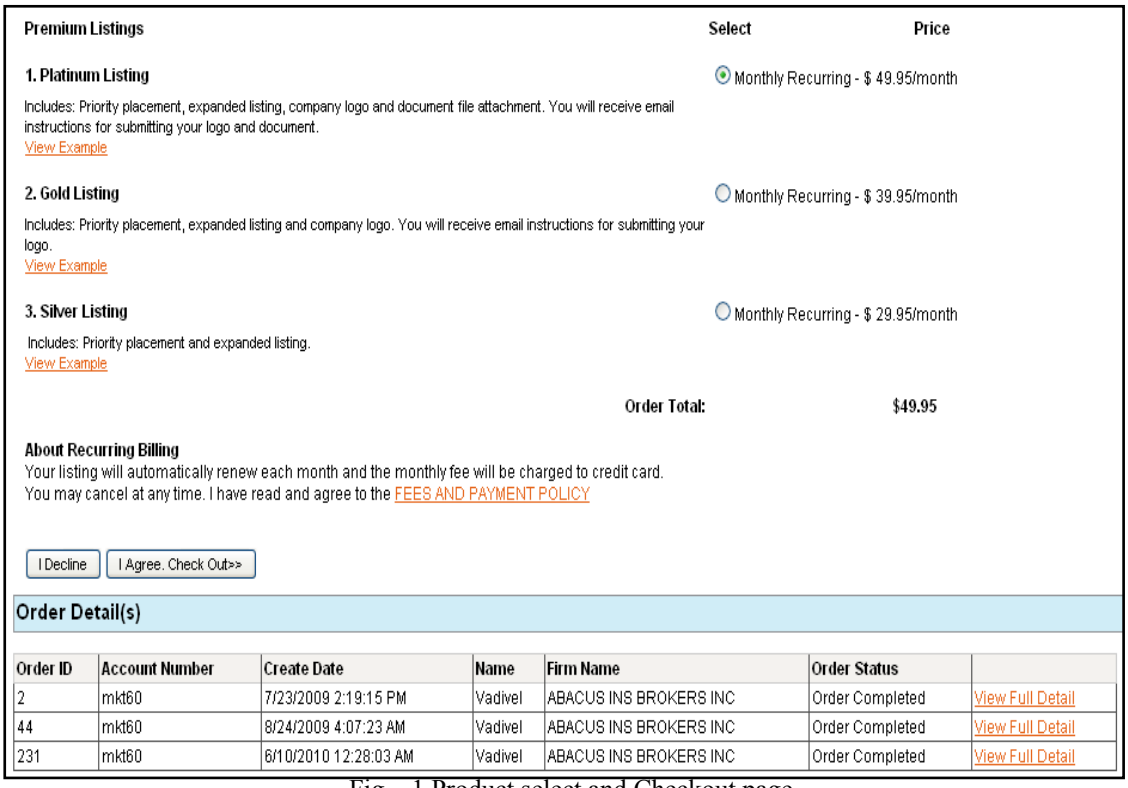
Once the user is happy that all the information has been entered correctly they should click the "Purchase Now" button to initiate the payment transaction. Processing payments is actually using a two step process:

1. The first step is to authorize the payment. The reason we do this is to basically test to see if the payment information is correct and that the payment card will accept the new payment being attempted without actually taking the funds. The reason we do this is to make sure the transaction will succeed. If this step fails we send the user back to the payment information page and display them the error. It basically means that we'll never process an order unless the payment succeeds.
2. The second step is to then retrieve the actual funds allocated during the first authorization step. At this point we're 99.9% confident that the transaction will succeed because the authorization was successful.

After a successful transaction the system performs some cleanup routines and processes the order:

1. Updates the status of the order to Complete
2. Constructs an invoice and sends this to the user
3. Constructs a notification email and sends this to the person setup in the installation configuration
4. Calls the Call-back page defined int the installation configuration. This page is located on calling application and is generally responsible for firing any triggers based on the products that were just purchased. For example it might need to perform an upgrade of a profile or add a new feature.

Once all this is complete the user is sent to the Order Confirmation Page where a summary of the order is presented.



Premium Listings Select Price

1. Platinum Listing Monthly Recurring - $ 49.95/month

Includes: Priority placement, expanded listing, company logo and document file attachment. You will receive email instructions for submitting your logo and document.
View Example

2. Gold Listing Monthly Recurring - $ 39.95/month

Includes: Priority placement, expanded listing and company logo. You will receive email instructions for submitting your logo.
View Example

3. Silver Listing Monthly Recurring - $ 29.95/month

Includes: Priority placement and expanded listing.
View Example

Order Total: $49.95

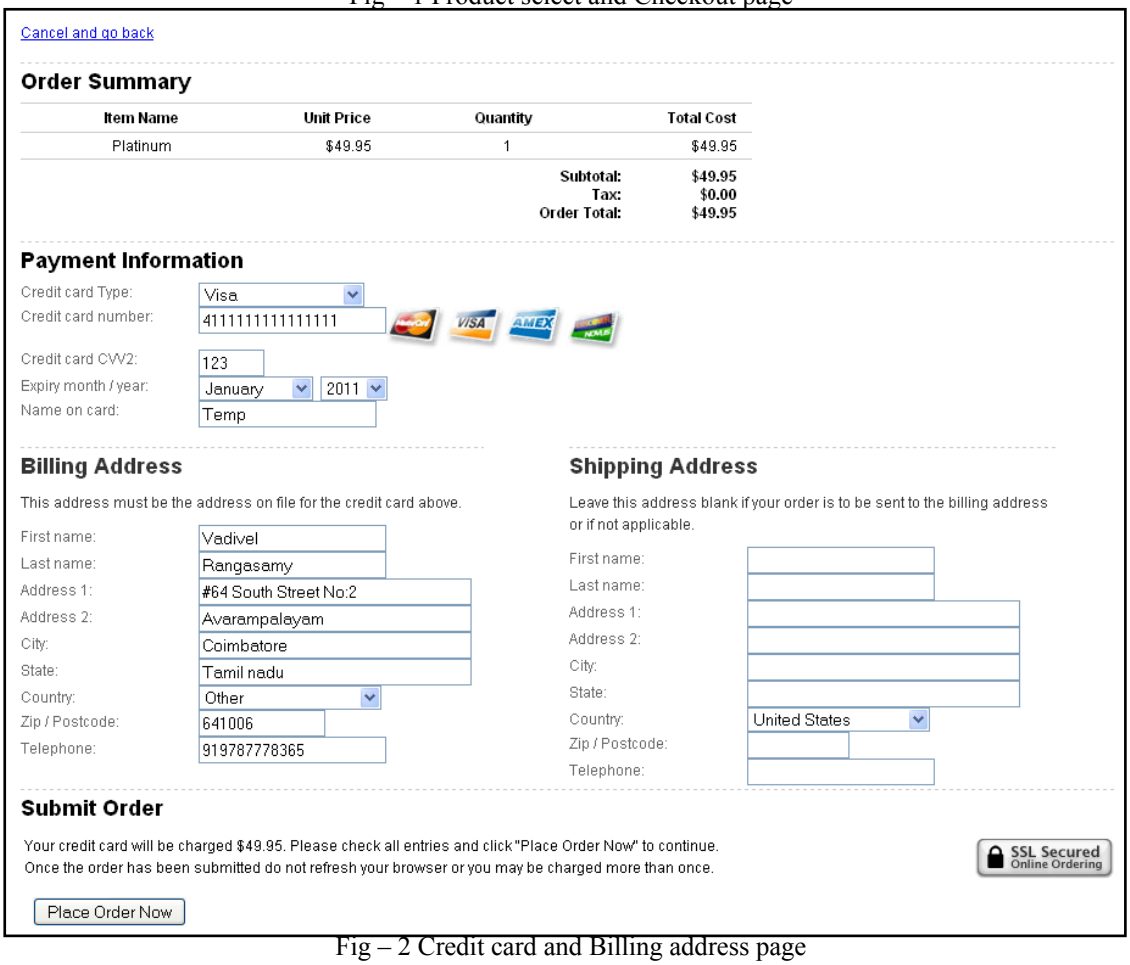
About Recurring Billing
Your listing will automatically renew each month and the monthly fee will be charged to credit card.
You may cancel at any time. I have read and agree to the FEES AND PAYMENT POLICY

I Decline | I Agree. Check Out>>

Order Detail(s)

Order ID	Account Number	Create Date	Name	Firm Name	Order Status	
2	mkt60	7/23/2009 2:19:15 PM	Vadivel	ABACUS INS BROKERS INC	Order Completed	View Full Detail
44	mkt60	8/24/2009 4:07:23 AM	Vadivel	ABACUS INS BROKERS INC	Order Completed	View Full Detail
231	mkt60	6/10/2010 12:28:03 AM	Vadivel	ABACUS INS BROKERS INC	Order Completed	View Full Detail

Fig – 1 Product select and Checkout page



Cancel and go back

Order Summary

Item Name	Unit Price	Quantity	Total Cost
Platinum	$49.95	1	$49.95
		Subtotal:	$49.95
		Tax:	$0.00
		Order Total:	$49.95

Payment Information

Credit card Type: Visa
Credit card number: 4111111111111111
Credit card CVV2: 123
Expiry month / year: January 2011
Name on card: Temp

Billing Address

This address must be the address on file for the credit card above.

First name: Vadivel
Last name: Rangasamy
Address 1: #64 South Street No:2
Address 2: Avarampalayam
City: Coimbatore
State: Tamil nadu
Country: Other
Zip / Postcode: 641006
Telephone: 919787778365

Shipping Address

Leave this address blank if your order is to be sent to the billing address or if not applicable.

First name:
Last name:
Address 1:
Address 2:
City:
State:
Country: United States
Zip / Postcode:
Telephone:

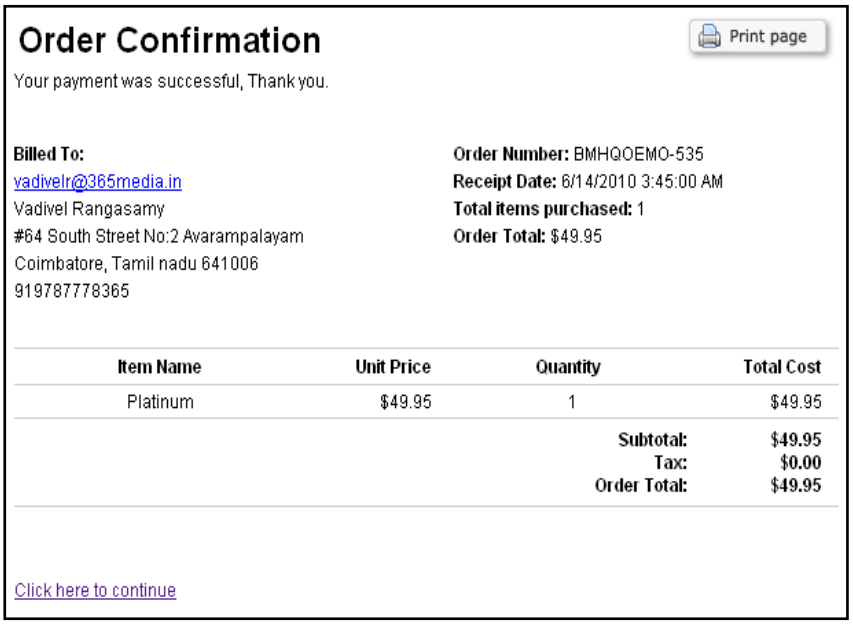
Submit Order

Your credit card will be charged $49.95. Please check all entries and click "Place Order Now" to continue.
Once the order has been submitted do not refresh your browser or you may be charged more than once.

SSL Secured Online Ordering

Place Order Now

Fig – 2 Credit card and Billing address page



Order Confirmation

Print page

Your payment was successful, Thank you.

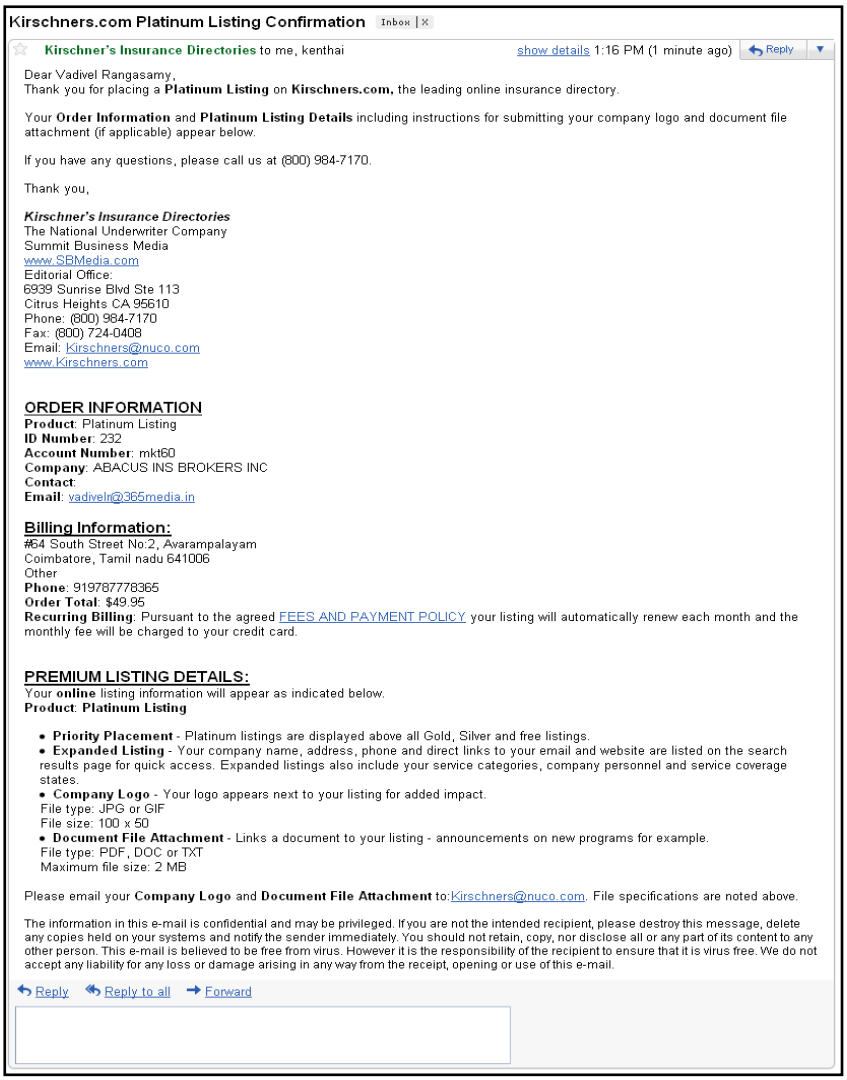
Billed To:
vadivelr@365media.in
Vadivel Rangasamy
#64 South Street No:2 Avarampalayam
Coimbatore, Tamil nadu 641006
919787778365

Order Number: BMHQOEMO-535
Receipt Date: 6/14/2010 3:45:00 AM
Total items purchased: 1
Order Total: $49.95

Item Name	Unit Price	Quantity	Total Cost
Platinum	$49.95	1	$49.95
		Subtotal:	**$49.95**
		Tax:	**$0.00**
		Order Total:	**$49.95**

Click here to continue

Fig – 3 Order confirmation page



Kirschners.com Platinum Listing Confirmation Inbox | ×

Kirschner's Insurance Directories to me, kenthai show details 1:16 PM (1 minute ago) Reply

Dear Vadivel Rangasamy,
Thank you for placing a **Platinum Listing** on **Kirschners.com,** the leading online insurance directory.

Your **Order Information** and **Platinum Listing Details** including instructions for submitting your company logo and document file attachment (if applicable) appear below.

If you have any questions, please call us at (800) 984-7170.

Thank you,

Kirschner's Insurance Directories
The National Underwriter Company
Summit Business Media
www.SBMedia.com
Editorial Office:
6939 Sunrise Blvd Ste 113
Citrus Heights CA 95610
Phone: (800) 984-7170
Fax: (800) 724-0408
Email: Kirschners@nuco.com
www.Kirschners.com

ORDER INFORMATION
Product: Platinum Listing
ID Number: 232
Account Number: mkt60
Company: ABACUS INS BROKERS INC
Contact:
Email: vadivelr@365media.in

Billing Information:
#64 South Street No:2, Avarampalayam
Coimbatore, Tamil nadu 641006
Other
Phone: 919787778365
Order Total: $49.95
Recurring Billing: Pursuant to the agreed FEES AND PAYMENT POLICY your listing will automatically renew each month and the monthly fee will be charged to your credit card.

PREMIUM LISTING DETAILS:
Your **online** listing information will appear as indicated below.
Product: **Platinum Listing**

- **Priority Placement** - Platinum listings are displayed above all Gold, Silver and free listings.
- **Expanded Listing** - Your company name, address, phone and direct links to your email and website are listed on the search results page for quick access. Expanded listings also include your service categories, company personnel and service coverage states.
- **Company Logo** - Your logo appears next to your listing for added impact.
  File type: JPG or GIF
  File size: 100 x 50
- **Document File Attachment** - Links a document to your listing - announcements on new programs for example.
  File type: PDF, DOC or TXT
  Maximum file size: 2 MB

Please email your **Company Logo** and **Document File Attachment** to:Kirschners@nuco.com. File specifications are noted above.

The information in this e-mail is confidential and may be privileged. If you are not the intended recipient, please destroy this message, delete any copies held on your systems and notify the sender immediately. You should not retain, copy, nor disclose all or any part of its content to any other person. This e-mail is believed to be free from virus. However it is the responsibility of the recipient to ensure that it is virus free. We do not accept any liability for any loss or damage arising in any way from the receipt, opening or use of this e-mail.

Reply Reply to all Forward

Fig – 4 Order confirmation email

IV. CONCLUSION

The work of the Semantic Web community to provide semantic description of web services will play a key role in enabling agents to automatically compose web services. In this eCommerce application has implemented in embedded windows and web applications with cross-platforms and it's successfully interoperability of applications. A standard communication between the agents is clearly defined and very less amount of data loss.

Existing agent platforms may need to be adapted to handle the specific requirements of web services. But in this system with no trouble to adaptable all kind of computer applications and tested in real world applications. The RETSINA functional architecture includes four basic types of agents: interface, task, information and middle agents who communicate via a special agent communication language. Each of these agents includes four reusable modules: communication and coordination, planning, scheduling and monitoring. The middle agent plays a critical role in matching providers with requesters and is offered as a solution to the heterogeneous nature of agents over the web.

In future work will continue on artificial intelligence to natural language technology research will assist discovery of web services and agents will play an important role in using web services to satisfy user requests.

V. REFERENCE

1) Boutrous Saab, C.; Coulibaly, D.; Haddad, S.; Melliti, T.; Moreaux, P.; Rampacek, S. –An Integrated Framework for Web Services Orchestration", Idea Group Publishing, 2009
2) Raymond Y. K. Lau, "Towards a web services and intelligent agents-based negotiation system for B2B eCommerce", Elsevier Science Publishers B. V.,October 2007
3) Sabou, M., Richards, D. and van splunter, S. An experience report on using DAML-S , Workshop on E-Services and the Semantic Web, Budapest, Hungary, May, 2003
4) B.Y. Wu and K.M. Chao. Spanning Trees and Optimization Problems. CRC Press, New York, USA, 2009.
5) Xia Yang Zhang Qiang Xu Zhao Zhang Ling, "Research on Distributed E-Commerce System Architecture", IEEE ,August 2007
6) Lixiao Geng Zhenxiang Zeng Yajing Jiang, "Research on E-Commerce personalized service based on intelligent agent technology", IEEE, November 2008
7) T. Finin, J. Mayeld, C. Fink, A. Joshi, and R. S. Cost. Information retrieval and the semantic web,January 2004.
8) Scott Short, "Building XML Web Services for the Microsoft .NET Platform", Microsoft Press, 2002
9) James Murty, "Programming Amazon Web Services", O'Reilly Media, March 2008
10) http://www.daml.org/ontologies/, daml ontology library, by daml.
11) http://www.schemaweb.info/, schema web.
12) http://www.semwebcentral.org/, semwebcentral, by infoether and bbn.
13) http://www.w3.org/2004/ontaria/, ontaria, by w3c.
14) https://subversion.365media.com/mediawiki/index.php /ECommerce

Acute Cystitis and Acute Nephritis Prediction Using Machine Learning Techniques

R. Kowsalya[1] G. Sasikala[2] J. Sangeetha Priya[3]

GJCST Classification
I.2.6,K.3.2,J.3

***Abstract*-Urinary System includes kidneys, bladder, ureters and urethra. This is the major system involves electrolyte balance of the body and filters the blood and excretes the waste products in the form urine. Even the small disturbance in the renal function will step in a disasters manifestation. Among them we are considering the two diseases that affect the system are acute cystitis and acute nephritis. This paper presents the implementation of three supervised learning algorithms, ZeroR, J48 and Naive Bayes in WEKA environment. The classification models were trained using the data collected from 120 patients. The trained models were then used for predicting the acute cystitis or acute nephritis of the patients. The prediction accuracy of the classifiers was evaluated using 10-fold cross validation and the results were compared.**

Keywords-Urinary System, Ureters, Urethra, AcuteCystitis, Acute Nephritis, classification, WEKA

I. Introduction

Machine learning is a scientific discipline that is concerned with the design and development ofalgorithms that allow computers to change behavior based on data, such as from sensor data or databases. 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. [1]

A major focus of machine learning research is to automatically learn to recognize complex patterns and make intelligent decisions based on data. Hence, machine learning is closely related to fields such as statistics, probability theory, data mining, pattern recognition, artificial intelligence, adaptive control, and theoretical computer science. The attributes considered for the algorithm comprises temperature of patient , nausea , Lumbar pain, Frequency of micturation (continuous need for urination) , micturition pain, burning sensation during micturition, itch, swelling of urethra outlet. Machine Learning Techniques are effective to classify the data and to improve the predictive accuracy

About-1st R. Kowsalya, Lecturer, GR Govindarajulu School of Applied Computer Technology, PSGR Krishnammal College for Women, Coimbatore.(telephone: 9442013066 email: kowsalya@grgsact.com)
About-2nd G. Sasikala, Lecturer, GR Govindarajulu School of Applied Computer Technology, PSGR Krishnammal College for Women, Coimbatore.(telephone: 98944 13801 email: sasikala@grgsact.com)
About-3rd J. Sangeetha Priya , Lecturer , GR Govindarajulu School of Applied Computer Technology, PSGR Krishnammal College for Women, Coimbatore.(telephone: 99949 10211 email:sangeethapriya@grgsact.com)

II. Motivation

Motivation behind is to apply and analyze three different machine learning algorithm for classification of the urinary system - acute cystitis and acute nephritis. The classification models were trained using the data collected from 120 patients. The trained models were then used for predicting the acute cystitis and acute nephritis of the patients. Data set includes descriptions of hypothetical samples corresponding to 120 patients. It is identified as definitely the patient is affected withInflammation of urinary bladder or Nephritis of renal pelvis origin. [3]

III. Acute Cystitis and Acute Nephritis

Urinary System includes kidneys, bladder, ureters and urethra. This is the major system involves electrolyte balance of the body and filters the blood and excretes the waste products in the form urine. The body has two kidneys located in the lumbar region (back at about the location of the elbows). Each kidney has about 1000 nephrons that act as filter. Each nephron composed of glomeruli and tubules, which works as a filter and an absorber. The blood which carries glucose, electrolytes, and metabolic end products passes through the nephrons that filters and absorb the needed materials for the tissue and excreates the waste products along with the water in the form of urine. The cleaned blood leaves the kidney and travels throughout the body. Thus the kidney places the major role in electrolyte balance. Another elementary function of kidney is secretion of erythropoietin, which maintains the blood pressure.

The bladder is a muscular bag in which urine is stored before being discharged through the urethra. The two ureter from each side of the kidney carries urine from the kidney to the bladder. It can hold between one half to two cups of urine before it needs to be emptied. Everyday about two to five cups of urine pass through the bladder. The urine output is directly proportional to the water intake but it does not hold good in summer season because most of the body water is excreted as sweat.

About 96% of urine is water. It also contains some waste salt and a substance called urea. Urea is made during the breakdown of proteins in liver. Urea is also excreted in sweat. If urea builds up in the body, it is a sign that the kidneys are not working properly. When the kidney fails,the metabolic waste products get accumulatedin the body andlead to the consequent manifestation. For example accumulation of urea may lead on to encephalopathy [4].

Machine Learning Techniques is used to classify the presumptive diagnosis of two diseases ofurinary system.
Acute cystitis, inflammation of the urinary bladder commonly crop up due to the ascending infections by several organisms. It manifests with clinical features of burning micturation, raising temperature, hematuria (passing blood in urine), sudden occurrence of pain in the abdomen region, burning micturition and micturition pain. Symptoms decay usually within several days on proper treatment. However, there is inclination to return. A person with acute cystitis should expect that the illness will turn into protracted form, which also sequlae into hydronephrosis.Acute nephritis, inflammation of the renal parenchyma occurs considerably more often at women than at men. Sudden fever, hematuria, elevated blood pressure, lumbar pain and oliguria are the symptoms of acute cystitis. Quite not infrequently there are nausea and vomiting and spread pains of whole abdomen.

IV. Machine Learning Approach and Algorithm Basis

For analyzing the data and classification of acute cystitis and acute nephritis, the three Machine learning algorithms ZeroR, J48 Pruned tree and Naive Bayes classifier were adopted here. Zero-R algorithm is used to predict the majority class in the training data.J48 Pruned tree algorithm is an implementation of the C4.5 decision tree learner. This implementation produces decision tree models. The algorithm uses the greedy technique to bring decision tree for classification. A decision-tree model is built by analyzing training data and the model is used to classify unseen data. J48 generates decision tree, the nodes of which evaluate the existence or significance of individual features.
The Naive Bayes Classifier technique is based on Bayesian theorem and is particularly suited when the dimensionality of the inputs is high. Naïve Bayes classifiers assume that the effect of a variable value on a given class is independent of the values of other variable.
The conditional probability of attribute value given class is computed by figuring out the proportion of instances.Depending on the accurate nature of the probability model, Naive Bayes classifiers can be trained very efficiently in a supervised learning setting.

V. Experimental Setup

The data analysis and classification was carried out using WEKA software environment for machine learning. The WEKA, Open Source, Portable, GUI-based workbench is a collection of state-of-the-art machine learning algorithms and data pre-processing tools [2]. It is designed in flexible manner to try out existing methods on new dataset. In this experiment, the data set collected from UCI Repository of 120 patients with 8 features is selected as the class label. The instances in the dataset are pertaining to the two categories based on the temperature of patient, occurrence of nausea, lumbar pain, urine pushing (continuous need for urination), micturition pain, burning of urethra, itch, swelling of urethra outlet, inflammation of urinary bladder and nephritis of renal pelvis origin. The attributes are labeled as a1, a2, a3, a4, a5, a6, d1, d2. To evaluate the robustness of the classifier, the normal methodology is to perform cross validation on the classifier. In general, ten fold cross validation has been proved to be statistically good enough in evaluating the performance of the classifier. The machine learning techniques is implemented using WEKA tool. The 10-fold cross validation was performed to test the performance of the three models. The prediction accuracy of the models was compared.

VI. Result and Discussion

The results of the experiments are described in Table 1, 2 and 3. The performances of the three models were evaluated based on the three criteria, the prediction accuracy, learning time and error rate and illustrated in Figures 1, 2 and 3.

Table 1. Predictive Performance Of The Classifiers

Classifiers	Zero R	Naive Bayes	J48 Pruned tree
Time taken to build the model (in sec)	0	0	0.02
Correctly Classified Instances	70	120	120
Incorrectly Classified Instances	50	0	0
Prediction Accuracy	58.3333 %	100%	100%

TABLE 2. COMPARISON OF ESTIMATES

Validation	Zero R	Naive Bayes	J48 Pruned tree
Kappa statistic	0	1	1
Mean absolute error	0.4864	0.0602	0
Root mean squared error	0.493	0.1017	0
Relative absolute error	100 %	12.3797 %	0 %
Root relative squared error	100 %	20.6264 %	0 %

Table 3. Comparison Of Evaluation Measures ByClass

Classifier	**TP Rate**	**FP Rate**	**Precision**	**Recall**	**F-measure**	**ROC**	**Class**
Zero R	1	1	0.583	1	0.737	0.5	no
	0	0	0	0	0	0.5	yes
Naïve Bayes	1	0	1	1	1	1	no
	1	0	1	1	1	1	yes
J48 Purned Tree	1	0	1	1	1	1	no
	1	0	1	1	1	1	yes

From the confusion matrix given in Table 4, it is observed that Naive Bayes and J48 Pruned Tree produce relatively good results.

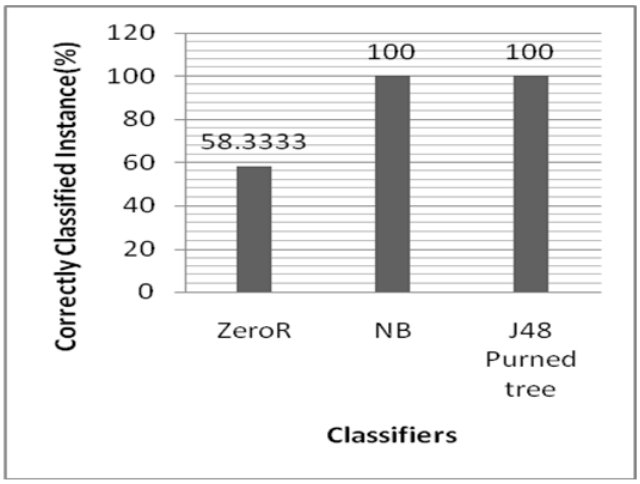
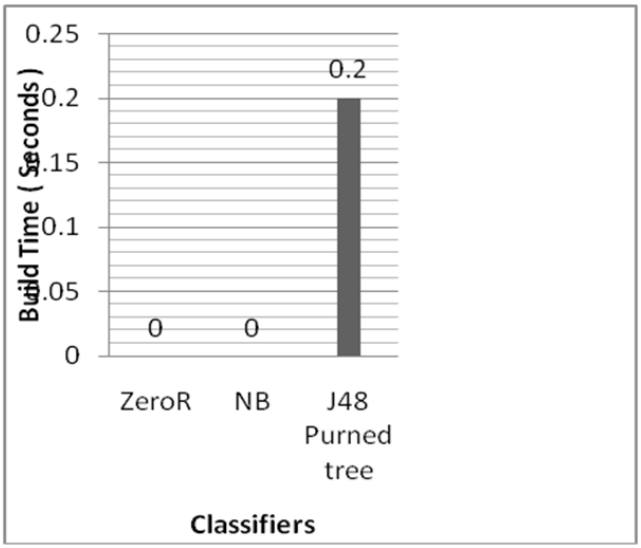


Fig.1. Prediction Accuracy



VII. Conclusion

Classifier systems play a major role in machine learning and knowledge-based systems. In this paper three supervised learning algorithm was implemented using WEKA software. By classifying each attributes to predict the accuracy of each algorithm and test the correctly classified instances of the attribute. The result percentage was compared to identify the algorithm that is well suited to classify the acute cystitis urinary bladder and acute nephritisis. The results indicate that the Naive Bayes classifier outperforms in prediction than ZeroR and J48 Pruned algorithm. Further work can be extended by repeating the experiment with other machine learning algorithms.

Figure 2 illustrates the learning time of the three schemes under consideration. J48 Pruned tree classifier takes moretime to build the model. The Naïve Bayes and ZeroR, the probabilistic classifier tends to learn more rapidly for the given dataset.

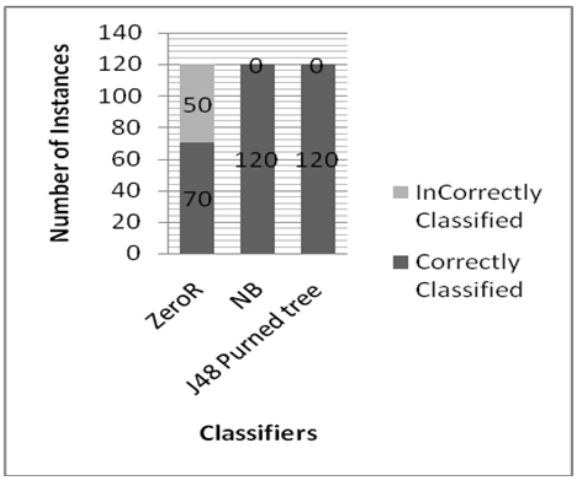


Fig.3. Error Rate

The confusion matrix was used to evaluate the classification error rate. From the confusion matrix given in Table 4, it is observed that Naive Bayes and J48 Pruned tree produce relatively good results but the time taken for the J48 Pruned tree is high when compared to the Naive Bayes.

CLASSIFER	a	b
Zero R	70 0 | a = no	50 0 | b = yes
Naive Bayes	70 0 | a = no	0 50 | b = yes
J48 Purned Tree	70 0 | a = no	0 50 | b = yes

VIII. References

1) Ethem Alpaydin.(2004). Introduction to Machine Learning, MIT Press.
2) Ian H. Witten, Eibe Frank. (2005). Data Mining – Practical MachineLearningToolsandTechniques,2nd Edition, Elsevier.
3) J.Czerniak, H.Zarzycki, (2005) Application of rough sets in the presumptive diagnosis of urinary system diseases, Artificial Intelligence and Security in Computing Systems, ACS'2002 9th International Conference Proceedings, 41-51.
4) Harrison's Principles of Internal Medicine - 17th Ed. (2008), Printed in the United States of America, The McGraw-Hill Companies, Inc.

Analysis of shortest path algorithms

Pawan Jindal[1],Amit Kumar[2],Shishir kumer[3]

GJCST Classification
F.2.1

***Abstract*-Shortest path algorithms have large number ofpractical applications in computer networks to flow the information from one computer to the another computer system in the minimum possible time. Researchers are continuously designing new algorithms to solve the shortest path problems which have less time complexity as well as less space complexity as compared to the existing algorithms. In this paper, analysis of shortest path algorithm is being done and it has been concluded that researchers have got remarkable success in designing better algorithms in the terms of space & time complexity to solve shortest path algorithms.**

General TermsAlgorithms, Theory.

Keywords-Shortest path algorithms.

I. INTRODUCTION

An algorithm is defined as computational procedure which takes a particular input and produces aparticular output. Algorithms are used to solve widerange of problems. If G(V,E) is directed weightedgraph, where V represents the set of vertices ofgraph & E represents the set of edges f graph. |V|represents the total number of vertices in graph & |E|represents the total number of edges in the graph. I nshortest path problems, a directed weighted graph isgiven & the goal is to determine the shortest pathamong vertices. There are many variants of shortestpath problems which are given below. In Singlesource shortest path problems, a graph G(V,E) isbeing given & the goal is to find a shortest pathfrom a given vertex to the remaining vertices of thegraph. In Single destination Shortest path problem,the goal is to determine the shortest path from eachvertex of a graph to a particular destination vertex.In Single pair shortest path problem, a pair ofvertices (u,v) is being given and the goal is to findthe shortest path from vertex u to the vertex v. In allpair shortest path problems, the goal is to determineM a shortest path from u to v for every pair of verticesu & v in the graph G(V,E).

II. COMPARISONS OF ALGORITHMS FOR SHORTEST PATH PROBLEMS

Bellman ford algorithm can be used to solve the single source shortest path problems in which edge weight may be negative. This algorithm returns a Boolean value which indicates whether there is negative weight cycle or not in a particular graph. If there is a negative weight cycle which is reachable from the source vertex, then Bellman Ford algorithm indicates that there is no any solution but if there is negative cycle then the algorithm produces the shortest path from the single source vertex to the remaining vertices. If G(V,E) be the graph, Where V represents the set of vertices & E represents the set of edges, then the timecomplexity for Bellman Ford algorithm is O(|V||E|). Dijikstra algorithm can also be used to solve the single source shortest path problems on a given weighted, directed graph G(V,E) if andonly if all the weights of edges are positive The time complexity of Dijikstra algorithm depends upon the implementation of min priority queue. If the minpriority queue is being implemented by using binary heap, then the time complexity of Dijikstra algorithm is O((V+E)lgv). But if the minpriority queue is being implemented by using Fibonacci Heap, then the time complexity for Dijikstra algorithm is O(VlgV+E). All pair shortest path problems can be solved by Floyd Warshall algorithm within the time complexity of O(V3). But the constraint is that there is no any negative weight cycle in the given graph but the edge may be of negative weight. Johnson‘s algorithm can be used to solve all pair shortest path problems within the time complexity of O(V2lgV+VE) time. If the graph contain negative cycle then Johnson‘s algorithm reports that the graphcontains negative cycle. If the graph does not contain negative cycle then Johnson‘s algorithm returns a particular matrix which shows the shortest distance among vertices. If the lengths of edges of a graph are integers, whose absolute value are bounded by N, then the time complexity of the algorithm which is used to calculate the shortest path from a given source node s to the remaining vertices is O(n05mlg(N)). Researchers are continuously applying their best efforts to design the new algorithms for shortest path problems which have less time complexity as well as less space complexity as compared to the existing algorithms. The time complexity for the shortest path algorithm which is given by Upton et al. [1979] is O(n1.5). Henzinger et al.[1997] designed a new algorithm for single source shortest pat problem which has the time complexity of O(n4/3log2/3 (D)) Where D represents the sum of the absolute value of the length. Fakcharoenphol and Rao[2006] designed a new algorithm for single source shortest pat problem in planar graph which has the time complexity of O(nlog3n) & the space complexity of O(nlogn). Ahuja[1] designed a new algorithm for single source shortest path problem which has the time complexity of O(E+V(lgW)0.5) for graph with positive edge weights where w is the longest weight of any edge in the graph. Thorup[2009] designed a new algorithm for single source

About-[1]Deptt. of Computer Science & Engineering Jaypee Institute of Engineering & Technology, Guna , M.P. India
(e-mail - pawan.jindal@jiet.ac.in)
About-[2]Deptt. of Computer Science & Engineering Jaypee Institute of Engineering & Technology, Guna , M.P. India
(e-mail-amit.kumar@jiet.ac.in)
About-[3]Deptt. of Computer Science & Engineering Jaypee Institute of Engineering & Technology, Guna , M.P. India
(e-mail-amit.kumar@jiet.ac.in)

shortest path problems which has the tiem complexity of O(ElglgV). Thorup[2] also designed a new algorithm for single source shortest path problem for undirected graph which has the time complexity of O(E +V). Researchers are continuously applying best efforts in designing new improved algorithm for computing shortest path. Fredman[3] proves that all pair shortest path problems can be solved by using O(V5/2) comparisons between the sums ofweights of edges and has designed a new algorithm which has the time complexity ofO(V3(lglgV/lgV)1/3)time, which is better than the running time complexity of theFloyd-Warshall algorithm. Suppose O(nw) be the running time of the algorithm for multiplying n × n Matrices. As w < 2.376 . Galil and Margalit [4, 5] and Seidel [6] designed an algorithms that solve the all-pairs shortest paths problem for undirected graphs with the time complexity of (Vw p(V)), where p(V) represents a particular function which is polylogarithmically boundedin v. After then several researchers have extended these results to give algorithms to solve the all-pairs shortest paths problem in undirected graphs in which the weights of are integers in the range {1,2,_ _ _,W}. Shoshan and Zwick [7], designed an algorithm which has the time complexity of O(W Vw p(V W)). Karger, Koller, and Phillips[8] and independently McGeoch[9] have designed a new algorithm for a graph with nonnegative edge weights, which has the time complexity of O(V E*+V2 lg V) where E* represents the set of edges in E that participate insome shortest path. For graph with real edge weights, Yuster[10] designed a new algorithm which achieves subcubic running time with the constraint that the number of weight edges emanating from each vertex is O(n0.338). If n is the total number of vertices then the space complexity of this algorithm is $O(n^2)$. The upper bound of the space complexity matches the lower bound of the space complexity.N The quadratic bound for space complexity for all pair shortest path problems is the major bottleneck for many various large scale applications e.g. in the case of internet, the table size of the order of n*n for answering the given distance queries is much larger than the network itself. The n*n table size is too large to be stored in random access memory. So researchers are applying their best efforts to design the efficient algorithms for the all pair approximate shortest path problems. Approximate shortest distance is different from exact shortest distance between two vertices. It means there is some error in the case of approximate shortest distance between two vertices. This error can be additive(surplus) or multiplicative(stretch). Suppose _(x,y) denotes the actual distance between two vertices x & y in a given graph G(V,E). An algorithm is said to compute all pair approximate (stretch) distance for any given graph G(V,E) if for any pair of vertices x,y∈V, the distance determined by that algorithm isat least $_1$(x,y) and at most t $_1$(x,y). Similarly an algorithm is said to be compute distance with surplus c if the distance determined by the algorithm isatleast $_1$ (x,y) and at most c+ $_1$(x,y). An algorithm which compute all pair t approximate distance wit t<2 can be easily used to calculate the Boolean matrix multiplication of two n*n boolean matrices. So computing all pair distances with stretch less than two is as hard as the multiplication of two Boolean matrices[11]. Any kind of data structure which is capable of answering a distance query with stretch less than three in constant time must occupy at least $_2(n^2)$space in the worst case. Zwick and Cohen[12] designed a new O(n1.5m0.5) algorithm to calculate all pair 2 approximate distances. They also designed an algorithm to compute all pair 7/3 approximate distances which has the time complexity of O(n7/3) & the space complexity of $_(n^2)$for stretch less than three. Zwick and Cohen[12] also designed an algorithm for stretch equal to three which has the time complexity of $O(n^2lg(n))$ & the spacecomplexity of $_(n^2)$. Thorup and Zwick[13] designeda new algorithm for all pair approximate shortestpaths. They showed that for an integer c>=2, anundirected weighted graph can be preprocessed inthe expected tiem of O(cmn1/k) to design a datastructure of size O(cn1+1/c). This particular datastructure is being capable of answering any distancequery with a stretch 2c-1 within the time complexityof O(c). In fact this particular data structure is notstoring all pair approximate distances explicitly,even then it can give the answer of any distancequery in the constant time. So this particular datastructure is known as approximate distance oracle.Algorithm for all pair three stretch distances as given by Thorup & Zwick[13] is preferred when space has to be optimized as compared to the time. Algorithm for all pair three stretch distance as given by Cohen & Zwick[12] is being preferred when time has to be optimized as compared to the space. Aingworth et al. [14] designed a simple algorithm for finding all distances with an additive error of at most 2 in an unweighted, undirected graph which has the time complexity of O(n5/2). Dor et al.[11] extended the algorithms as given by Aingworth et al. [14] and designed a new algorithm to determine the distances with surplus 2(k−1) for all pair of vertices in unweighted undirected graphs which has the time complexity of O(kn2-1/km1/kpolylogn). There are also large number of algorithms for all pair approximate shortest paths in unweighted graphs which have multiplicative error as well as additive error simultaneously and which achieve close to quadratic running time.

III. Conclusion

In this paper, analysis of shortest path algorithm is being done and it has been concluded that researchers have got remarkable success in designing better algorithms in the terms of space & time complexity to solve shortest path algorithms.

IV. References

1) Ravindra K. Ahuja, Kurt Mehlhorn, James B.Orlin, and Robert E. Tarjan. Faster algorithms forthe shortest path problem. Journal of the ACM,37:213–223, 1990.
2) Mikkel Thorup. Undirected single-sourceshortest paths with positive integer weights in linear time. Journal of the ACM, 46(3):362–394, 1999.

3) Michael L. Fredman. New bounds on thecomplexity of the shortest path problem. SIAMJournal on Computing, 5(1):83–89, 1976.
4) Zvi Galil and Oded Margalit. All pairs shortest distances for graphs with small integer length edges.Information and Computation, 134(2):103–139,1997.
5) Zvi Galil and Oded Margalit. All pairs shortestpaths for graphs with small integer length edges. Journal of Computer and System Sciences,54(2):243–254, 1997.
6) Raimund Seidel. On the all-pairs-shortest-pathproblem in unweighted undirected graphs. Journal ofComputer and System Sciences, 51(3):400–403,1995.
7) Avi Shoshan and Uri Zwick. All pairs shortestpaths in undirected graphs with integer weights. InProceedings of the 40th Annual Symposium onFoundations of Computer Science, pages 605–614,1999.
8) David R. Karger, Daphne Koller, and Steven J.Phillips. Finding the hidden path: time bounds forall-pairs shortest paths. SIAM Journal onComputing, 22(6):1199–1217, 1993.
9) C. C. McGeoch. All pairs shortest paths and the essential subgraph. Algorithmica, 13(5):426–441,1995.
10) Raphael Yuster. Efficient algorithms on sets ofpermutations, dominance, and real-weighted apsp. InProceedings of 20th Annual ACM-SIAMSymposium on Discrete Algorithms,pages 950–957,2009.
11) Dorit Dor, Shay Halperin, and Uri Zwick. Allpairs almost shortest paths. Siam Journal onComputing, 29:1740–1759, 2000.
12) Edith Cohen and Uri Zwick. All-pairs smallstretch paths. Journal of Algorithms, 38:335– M353,2001.
13) Mikkel Thorup and Uri Zwick. Approximatedistance oracles. Journal of Association ofComputing Machinery, 52:1–24, 2005.
14) Donald Aingworth, Chandra Chekuri, PiotrIndyk, and Rajeev Motwani. Fast estimation ofdiameter and shortest paths(without matrixmultiplication). SIAM Journal onComputing,28:1167–1181, 1999.

Allowing and Stroring Of Authorized And Unauthorized Database User According To the Policy Verfication and Validation of Distributed Firewall under the Specialzed Database

P.Senthilkumar[1] Dr.S.Arumugam[2]

GJCST Classification
C.2.0,D.4.6,H.2.7

***Abstract*-The society has grown to rely on internet services, and the number of internet client increases every day. As more users are connected to the network, millions a user to do their damage becomes very great and lucrative. In conventional firewall rely on topology restrictions and controlled network entry points to enforce packet filtering. In this paper, I propose method of multiple firewall concepts and maintain the database for both the authorized and unauthorized entry details based on security policy to enforce the static and dynamic packet filtering. This technique is implemented in software tool called distributed firewall policy advisor and specialized database (SDB).**

Keywords-Firewall, Distributed Firewall, policy Language, policy verification,Policy validation, SpecializedDatabase (SDB), Distributed firewall policy Advisor (DFPA).

I. INTRODUCTION FIREWALL

The firewall is a computer hardware or software that limits access to a computer over a network or from an outside source. The firewall is used to create security check points at the boundaries of private network.

A firewall is placed at an entry point where a private computer network is connected to the outside Internet. It intercepts all the packets that are exchanged between the private computer network and the rest of the Internet and examines the IP, TCP and UDP headers of each intercepted packet and decides whether to accept the packet or to discard the packet network of a large enterprise has tens or even hundreds of firewalls. These firewalls are placed at the entry points of the private In the case of companies, if when ordinary firewall is used everyone were given the same class policy. By the implementation of the distributed firewall, multiple firewall concepts each and every one with in the organization was provided with separate access policy, separate authentication.

A. General Techniques

General techniques that firewall use to control access and enforce the site‘s security policy.

Service control

It determines the types of internet service that can be accessed inbound (or) outbound.

Direction control

It determines the direction in which particular service request may be indicate and allowed to flow through the firewall.

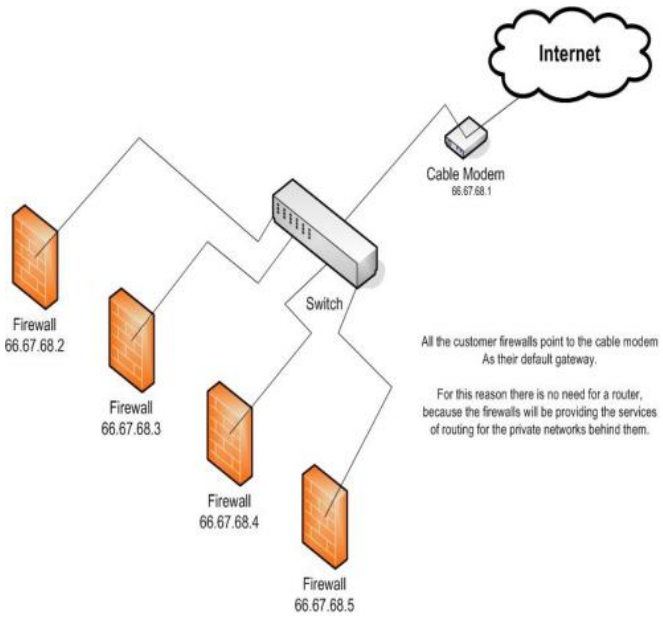
User control

Control access to service according to which user is attempting to access it.

Behavioral control

Controls now particular services are used.

B. Firewall diagram



II. THE DISTRIBUTED FIREWALL

A distributed firewall uses a central policy, but pushes enforcement towards the edges. That is, the policy defines what connectivity, inbound and outbound, is permitted; this policy is distributed to all endpoints, which enforce it. In the full-blown version, endpoints are characterized by their IPsec identity, typically in the form of a certificate. Rather than relying on the topological notions of —inside” and —outside”, as is done by a traditional firewall, a distributed firewall assigns certain rights to whichever machines own the private keys corresponding to certain public keys. [1][2]

To implement a distributed firewall for allowing and storing authorized and unauthorized specialized database, we need a

About-[1]Lecturer-CSE, Nandha College of Technology (e-mail psenthilnandha@rediffmail.com)
About-[2]Chief Executive Officer Nandha Engineering College Erode

strong verification and validation security policy language that can describe which connections are acceptable.

Basic Working of Distributed Firewalls

Distributed firewalls are the following three components.

1. A language for expressing policies and resolving requests. In their simplest form, policies in a distributed firewall are functionally equivalent to packet filtering rules. However, it is desirable to use an extensible system (so other types of applications and security checks can be specified and enforced in the future). The language and resolution mechanism should also support credentials, for delegation of rights and authentication purposes [4].
2. A mechanism for safely distributing security policies. This may be the IPsec key management protocol when possible, or some other protocol. The integrity of the policies transferred must be guaranteed, either through the communication protocol or as part of the policy object description (e.g., they may be digitally signed).
3. A mechanism that applies the security policy to incoming packets or connections, providing the enforcement part.Distributed firewalls rest on three notions:

- A policy language that states what sort of connections are permitted or prohibited.[3]
- Any of a number of system management tools, such as Microsoft's SMS or ASD, and
- IPSEC, the network-level encryption mechanism for TCP/IP.

Components of a distributed firewall

- A central management system for designing the policies.
- Policy Distribution.
- Host end Implementation.

Central management system

Central Management, a component of distributed firewalls, makes it practical to secure enterprise-wide servers, desktops, laptops, and workstations. Central management provides greater control and efficiency and it decreases the maintenance costs of managing global security installations. This feature addresses the need to maximize network security resources by enabling policies to be centrally configured, deployed, monitored, and updated. From a single workstation, distributed firewalls can be scanned to understand the current operating policy and to determine if updating is required

Policy distribution

The policy distribution scheme should guarantee the integrity of the policy during transfer. The distribution of the policy can be different and varies with the implementation. It can be either directly pushed to end systems, or pulled when necessary. [3]

Host-end implementation

The security policies transmitted from the central management server have to be implemented by the host. The host end part of the Distributed Firewall does provide any administrative control for the network administrator to control the implementation of policies. The host allows traffic based on the security rules it has implemented.

Policy Language

Policy is enforced by each individual host that participates in a distributed firewall. The distributed firewall administrator--who is no longer necessarily the "local" administrator, since we are no longer constrained by by topology--defines the security policy in terms of host identifiers. The resulting policy (probably, though not necessarily, compiled to some convenient internal format) is then shipped out, much like any other change. This policy file is consulted before processing incoming or outgoing messages, to verify their compliance. It is most natural to think of this happening at the network or transport layers, but policies and enforcement can equally well apply to the application layer.

Policy verification

Policy verification is enforced by the each incoming packet as per the user specified policy and also verifies the inconsistencies.

Policy validation

A policy validation method normally validating firewall security policy in a heterogeneous network with a complex layout.The policy validation system is concerned; there are two distinct kinds of failure.[13]

*Host Failure*Any of the network hosts can fail at any time. Generally, a host failure may be difficult to distinguish from a network failure, from the perspective of the rest of the network. Recovery, however, is somewhat different. The things that a node needs to keep track of—subordinates, ongoing tests, previous test results, commands, the node ID, and so forth—do not change very quickly, and it is possibleto store all of that information on disk.. [13]

*Network Failure*The network can obviously fail at any time, or can simply not be laid out as expected. From this perspective, any command that gets lost can be viewed as an unexpected, failed network test. These can be ignored or reported to the root Manager in some way, as they indicate a network status that to the distributed firewall administrator. [13]

Distributed firewall policy Advisor (DFPA)

In DFPA techniques are simplifies the management of filtering rules and also maintain the strong security of firewalls.

The filtering rules and policy rules are implemented using java programming language in a software tool called DFPA. [6][7]

Specialized Database (SDB)

Database is nothing but collection of interrelated data and a set of programs to access those data. The collection of data usually referred to as Database (DB).

The current research propose the specialized database for allowing and storing of authorized and unauthorized database user according to policy verification and validation scheme.

III. THREAT COMPARISON

Distributed firewalls have both strengths and weaknesses when compared to conventional firewalls. By far the biggest difference is their reliance on topology. If your topology does not permit reliance on traditional firewall techniques. [5]

A. Service Exposure and Port Scanning

Both types of firewalls are excellent at rejecting connection requests for inappropriate services. Conventional firewalls drop the requests at the border; distributed firewalls do so at the host. A more interesting question is what is noticed by the host attempting to connect. Today, such packets are typically discarded, with no notification. A distributed firewall may choose to discard the packet, under the assumption that its legal peers know to use IPSEC; alternatively, it may instead send back a response requesting that the connection be authenticated, which in turn gives notice of the existence of the host.

Firewalls built on pure packet filters cannot reject some "stealth scans" very well. One technique, for example, uses fragmented packets that can pass through unexamined because the port numbers aren't present in the first fragment. A distributed firewall will reassemble the packet and then reject it.

B. Application-level Proxies

Some services require an application-level proxy. Conventional firewalls often have an edge here; the filtering code is complex and not generally available on host platforms. As noted, a hybrid technique can often be used to overcome this disadvantage.

In some cases, of course, application-level controls can avoid the problem entirely. If the security administrator can configure all Web browsers to reject ActiveX, there is no need to filter incoming HTML via a proxy.

In other cases, a suitably sophisticated IPSEC implementation will suffice. For example, there may be no need to use a proxy that scans outbound FTP control messages for PORT commands, if the kernel will permit an application that has opened an outbound connection to receive inbound connections. This is more or less what such a proxy would do.

C. Intrusion Detection

Many firewalls detect attempted intrusions. If that functionality is to be provided by a distributed firewall, each individual host has to notice probes and forward them to some central location for processing and correlation.

The former problem is not hard; many hosts already log such attempts. One can make a good case that such detection should be done in any event. Collection is more problematic, especially at times of poor connectivity to the central site. There is also the risk of co-ordinated attacks in effect causing a denial of service attack against the central machine.

D. Insider Attacks

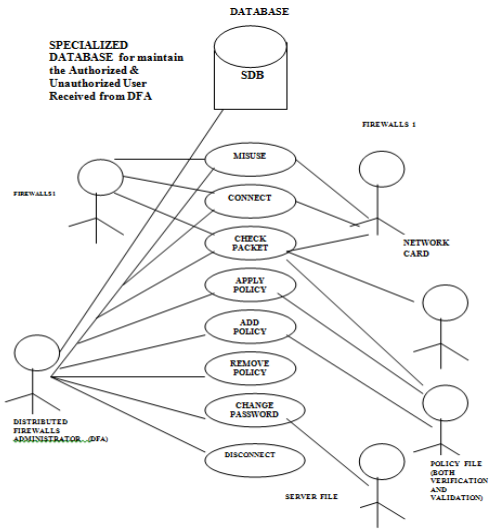
At first glance, the biggest weakness of distributed firewalls is their greater susceptibility to lack of cooperation by users. Although there are technical measures that can be taken, as discussed earlier, these are limited in their ability to cope with serious misbehavior. That said, we assert that this problem is not a real differentiator. Even conventional firewalls are easily subverted by an uncooperative insider. In other words, an insider who wishes to violate firewall policy, the firewall administrator filter that packet.

On the other hand, distributed firewalls can reduce the threat of actual attacks by insiders, simply by making it easier to set up smaller groups of users. Thus, one can restrict access to a file server to only those users who need it, rather than letting anyone inside the company pound on it.

IV. IMPLEMENTAION TECHNIQUES

A. Use case diagram

A use case is an interaction between users and a system; it captures the goal of the users and the responsibility of the system to its users. The current research in our implementation techniques diagrammatic representation as follows



It is an initiative way of describing the behavior of a system by viewing the interaction between the system and its environment.

List of actors in the distributed firewall

- Add policy
- Remove policy
- Apply policy
- Connect
- Disconnect
- Change password

- Misuse
- Check packets

Add policy
The distributed firewall administrator adds the policy to the firewall, which is stored in the temporary file.
Remove policy
The distributed firewall administrator removes the policy from the firewall, which is stored in the temporary file.
Apply policy
The distributed Firewall administrator updates the policy of the firewall from the temporary file.
Connect
Distributedfirewall administrator to connect the system.
Successful case
Distributedfirewall administrator makes a request control from the firewall, the control is granted.
Failure case
Firewall administrator makes a request to the firewall, as there is no firewall request gets timeout.
Disconnect
Distributedfirewall administrator change to the new password by giving the old password and the new password.
Misuse
Firewall gives the blocked details to the firewall administrator which is stored in the misuse file and that can be viewed by the firewall administrator.
Check packet
Firewall checks the packets as per theuser the policy.

V. Related Work

Current research on distributed firewall for authorized and unauthorized database user according to the policy verification and validation mainly focus the following.

1) Maintaining the database for both authorized and unauthorized (ie.collecting the information from distributed firewall administrator).
2) Verifying and validating the security policy in the networks.
3) The testing and validating firewalls regularly.
4) Identify the Static and dynamic vulnerability analysis.
5) Strong Authentication and Authorization for each firewalls.

VI. Conclusion

The main objective of this research is to implement a authorized and unauthorized database user according to the policy verification and validation of distributed firewall under the specialized database(SDB).In distributed firewall environment in order to keep track of some certain actions in the first stage (Create, Read, Update, Delete) that are performed on the policy rule set. Then distributed firewall concept is explained and the comparison of two firewall designs is presented in terms of their performance in network security. The next stage is to give the details of distributed firewall environment for which the proposed the maintain specialized database is designed. Such an application will be very helpful in network security management in protecting the consistency among the overall security policy. The data provided by the application can be used to implement more advanced tools like distributed firewall policy advisor tools(DFPA).

VII. References

1) G.Yan, S. Chen, and S. Eidenbenz. Dynamic balancing of packet filtering workloads on distributed firewalls. Technical Report LA-UR- 07-3281, Los Alamos National Laboratory, 2007.
2) L.Yuan, J. Mai, Z. Su, H. Chen, C. Chuah, and P. Mohapatra. Fireman A toolkit for firewall modeling and analysis. In Proceedings of IEEE Symposium on Security and Privacy, May 2006.
3) E.Al-Shaer, H. Hamed, R. Boutaba, and M. Hasan. Conflict classification and analysis of distributed firewallpolicies. IEEE JSAC, 23(10), October 2005.
4) M.Blaze, J.Feigenbaum, J.Loandis and A.Keroymtis.The role of Trust management in Distributed systems security.In Secure Internet programming [20], pages 185-20.
5) Frank Swiderski and Window Snyder. Threat Modeling. Microsoft Press, 2004.
6) E.Al-Shaer and H. Hamed. ―Firewall Policy Advisor for Anomaly Detection and Rule Editing.‖ IEEE/IFIP Integrated Management Conference (IM‘2003), March 2003.
7) E.Al-Shaer and H. Hamed. ―Design and Implementation of Firewall Policy Advisor Tools.‖ DePaul CTI Technical Report, CTI-TR-02-006, August 2002.
8) D. Chapman and E. Zwicky. Building Internet Firewalls, Second Edition, Orielly & Associates Inc., 2000.
9) D. Eppstein and S. Muthukrishnan. ―Internet Packet Filter Management and Rectangle Geometry.‖ Proceedings of 12th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA), January 2001.
10) A. Mayer, A. Wool and E. Ziskind. ―Fang: A Firewall Analysis Engine.‖ Proceedings of 2000 IEEE Symposium on Security and Privacy, May 2000.
11) S.Ioannidis, A. D. Keromytis, S. M. Bellovin and J. M. Smith, ―Implementing a Distributed Firewall‖, ACM Conference on Computer and Communications Security, Athens, Greece, November 2000.
12) S. M. Bellovin, ―Distributed Firewall‖, ;login: magazine, Special issue on Security, November 1999.
13) Kyle Wheeler. Distributed firewall policy validation, December 7, 2004

Towards Secure Design Choices for Implementing Graphical Passwords

GJCST Classification
D.4.6,K.6.5

Machha.Narender[1] M.Y.Babu[2] M.Mohan Rao[3]

***Abstract*-Access to computer systems is most often based on the use ofalphanumeric passwords. However, users have difficultyremembering a password that is long and randomappearing.Instead, they create short, simple, and insecurepasswords. Graphical passwords have been designed to tryto make passwords more memorable and easier for people touse and, therefore, more secure. Using a graphicalpassword, users click on images rather than typealphanumeric characters.. In this paper we describe theDAS(Draw-A-Secret) scheme, its security characteristics,and the empirical study we carried out comparing DAS toalphanumeric passwords. In the empirical study participantslearned either an alphanumeric or graphical password andsubsequently carried out three longitudinal trials to inputtheir passwords over a period of five weeks. The results showthat the graphical group took longer and made more errorsin learning the password, but that the difference was largelya consequence of just a few graphical participants who haddifficulty learning to use graphical passwords. In thelongitudinal trials the two groups performed similarly onmemory of their password, but the graphical group tookmore time to input a password.**

I. Introduction

Until recently computer andnetwork, security hasbeen formulated as a technical problem.However, it is now widely recognized that mostsecurity mechanisms cannot succeed withouttaking into account the user (Patrick, Long, &Flinn, 2003).. A key area in security research isauthentication, the determination of whether auser should be allowed access to a given systemor resource. Traditionally, alphanumericpasswords have been used for authentication, butthey are known to have security and usabilityproblems. Today other methods, includinggraphical passwords, are possible alternatives.This paper reports on research aimed to design anew kind of graphical password system,empirically test its usability, and compare it toalphanumeric passwords. The significance of thisresearch is the provision of a flexible graphicalpassword system with extensive human factorsdata to support it.We refer to the security and usability problemsassociated with alphanumeric passwords as "thepassword problem" (Wiedenbeck, Waters,Birget, Broditskiy & Memon, 2005). Theproblem arises because passwords are expectedto comply with two fundamentally conflictingrequirements:

1) Passwords should be easy to remember, and the user authentication protocol should beexecutable quickly and easily by humans.
2) Passwords should be secure, i.e., they should look random and should be hard to guess; they should be changed frequently, and should be different on different accounts of the same user; they should not be written down or stored in plain text.

This problem has led to innovations to improvepasswords. One innovation is graphicalpasswords, i.e., passwords that are based onimages rather than alphanumeric strings. The basic idea is that using images will lead togreater memorability and decrease the tendencyto choose insecure passwords. This, in turn,should increase overall password security.Several graphical password systems, described in the next section, have been developed and someHCI evaluation has been done.

II. Background on Passwords

A. Problems with Alphanumeric Passwords

The password problem arises largely from limitations of humans' long-term memory (LTM). Once a password has been chosen and learned the user must be able to recall it to log in. But, people regularly forget their passwords. Decay and interference explain why people forget their passwords. Items in memory may compete with a password and prevent its accurate recall (Wixted, 2004). If a password is not used frequently it will be even more susceptible to forgetting. A further complication is that users have many passwords for computers, networks, and web sites. The large number of passwords increases interference and is likely to lead to forgetting or confusing passwords. Users typically cope with the password problem by decreasing their memory load at the expense of security. First, they write down their passwords (Adams & Sasse, 1999). Second, when they have multiple passwords, they use one password for all systems or trivial variations of a single password. In terms of security, a password should consist of a string of 8 or more random characters, including upper and lower case alphabetic characters, digits, and special characters. A random password does not have meaningful content and must be memorized by rote, but rote learning is a weak way of remembering (Rundus, 1971). As a result, users are known to ignore the recommendations on password choice. Two recent surveys have shown that users choose short, simple passwords that are easily guessable, for example, "password," personal names of family members, names of pets, and dictionary words (Sasse et al., 2001; Brown, Bracken, Zoccoli, & Douglas, 2004). To users the

About-[1]Assistant Professor ,HITS College of Engineering.
(e-mail-machha.narender@gmail.com)
About-[2]Assistant Professor,Aurora Engineering College
(e-mail- mannavababu@gmail.com)
About-[3]Assistant Professor Tirumala Engg College
(e-mail-mohanrao19@yahoo.com)

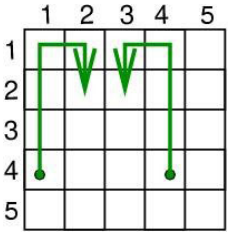
most important issue is having a password that can be remembered reliably and input quickly. They are unlikely to give priority to security over their immediate need to get on with their real work.

B. Why Graphical Passwords?

Graphical passwords were originally described by Blonder (1996). In his description of the concept an image would appear on the screen, and the user would click on a few chosen regions of it. If the correct regions were clicked in, the user would be authenticated. Memory of passwords and efficiency of their input are two key human factors criteria. Memorability has two aspects: (1) how the user chooses andencodes the password and (2) what task the user does when later retrieving the password. In a graphical password system, a user needs to choose memorable locations in an image. Choosing memorable locations depends on the nature of the image itself and the specific sequence of click locations. To support memorability, images should have semantically meaningful content because meaning for arbitrary things is poor (Norman, 1988). This suggests that jumbled or abstract images will be less memorable than concrete, real-world scenes. LTM does not store a replica of the image itself, but rather a meaningful interpretation (Mandler & Ritchey, 1977). To retrieve the locations a user will be dependent on the encoding used while learning. A poor encoding will hurt retrieval by failing to distinguish similar objects. Depending on the graphical password system, at retrieval time users will be presented with either a recognition task or a cued recall task. In a graphical password system based on recognition, the user has to be able only to recognize previously seen images, making a binary choice of whether the image is known or not known. Recognition is an easier memory task than pure, unaided recall (Norman, 1988). In our password system we use an intermediary form of recollection between pure recall and recognition, cued recall. Scanning an image to find previously chosen locations in it is cued recall because viewing the image reminds, or cues, users about their click areas. Psychologists haveshown that with both recognition and recalltasks, images are more memorable than words orsentences (Sheperd, 1967; Paivio, Rogers &Smythe, 1972; Standing, 1973). This isencouraging in terms of memory for graphicalpasswords.Efficiency is important in password systemsbecause users want to have quick access tosystems. The time to input a graphical passwordby a highly skilled, automated user can bepredicted by Fitts' Law (1954). The law statesthat the time to point to a target depends on thedistance and size of the target ‐ greater distanceand smaller targets lead result in slowerM performance. Existing evidence suggests thatalphanumeric passwords may be faster to inputthan graphical passwords (Dhamija & Perrig,2000). However, the question remains how bigthe difference may be.

III. Procedure to Implement

Drawing a password on a grid.
Passwords are a series of strokes, separated by ―pen-up" events.
Picture maps to a sequence of (x, y) points (e.g. (1,4), (1, 3), (1,2), (1,1), (2,1), (2,2)).
Strength in temporal order.
Length is the sum of the number of cells in each stroke (excluding pen-ups), e.g. 12 in diagram to right.
Stroke-count is the number of strokes in a password (e.g. 2).



A. Important points

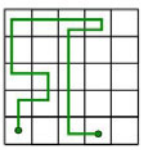
Motivation: Gain understanding of how certain parameters we call password complexity properties affect the security of graphical passwords (to aid in better design choices, password rules, and mnemonics).
We identify a set of complexity properties based on a set of pattern complexity factors from Attneave [1].
We refer to passwords that minimize their complexity properties to be probable passwords, belonging to the probable space.

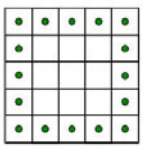
B. Results

We identified a complexity property with a significant impact on the password space: strokecount, X.Larger impact than other complexity properties.Evidence users will choose low X (e.g. 4).We look at ways to increase security of graphicalpassword implementations in light of theseresults.
The graphical password scheme we examined(DAS). Our definition of graphical passwordcomplexity properties. Results of examiningcomplexity properties in relation to DAS.Methods to increase the DAS password space.Security implications and recommendations.Parameters that we hypothesize would adverselyaffect memorability, which we call complexitypropertiesIn textual passwords, these factorscould be length, and the amount of numbers,special characters, etc

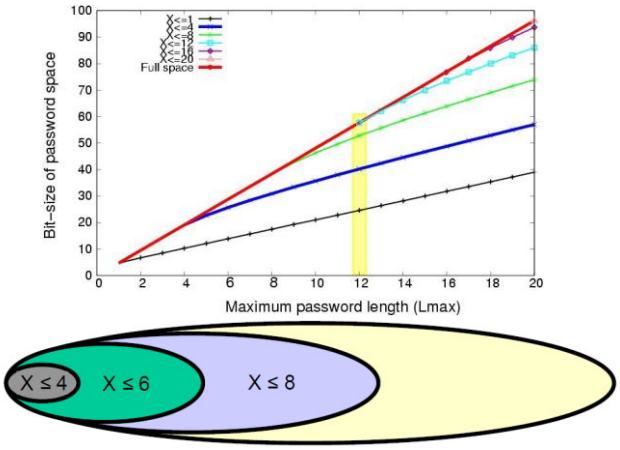
A. Complexity Properties Identified

We identify a set of complexity properties basedon a set of visual pattern complexity factors from Attneave:
Password-length
Stroke-count.
Symmetry (examined in previous work).
Number of turns (likely deserves its own study).



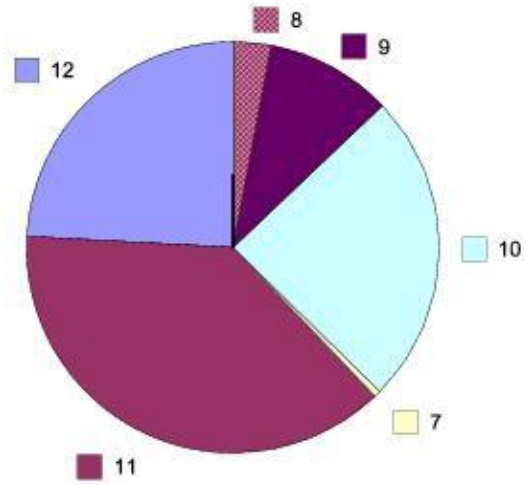


B. Maximum Stroke-count(X) and Length



C. Stroke-count (X)

12 dots (24%), 10 dots, 1 line (38%)
Proportion of password space attributable to passwords consisting of exactly *X* strokes.
Here *Lmax = 12*, on a 5 by 5 grid.
Note that for 6 or fewer strokes, the proportion is so small it is not visible

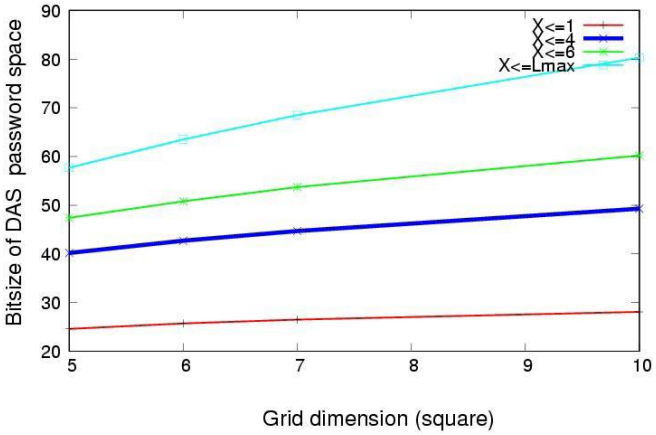


D. Security implications

These values are for Lmax=12, 5 by 5 grid.
X = stroke-count.
Key point is relative times.
We think X ≤ 4 is more representative of what users would choose.

Password set	Time to exhaust(1CPU-32GHz)
Full DAS	541.8 Years
X<6	157.1 Days
X<4	1.1 Days
X<1	1.9 Seconds

E.Increasing DAS's Password Space -Increasing Grid size

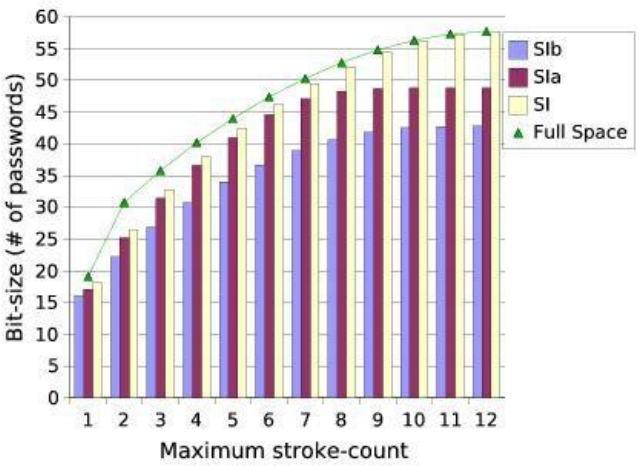


In the above graph, Lmax = 12. Less thanexpected increase achieved, especially when X ≤ Lmax/2.
Password now becomes a combinationof the drawing grid chosen, and thedrawing itself. Amount of extra security achieved depends on selection grid size, and minimum/maximum accepted drawing grid dimensions.e.g. 30 by 30 selection grid, minimum 5, maximum 10 grid dimension provides 16 bits

F. Resulting Recommendations

DAS Password rules:
At least one stroke of length 1.
A stroke-count of at least Lmax/2.
Avoid global symmetry (Usenix Security 2004).
Implementation decisions:
Increasing grid size provides low payback if users choose passwords with a low strokecount (likely).
Grid selection (or related variation) should be implemented to increase the DAS space.

G. Summary of Current Knowledge



IV. Future Work

Alternate encodings for DAS to increase size of password space (and decrease number of passwords "disallowed"). A better understanding of the breakdown of what users have the most difficulty recalling, leading to a more formal definition of complexity properties. Perhaps sacrificing the most difficult to recall parts of DAS to encourage users to choose more strokes would be useful (e.g. direction of strokes). Password set Time to exhaust(1CPU-32GHz) Full DAS 541.8 Years
X<6 157.1 Days X<4 1.1 Days X<1 1.9 Seconds Psychology studies to see how parameters such as stroke-count and temporal order affect memory. Stroke-count is the complexity property with the largest impact on DAS's password space. A more viable attack strategy for DAS passwords than previous work. Secure design choices in implementations: Grid selection instead of simple grid size increase. Password rules: user guidelines and proactive checking.

V. References

1) Adams, A. and Sasse, M.A. (1999). Users are notthe enemy. Communications of the ACM 42, 12,41-46.
2) Birget, J.C., Hong, D., and Memon, N. (2003).Robust discretization, with an application tographical passwords. Cryptology ePrint Archive.http://eprint.iacr.org/2003/168 accessed January17, 2005.
3) Blonder, G.E. (1996). Graphical Passwords.United States Patent 5559961.Boroditsky, M. Passlogix password schemes.http://www.passlogix.com, accessed December2, 2002.
4) Brostoff, S. and Sasse, M.A. (2000). ArePassfaces more usable than passwords: A f ieldtrial investigation. In McDonald S., et al. (Eds.),People and Computers XIV - Usability or Else,Proceedings of HCI 2000, Springer, pp. 405-424.
5) Brown, A.S., Bracken, E., Zoccoli, S. andDouglas, K. (2004). Generating andremembering passwords. Applied CognitivePsychology, 18, 641-651.
6) Dhamija, R. and Perrig, A. (2000). Deja Vu:User study using images for authentication. InNinth Usenix Security Symposium.
7) Fitts, P.M. (1954). The information capacity ofthe human motor system in controlling amplitudeof movement. Journal of ExperimentalPsychology, 47, 381-391.
8) Mandler, J.M. and Ritchey, G.H. (1977). Longtermmemory for pictures. Journal ofExperimental Psychology: Human Learning andMemory, 3, 386-396.
9) Morris, R. and Thompson, K. (1979). Passwordsecurity: A case study. Communications of theACM, 22, 594-597.
10) Norman, D.A. (1988). The Design of Everyday Things. Basic Books, New York.

Cognitive Radio Networks for Wireless Communication

GJCST Classification C.2.1

M.Mohan Rao[1] M.Y.Babu[2] B.Venkata Krishna[3] M.Narender[4]

***Abstract*-The world of wireless communications is nowadays facing a serious problem of spectrum shortage. Such problem is not only due to"real" limitations on the available bandwidth, but also (and mainly) to inefficient policies in spectrum management. Indeed, today's wireless networks are characterized by a fixed spectrum assignment policy, which often leads to waste large spectrum portions due to sporadic utilization by the licensed users. The recentadvances in the field of software defined radios are pushing forward a novel networking paradigm where all the users or part of them access the spectrum in an opportunistic way. Acommon cognitive radio network model features the presence of primary (or licensed) users who have priority access to the bandwidth, whereas secondary users can accessthe bandwidth only when vacated by the primary ones. Moreover, the strict constraint for the secondary users is not to harm primary users' transmissions.**

Keywords-Full Cognitive Radio, Spectrum Sensing Cognitive Radio, Licensed Band Cognitive Radio, Unlicensed Band Cognitive Radio

I. INTRODUCTION

The idea of cognitive radio was first presented officially by Joseph Mitola III in a seminar at KTH, The Royal Institute of Technology, in1998, published later in an article by Mitola andGerald Q. Maguire, Jr in 1999. [1] It was a novelapproach in wireless communications that Mitolalater described as:The point in which wireless personal digitalAssistants (PDAs) and the related networks aresufficiently computationally intelligent aboutradio resources and related computer-tocomputercommunications to detect usercommunications needs as a function of usecontext, and to provide radio resources andwireless services most appropriate to thoseneeds.It was thought of as an ideal goal towards whicha software-defined radio platform should evolve:a fully reconfigurable wireless black box thatautomatically changes its communication variables in response to network and user demands. Regulatory bodies in various countries (including the Federal Communications Commission in the United States and Ofcom in the United Kingdom) found that most of the radio frequency spectrum was inefficiently utilized. For example, cellular network bands are over loaded in most parts of the world, but amateur radio and paging frequencies are not. Independent studies performed in some countries confirmed that observation, and concluded that spectrum utilization depends strongly on time and place. Moreover, fixed spectrum allocation prevents rarely used frequencies (those assigned to specific services) from being used by unlicensed users, even when their transmissions would not interfere at all with the assigned service. This was the reason for allowing unlicensed users to utilize licensed bands whenever it would not cause any interference (by Avoiding them whenever legitimate user presence is sensed). This paradigm for wireless communication is known as cognitive radio.

Depending on the set of parameters taken into account in deciding on transmission and reception changes, and for historical reasons, we can distinguish certain types of cognitive radio. The main two are Full Cognitive Radio("Mitola radio"): in whichevery possible parameter observable by aWireless node or network is taken into account.

Spectrum Sensing Cognitive Radio: in whichonly the radio frequency spectrum is considered.Also, depending on the parts of the spectrumAvailable for cognitive radio, we can distinguish:

Licensed Band Cognitive Radio: in whichcognitive radio is capable of using bandsassigned to licensed users, apart from unlicensed mbands, such as U-NII band or ISM band. TheIEEE 802.22 working group is developing astandard for wireless regional area network(WRAN) which will operate in unused televisionchannels.

Unlicensed Band Cognitive Radio: which canonly utilize unlicensed parts of radio frequencyspectrum. One such system is described in theIEEE 802.15 Task group 2 specification. Whichfocuses on the coexistence of IEEE 802.11 andBluetooth.

II. TECHNOLOGY

Although cognitive radio was initially thought of as a software-defined radio extension (Full Cognitive Radio), most of the research work is currently focusing on Spectrum Sensing Cognitive Radio, particularly in the TV bands. The essential problem of Spectrum Sensing Cognitive Radio is in designing high quality spectrum sensing devices and algorithms for exchanging spectrum sensing data between nodes. It has been shown that a simple energy detector cannot guarantee the accurate detection of signal presence, calling for more sophisticated spectrum sensing techniques and requiring information about spectrum sensing to be exchanged between nodes regularly. Increasing the number of cooperating sensing nodes decreases the probability of

About-[1]Asst.Professor, Tirumala Engg College (e-mail-mohanrao19@yahoo.com)
About-[2]Asst.Professor, Aurora Engg College e-mail-mannavababu@gmail.com
About-[3]Asst.Professor, HITS College of Engg (e-mail-krishna5_bandi@yahoo.com)
About-[4]Asst.Professor, HITS College of Engg (e-mail- machha.narender@gmail.com)

false detection.[12] Filling free radio frequency bands adaptively using OFDMA is a possible approach. Timo A. Weiss and Friedrich K. Jondral of the University of Karlsruhe proposed a Spectrum Pooling system[5] in which free bands sensed by nodes were immediately filled by OFDMA sub bands. Applications of Spectrum Sensing Cognitive Radio include emergency networks and WLAN higher throughput and transmission distance extensions.
Evolution of Cognitive Radio toward Cognitive Networks is under process, in which Cognitive Wireless Mesh Network (e.g. CogMesh) is
considered as one of the enabling candidates aiming at realizing this paradigm change.

III. COGNITIVE SYSTEM

We can exploit the information from physical and link layer to help routing protocol in making various routing decisions. By exploiting radio layer information routing protocol can:
Differentiate routes depending on channel type due to changing propagation characteristics of various radio links. This leads to better QoS when compared to algorithm taking into account number of hops only. Increase nodes connectivity due to wider set of available radio links andavailable longer transmission distances: any cognitive radio node is capable of transmitting with broad set of frequencies, i.e. UNII and USM band [4] or UNII, USM and TV band [1]. By utilizing simple measure that the higher the frequency the shorter the transmission distance, routing algorithm may decide which radio link should be used for specific hop. It has very important implications to emergency network since high frequency signals have bigger problems with thick objects penetration. It is why routing has to utilize the channel information and send high priority packets on highly resilient channels (lower frequency channels).
· Detect faster link failures.
· Perform more efficient multicast due to
increased connectivity.

IV. COGNITIVE RADIO SYSTEM

It is already known that physical and data link layer protocols designed for standard fixed bandwidth ad hoc networks must be changed and adapted to cognitive radio environment to effectively utilize spectrum information. The role of those modified layers of the protocol stack is to manage radio resources in the way appropriate for the nodes in the whole CRN. The remaining layers might be adapted explicitly to cognitive radio networks. Indeed in authors claim that higher layers [above link layer] will implement standard protocols not specific to cognitive radios. However it is valuable to examine in the AAF project the impact of cognitive radio capabilities on routing protocols in ad-hoc networks (application layer is beyond the scope of the AAF project). Especially the project should answer the question what is the benefit for routing protocols from introducing cognitive capabilities to network nodes in terms of:

- Time constraints: route setup time and end-to-end latency;
- Casting issues (multicast, broadcast, geocast and unicast);
- Throughput: overhead value, overall transmitted traffic value, packet loss value;□
- Route quality: route length, route discovery and reconstruction time.

V. MAIN FUNCTIONS

The main functions of Cognitive Radios are:
Spectrum Sensing: detecting the unusedspectrum and sharing it without harmfulinterference with other users, it is an importantrequirement of the Cognitive Radio network to sense spectrum holes, detecting primary users isthe most efficient way to detect spectrum holes.Spectrum sensing techniques can be classifiedinto three categories:
Transmitter detection: cognitive radios musthave the capability to determine if a signal froma primary transmitter is locally present in acertain spectrum, there are several approachesproposed:

- matched filter detection
- energy detection
- cyclostationary feature detection
- Interference based detection

Cooperative detection:refers to spectrumsensing methods where information frommultiple Cognitive radio users are incorporatedfor primary user detection.
Spectrum Management: Capturing the best available spectrum to meet user communication requirements. Cognitive radios should decide on the best spectrum band to meet the Quality of service requirements over all available spectrum bands, therefore spectrum management functions are required for Cognitive radios, these management functions can be classified as:

- Spectrum analysis
- Spectrum decision

Spectrum Mobility: is defined as the process when a cognitive radio user exchanges its frequency of operation. Cognitive radio networks target to use the spectrum in a dynamic manner by allowing the radio terminals to operate in the best available frequency band, maintaining seamless communication requirements during the transition to better spectrum
Spectrum Sharing:providing the fair spectrum scheduling method, one of the major challenges in open spectrum usage is the spectrum sharing. It can be regarded to be similar to generic media access control MAC problems in existing systems

VI. COGNITIVE RADIO (CR) VERSUS INTELLIGENT ANTENNA (IA)

Intelligent antenna (or smart antenna) is antenna technology that uses spatial beam forming and spatial coding to cancel interference; however, it requires intelligent multiple or cooperative antenna array. On the other hand, cognitive radio (CR) allows user terminals to sense whether a portion of the spectrum is being used or not, so as to share the spectrum among neighbor users. The following table compares the different points between two advanced

approaches for the future wireless systems: Cognitive radio (CR) vs. Intelligent antenna (IA).

Point	Cognitive radio (CR)	Intelligent antenna (IA)
Principal goal	Open Spectrum Sharing	Ambient Spatial Reuse
Interference processing	Avoidance by spectrum sensing	Cancellation by spatial pre/post-coding
Key cost	Spectrum sensing and multi-band RF	Multiple or cooperative antenna arrays
Challenging algorithm	Spectrum management tech	Intelligent spatial beam forming/coding tech
Applied techniques	Cognitive Software Radio	Generalized Dirty-Paper and Wyner-Ziv coding
Basement approach	Orthogonal modulation	Cellular based smaller cell
Competitive technology	Ultra wideband for the higher band utilization	Multi-sectoring (3, 6, 9, so on) for higher spatial reuse
Summary	Cognitive spectrum sharing technology	Intelligent spectrum reuse technology

Intelligent antenna (IA) is antenna technology which exploits electronic intelligence to enhance the performance of radio communication systems, as well as being used to enhance the performance of free band systems. For instance, IA-based multiple antenna terminals enable to communicate multiple radio links simultaneously up to the number of embedded multiple antennas.

Dirty paper coding (DPC)-pre-cancels the knowninterference signal at the transmitterwithout the additional transmit power regardlessof knowing the interference at the receiver,which can be used to optimize cognitive wireless network channels.

VII. Security

One of the factors which should be considered during design process of CRN emergency network is security of the network infrastructure and security of transmitted information. Without proper network security terrorists responsible for the disaster would beable to eavesdrop emergency information and utilize it for future attacks. Moreover the network elements due to their poor security could become a target of attack itself. Because cognitive radio constitute a new approach for building wireless networks it simultaneously opens a door for new methods of attacks on their physical structure. Below we outline some of the possible methods of attacks on CRN and ways of prevention:

Licensed user emulation attack: Because cognitive radios cannot be completely sure whether a licensed spectrum is free and available for transmission they simply defer from licensed bands and utilize other non-licensed parts of the band if they are not sure if it is really free.Suppose that attacker knows in which specific area CRN works. Knowing which licensed bands CRN might use attacker can simply transmit signal in the licensed band emulating real transmission and thus limiting overall CRN capacity. Until now wedon't know any method of prevention against this attack.

*Common control channel jamming:*One of the possible solutions for common control channel deployment is the UWB. In this case, potential attacker can simply transmit periodical pulses which have the same spectrum as common control channel of CRN but with higher power than legitimate users. Throughout jamming of just one channel attacker blocks the possibility of communication between all CR nodes. This is the reason for building sophisticated UWB transmission methods for control channels utilizing UWB. It has to be underlined that a need for special care of control channel is the same for any type of approach (dedicated channel, channel hopping etc.).

Attacks on spectrum managers: We cannot allow having one central spectrum manager responsible for assigning frequency bands for nodes (see paragraph 2.3) because it constitutes a single point of attack. Whenever the spectrum manager is not available for CR nodes the communication process becomes impossible. That is why information about spectrum availability should be as distributed and replicated as possible. This constraint is in line with the requirement for more accurate measurements of spectrum availability. One of the preventing ways for this attack is to use specific pilot channel in each license band. It would inform secondary users about the reservation of the nodes.

Eavesdropping:Usually in the infrastructure-based corporate WLAN it was assumed that signal will not leavebuilding due to his short distance and will be limited to eavesdropping and sniffing. However cognitive radios are allowed to work in the bands lower than UNII and ISM. This means that they can perform longer transmission distances with the same powers. It also allows for easy physical data collection from locations far distanced from CRN location where attackers invisible to emergency services. This yields a need for strong data encryption at the physical level. Frequent leaving and joining the emergency network must be preceded by authentication process. It is open for discussion which layer should be responsible for this step. Currently the most possible approach is that application layer will perform all the necessary authentication procedures. Moreover the entire WEP infrastructure should be the basis for authentication procedures in CRNs.

VIII. Conclusion

The rapidly changing radio environment, more radio channels to utilize, number of parameters to choose during decisions taken by MAC and routing protocols, etc. makes design of CRNs very challenging. In this deliverable we

have outlined some specific parameters and constraints which have to be taken into consideration while designing protocols for layers above PHY. Many protocols have the same designrequirements (like robustness, no clocksynchronization or localizing capabilities)which simplify design by small fraction.Moreover we can state that UWB as aCommon control channel might become agood solution for realizing certain functionsoutlined in this document. We also outlinethat cooperation between physical and linklayer is essential for accurate operation of CRN. We have to emphasize that newrequirements might occur during designprocess so this document will be constantlyupdated.

IX. References

1) IEEE Xplore - Login J. Mitola III and G. Q. Maguire, Jr., "Cognitive radio: making software radios more personal," IEEE Personal Communications Magazine, vol. 6, nr. 4, pp. 13-18, Aug. 1999
2) S.Haykin,"Cognitive Radio: Brain-empowered Wireless Communications", IEEE Journal on Selected Areas of Communications, vol. 23, nr. 2, pp. 201-220, Feb. 2005
3) Carl, Stevenson; G. Chouinard, Zhongding Lei, Wendong Hu, S. Shellhammer & W. Caldwell (2009-01). "IEEE 802.22: The First Cognitive Radio Wireless Regional Area Networks (WRANs)
4) Natasha Devroye, Patrick Mitran and V. Tarokh, Limits on Communication in a Cognitive Radio Channel," IEEE Communications Magazine, pp. 44-49, June 2006.
5) Chlamtac, M. Conti, J. J. -N. Liu, "Mobile Ad-hoc networking: imperatives and challenges". Ad- Hoc Networks, vol. 1, no. 1, pp. 13-64. July 2003
6) *Pei, M. Gerla, X. Hong, "LANMAR: Landmark Routing for Large Scale Wireless Ad Hoc Networks with Group Mobility", IEEE/ACM MobiHOC, 2000.*
7) W.-H. Liao, Y.-C. Tseng, J.-P. Sheu, "GRID: A Fully Location-Aware Routing Protocol for Mobile Ad-Hoc Networks", Telecommunication Systems (18), 2001
8) YuanYuan Wang —Medium Access Control Protocol for Cognitive Radio Network", M.S. thesis, TU Delft 2005.

Dynamic Discoverability and Automatic Configuration Using Trustworthy Computing on the Web

GJCST Classification
H.5.3.H.3.5

Maccha.Narender[1] M.Y.Babu[2] M.Mohan Rao[3]

***Abstract*-While many technologies that make use of computing haveproven themselves extremely reliable and trustworthy-computers helped transport people to the moon and back,they control critical aircraft systems for millions of flightsevery year, and they move trillions of dollars around theglobe daily—they generally haven't reached the point wherepeople are willing to entrust them with their lives, implicitlyor explicitly. Many people are reluctant to entrust today'scomputer systems with their personal information, such asfinancial and medical records, because they are increasinglyconcerned about the security and reliability of these systems,which they view as posing significant societal risk. Ifcomputing is to become truly ubiquitous—and fulfill theimmense promise of technology—we will have to make thecomputing ecosystem sufficiently trustworthy that peopledon't worry about its fallibility or unreliability the way theydo today.**

I. Introduction

Trust is a broad concept, and making something trustworthy requires a social infrastructure as well as solid engineering. All systems fail from time to time; the legal and commercial practices within which they're embedded can compensate for the fact that no technology will ever be perfect. Hence this is not only a struggle to make software trustworthy; because computers have to some extent already lost people's trust, we will have to overcome a legacy of machines that fail, software that fails, and systems that fail. We will have to persuade people that the systems, the software, the services, the people, and the companies have all, collectively, achieved a new level of availability, dependability, and confidentiality. We will have to overcome the distrust that people now feel for computers. The Trustworthy Computing Initiative is a label for awhole range of advances that have to be made for people to be as comfortable using devices powered by computers and software as they are today using a device that is powered by electricity. It may take us ten to fifteen years to get there, both as an industry and as a society. This is a "sea change" not only in the way we write and deliver software, but also in the wayour society views computing generally. There areimmediate problems to be solved, andfundamental open research questions. There are Actions that individuals and companies can andshould take, but there are also problems that canonly be solved collectively by consortia, researchcommunities, nations, and the world as a whole.

About-[1]Asst.Professor, HITS College of Engg
(e-mail- machha.narender@gmail.com)
About-[2]Asst.Professor, Aurora Engg College
e-mail-mannavababu@gmail.com
About-[3]Asst.Professor, Tirumala Engg College
(e-mail-mohanrao19@yahoo.com)

II. Trustworthy Computing

Computing devices and information services will only be truly pervasive when they are so dependable that we can just forget about them. In other words, at a time where computers are starting to find their way into just about every aspect of our life, we need to be able to trust them. Yet the way we build computers, and the way that we now build services around those computers, hasn't really changed that much in the last 30 or 40 years. It will need to.

III. A Framework for Trustworthy Computing

We failed to find an existing taxonomy that could provide a framework for discussing Trustworthy Computing. There is no shortage of trust initiatives, but the focus of each is narrow. For example, there are treatments of trust in ecommerce transactions and trust between authentication systems, and analyses of public perceptions of computing, but a truly effective approach needs to integrate engineering, policy, and user attitudes. Even just on the engineering side, our scope is broader than, say, the SysTrust/SAS70 models, which deal purely with large online systems. First, there are the machines themselves. They need to be reliable enough that we can embed them in all kinds of devices−in other words, they shouldn't fail more frequently than other similarly important technologies in our lives. Then there's the software that operates those machines: do people trust it to be equally reliable? And finally there are the service components, which are also largely software-dependent. This is a particularly complicated problem, because today we have to build dependability into an end-to-end, richly interconnected (and sometimes federated) system. Since trust is a complex concept, it is helpful to analyze the objective of Trustworthy Computing from a number of different perspectives. We define three dimensions with which to describe different perspectives on trust: Goals, Means, and Execution.

IV. Goals

The Goals consider trust from the user's point ofview. The key questions are: Is the technologythere when I need it? Does it keep myconfidential information safe? Does it do

whatit's supposed to do? And do the people who ownand operate the business that provides it alwaysdo the right thing? These are the goals that anyTrustworthy Computing has to meet:

Goals	The basis for a customer's decision to trust a system
Security	The customer can expect that systems are resilient to attack, and that the confidentiality, integrity, and availability of the system and its data are protected.
Privacy	The customer is able to control data about themselves, and those using such data adhere to fair information principles
Reliability	The customer can depend on the product to fulfill its functions when required to do so.
Business Integrity	The vendor of a product behaves in a responsive and responsible manner.

V. Means

Once the Goals are in place, we can look at the problem from the industry's point of view. Means are the business and engineering considerations that are employed to meet the Goals; they are the nuts and bolts of a trustworthy service. Whereas the Goals are largely oriented towards the end-user, the Means are inwardly facing, intra-company considerations. Think of the Goals as what is delivered, and the Means as how.

VI. Execution

Execution is the way an organization conducts its operations to deliver the components required for Trustworthy Computing. There are three aspects to this: Intents, Implementation, and Evidence. Intents are the corporate and legislative guidance that sets requirements for the design, implementation, and support of the product.

Implementation is the business process that operationalizes the Intents. Evidence is the mechanism by which we verify that the Implementation has delivered on the Intent. This problem can only be tackled by working on two parallel tracks. The first track is the immediate problems−what people read and worry about every day. We need to address known current problems and mitigate currently known weaknesses. This is also a way to learn about the more fundamental problems. We need to be as well-informed as we can about what is really going on and what we can and cannot fix within the constraints of the current systems. The computer industry needs to identify and solve the most critical challenges, and fold the solutions in an incremental way into the huge legacy systems that have been built. There will be long technological replacement cycle during which the critical infrastructure systems that society depends on are gradually upgraded to a new and improved status. If these systems already exist, people are not just going to throw them out the.

window and start over from scratch. So we have to identify critical infrastructure and systems weaknesses and upgrade them on a high-priority basis, and ensure that new infrastructures are built on sound principles.

Means	The business and engineering considerations that enable a system supplier to deliver on the Goals
Secure by Design, Secure by Default, Secure in Deployment	Steps have been taken to protect the confidentiality, integrity, and availability of data and systems at every phase of the software development process —from design, to delivery, to maintenance.
Fair Information Principles	End-user data is never collected and shared with people or organizations without the consent of the individual. Privacy is respected when information is collected, stored, and used consistent with Fair Information Practices.
Availability	The system is present and ready for use as required.
Manageability	The system is easy to install and manage, relative to its size and complexity. (Scalability, efficiency and cost-effectiveness are considered to be part of manageability.)
Accuracy	The system performs its functions correctly. Results of calculations are free from error, and data is protected from loss or corruption.
Usability	The software is easy to use and suitable to the user's needs.
Responsiveness	The company accepts responsibility for problems, and takes action to correct them. Help is provided to customers in planning for, installing and operating the product.
Transparency	The company is open in its dealings with customers. Its motives are clear, it keeps its word, and customers know where they stand in a transaction or interaction with the company.

VII. Fundamental Problems Policy

Society is only now coming to grips with the fact that it is critically dependent on computers. The computer industry must find the appropriate balance between the need for a regulatory regime and the impulses of an industry that has grown up unregulated and relying upon de facto standards. Many contemporary infrastructure reliability problems are really policy issues. The poor coverage and service of US cellular service providers is due in part to the FCC's policy of not granting nationwide licenses. These policy questions often cross national borders, as
illustrated by the struggle to establish global standards for third-generation cellular technologies. Existing users of spectrum (often the military) occupy different bands in different countries, and resist giving them up, making it difficult to find common spectrum worldwide.

VIII. Processing Complexity

We are seeing the advent of mega-scale computing systems built out of loose affiliations of services, machines, and application software. The emergent (and very different) behavior of such systems is a growing long-term risk. An architecture built on diversity is robust, but it also operates on the edge of chaos. This holds true in all very-large-scale systems, from naturalsystems like the weather to human-made systemslike markets and the power grid. All the previousmega-scale systems that we've built−the power
grid, the telephone systems−have experiencedunpredicted emergent behavior. That is why in1965 the power grid failed and rippled down thewhole East Coast of the United States, and that'swhy whole cities occasionally drop off the
telephone network when somebody implementsa bug fix on a single switch. The complexity ofthe system has outstripped the ability of any oneperson−or any single entity−to understand allof the interactions.Incredibly secure and trustworthy computersystems exist today, but they are largelyindependent, single-purpose systems that aremeticulously engineered and then isolated. Wereally don't know what's going to happen as wedynamically stitch together billions−perhapseven trillions−of intelligent and interdependentdevices that span many different types and
generations of software and architectures.As the power of computers increase, in bothstorage and computational capacity, the absolutescale, and complexity of the attendant softwaregoes up accordingly. This manifests itself inmany ways, ranging from how you administerthese machines to how you know when they arebroken, how you repair them, and how you addmore capability. All these aspects ultimately playinto whether people perceive the system as
trustworthy.

IX. Machine-to-Machine Processes

The Web Services model is characterized bycomputing at the edge of the network. Peer-topeerapplications will be the rule, and there willbe distributed processing and storage. An administrative regime for such a system requiressophisticated machine-to-machine processes.Data will be self-describing. Machines will beloosely coupled, self-configuring, and self organizing. They will manage themselves to conform to policy set at the center.Web applications will have to be designed tooperate in an asynchronous world. In the PCparadigm, a machine knows where itsperipherals are; the associations have beenestablished (by the user or by software) at somepoint in the past. When something disrupts thatsynchronicity, the software sometimes simplyhangs or dies. Improved plug-and-play devicesupport in Windows XP and "hot-pluggable"architectures such as USB and IEEE 1394 point
the way toward a truly "asynchronous" PC, butthese dependencies do still exist at times. On theWeb, however, devices come and go, and latencyis highly variable. Robust Web architecturesneed dynamic discoverability and automaticconfiguration. If you accept the idea thateverything is loosely coupled and asynchronous,you introduce even more opportunities forfailure. For every potential interaction, you haveto entertain the idea that it won't actually occur,because the Web is only a "best-effort"mechanism−if you click and get no result, youclick again. Every computing system thereforehas to be redesigned to recover from failedinteractions.

X. Identity

Questions of identity are sometimes raised in thecontext of Trustworthy Computing. Identity isnot explicitly called out in the framework,because a user does not expect a computersystem to generate their identity. However, useridentity is a core concept against which servicesare provided. Assertions of identity (that is,authentication) need to be robust, so that takingactions that depend on identity (that is,authorization) can be done reliably. Hence, usersexpect their identities to be safe from unwanteduse.
Identity is difficult to define in general, butparticularly so in the digital realm. We use theworking definition that identity is the persistent,collective aspects of a set of distinguishing
characteristics by which a person (or thing) isrecognizable or known. Identity is diffuse andcontext-dependent because these aspect"snippets" are stored all over the place in digital,physical, and emotional form. Some of thisidentity is "owned" by the user, but a lot of it isconferred by others, either legally (for example,by governments or companies) or as informalsocial recognition.
Many elements of Trustworthy Computing systems impinge on identity. Users worry about the privacy of computer systems in part because they realize that seemingly unrelated aspects of their identity can be reassembled more easily when the snippets are in digital form. This is bestn evidenced by growing public fear of credit-card fraud and identity theft as a result of the relative transparency and anonymity of the Internet versus offline transactions, even though both crimes are equally possible in the physical world. Users expect that information about themselves, including those aspects that make up identity, are not disclosed in unapproved ways.

XI. People

It's already challenging to manage extremelylarge networks of computers, and it's just gettingharder. The immensity of this challenge has beenmasked by the fact that up to this point we havegenerally hired professionals to manage large systems. The shortcomings of the machines, thenetworks, the administration, the tools, and theapplications themselves are often mitigated bytalented systems managers working hard tocompensate for the fact that these componentsdon't always work as expected or desired.Many of the system failures that get a lot of attention happen because of system complexity. People make an administrator error, fail to install a patch, or configure a firewall incorrectly, and a simple failure cascades into a catastrophic one. There is a very strong dependency on human operators doing the right thing, day in and dayout.

There are already too few knowledgeable administrators, and we're losing ground. Worse, the needs of administration are evolving beyond professional IT managers. On the one hand we are at the point where even the best operators struggle: systems are changing too rapidly for people to comprehend. On the other, the bulk of computers will eventually end up in nonmanaged environments that people own, carry around with them, or have in their car or their house. We therefore need to make it easier for people to get the right thing to happen consistently with minimal human intervention. We must aim towards a point where decision-makers can set policy and have it deployed to thousands of machines without significant ongoing effort in writing programs, pulling levers, and pushing buttons on administrators' consoles.

The industry can address this in any of a number of ways. Should we actually write software in a completely different way? Should we have system administrators at all? Or should we be developing machines that are able to administer other machines without routine humanintervention?

XII. Programming Tools

Each of these approaches requires new classes of software. As the absolute number and complexity of machines goes up, the administration problem outstrips the availability and capability of trained people. The result is that people in the programmingtools community are going to have to think about developing better ways to write programs. People who historically think about how to manage computers are going to have to think about how computers can become more selforganizing and self-managing. We need to continue to improve programming tools, because programming today is too error-prone. But current tools don't adequately support the process because of the number of abstraction layers that require foreground management. In other words, the designer needs not only to consider system architecture and platform/library issues, but also everything from performance, localization, and maintainability to data structures, multithreading and memory management. There is little support for programming in parallel, most control structures are built sequentially and the entire process is painfully sequential. And that is just in development; at the deployment level it is incredibly difficult to test for complex interactions of systems, versions, and the huge range in deployment environments. There is also the increasing diffusion of tools that offer advanced development functionality to a wider population but do not help novice or naive users write good code. There are also issues around long-term perspectives: for example, tools don't support "sunset-ing" or changing trends in capability, storage, speed, and so on. Think of the enormous effort devoted to Y2K because programmers of the 1960s and 1970s did not expect their code would still be in use on machines that far outstripped the capabilities of the machines of that era.

XIII. Interoperability

The growth of the Internet was proof that interoperable technologies−from TCP/IP to HTTP−are critical to building large-scale, multipurpose computing systems that people find useful and compelling. (Similarly, interoperable standards, enforced by technology, policy orboth, have driven the success of many othertechnologies, from railroads to television.) It isobvious and unavoidable that interoperablesystems will drive computing for quite some time. But interoperability presents a unique set ofproblems for the industry, in terms oftechnologies, policies and business practices.Current "trustworthy" computing systems, suchas the air-traffic-control network, are very complex and richly interdependent, but they arealso engineered for a specific purpose, rarelymodified, and strictly controlled by a centralauthority. The question remains whether adistributed, loosely organized, flexible, anddynamic computing system−dependent oninteroperable technologies−can ever reach thesame level of reliability and trustworthiness.Interoperability also poses a problem in terms ofaccountability and trust, in that responsibility forshortcomings is more difficult to assign. Iftoday's Internet−built on the principle ofdecentralization and collective management−were to suffer some kind of massive failure, whois held responsible? One major reason whypeople are reluctant to trust the Internet is thatthey can't easily identify who is responsible forits shortcomings – who would you blame for acatastrophic network outage, or the collapse of the Domain Name System? If we are to createand benefit from a massively interoperable (andinterdependent) system that people can trust, wemust clearly draw the lines as to who isaccountable for what.

XIV. Conceptual models

We face a fundamental problem withTrustworthy Computing: computer science lacksa theoretical framework. Computer security−itself just one component of TrustworthyComputing−has largely been treated as anoffshoot of communications security, which isbased on cryptography. Cryptography has a solidmathematical basis, but is clearly inadequate foraddressing the problems of trusted systems. Thecomputer-science community has not yetidentified an alternative paradigm; we're stuckwith

crypto. There may be research incomputational combinatory, or a different kindof information theory that seeks to study thebasic nature of information transfer, or researchin cooperative phenomena in computing, thatmay eventually form part of an alternative. But,today this is only speculation. A computing system is only as trustworthy as its weakest link. The weakest link is all too frequently human: a person producing a poor design in the face of complexity, an administrator incorrectly configuring a system, a business person choosing to deliver features over reliability, or a support technician falling victim to impostors via a "social engineering" hack. The interaction between sociology and technology will be a critical research area for Trustworthy Computing. So far there is hardly any crossfertilization between these fields.

XV. Conclusion

Delivering Trustworthy Computing is essentialnot only to the health of the computer industry,but also to our economy and society at large.Trustworthy Computing is a multi-dimensionalset of issues. All of them accrue to four goals: Security, Privacy, Reliability, and BusinessIntegrity. Each demands attention. Whileimportant short-term work needs to be done,hard problems that require fundamental researchand advances in engineering will remain. Bothhardware and software companies, as well asacademic and government research institutions,need to step up to the challenge of tackling theseproblems.

XVI. References

1) K. Sycara et al., —Automated Discovery,Interaction and Composition of Semantic WebServices,” J. Web Semantics, vol. 1, no. 1, 2003,pp. 27–46.
2) Web Services Conceptual Architecture (WSCA1.0), IBM Corp. specification, 2001; http://www-306.ibm.com/software/solutions/webservices/pdf/WSCA.pdf.
3) S. Ran, —A Model for Web Services Discoverywith QoS,” SIGEcom Exchanges, vol. 4, no. 1,2004, pp. 1– 10.
4) B. Sabata et al., —Taxonomy for QoSSpecifications,” Workshop on Object-OrientedReal-Time Dependable Systems (WORDS_97),IEEE CS Press, 1997.
5) K.-C. Lee et al., —QoS for Web Services:Requirements and Possible Approaches,” World Wide Web Consortium (W3C) note, Nov. 2003;www.w3c.or.kr/kr- office/TR/2003/ws-qos/.
6) K. Ballinger et al., WS-I Basic Profile Version 1.0a, Web Services Interoperability Org., 2003;http://www.ws-i.org/Profiles/.J.O. Kephart and D.M. Chess, —The Vision of Autonomic Computing,” Computer, vol. 36, no.1, 2003, pp. 41–50.
B. Yu and M.P. Singh, —An Evidential Model ofDistributed Reputation Management,” Proc.1st Int‘l Joint Conf.Autonomous Agents and Multiagent Systems, ACM Press, 2002, pp. 294–301

Network Layer with High Performance of Cognitive Radio networksPlatform

M.Y.Babu[1]Machha.Narender[2]M.Mohan Rao

GJCST Classification
C.2.2,C.4

***Abstract*-Network Layer with Radio networks High Performance Platform" being developed under the NSF NeTS ProWIN (programmable wireless networks) grant CNS-0435370. The network-centric cognitive radio architecture under consideration in this project is aimed at providing a high-performance platform for experimentation with various adaptive wireless network protocols ranging from simple etiquettes to more complex ad-hoccollaboration. Particular emphasis has been placed on high performance in a networked environment where each nodemay be required to carry out high throughput packet forwarding functions between multiple physical layers. Keydesign objectives for the cognitive radio platform include 1.multi-band operation, fast frequency scanning and agility;**

2.software-defined modem including waveforms such as DSSS/QPSK and OFDM operating at speeds up to 50 Mbps;

3.packet processor capable of ad-hoc packet routing with aggregate throughput 100 Mbps; 4.Spectrum policyprocessor that implements etiquette protocols and algorithmsfor dynamic spectrum sharing

I. Cognitive Radio Architecture & Design

The cognitive radio prototype's architecture is based on four major elements: (1) MEMS-based tri-band agile RF front-end, (2) FPGA-based software defined radio (SDR); (3) FPGA-based packet processing engine; and (4) embedded CPU core for control and management. Thesecomponents will be integrated into a single prototype board which leverages an SDR implementation from Lucent Bell Labs as the starting point. A proof-of-concept demonstration
board is planned for the end of year 2 (Sept 2006), and several prototype boards will full functionality are expected to be ready at the end of year 3 (Sept 2007).

The network-centric cognitive radio architectureunder consideration in this project is aimed atproviding a high-performance platform forexperimentation with various adaptive wirelessnetwork protocols ranging from simple etiquettesto more complex ad-hoc collaboration. Thebasic design provides for fast RF scanning capability, an agile RF transceiver working over a range of frequency bands, a software-defined radio modem capable of supporting a variety ofwaveforms including OFDM and DSSS/QPSK, a packet processing engine for protocol androuting functionality, and a general purposeprocessor for implementation of spectrumetiquette policies andalgorithms.The proposed architecture along with theassociated partitioning of design/prototyping responsibilities between Rutgers, GA Tech and Lucent is shown in Figure 1.1 below

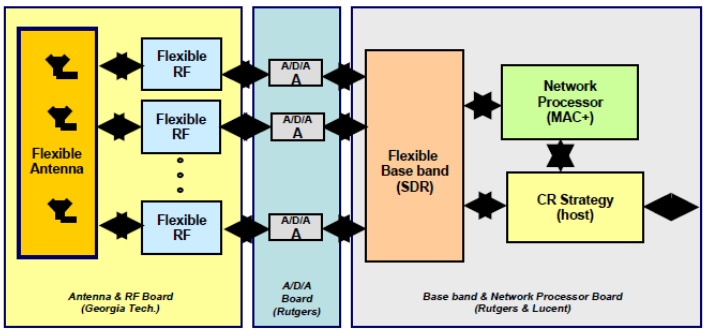


Figure 1.1 - Architecture of network-centriccognitive radio networks platform

In the original proposal, we identified the need for a base band and network processor board that would interface to the RF front-end and allow dynamically reconfigurable software and hardware implementations of multiple wirelesslinks supporting individual data rates up to50Mb/s and a maximum aggregate data rate of100 Mb/s. It was expected that this board wouldcontain some mix of DSP and FPGA blockstogether with their required memories. At thefirst coordination meeting in 4Q2004, we made adecision to avoid the use of DSP's because of thedifficulty associated with programming thesedevices. Rather, we decided to use acombination of FPGA for hardwareimplementation and embedded RISC forsoftware implementation. Embedded RISC mcannot match the cost and power efficiency of aDSP, but it was felt that ease of programmingwas of more importance in an experimental platform - especially one that would be used bystudents. The group also decided to aim for triband(700 MHz, 2.4 GHz and 5.1 GHz)capabilities using a novel MEMS device fromGA Tech - this was viewed as an importantflexibility feature for an experimental platformof this type. The analog front-end would alsosupport two channels, one for measurement andone for data, with bandwidths selectable in 1MHz increments.

A. Hardware architecture

Even though the prototyping effort is focused on an FPGA-based design, we are also exploring the architectural benefits of custom integrated circuitry, primarily related to power consumption and the silicon area, which are important performance parameters for hardware designs used in

About-[1]Asst.Professor, Aurora Engg College
e-mail-mannavababu@gmail.com
About-[2]Asst.Professor, HITS College of Engg
(e-mail- machha.narender@gmail.com)
About-[3]Asst.Professor, Tirumala Engg College
(e-mail-mohanrao19@yahoo.com)

mobile/portable platforms. The approach we have chosen to take involves identifying the hardware architecture appropriate for low-power configurable design based on heterogeneous blocks (i.e. blocks that are highly optimized for aparticular function, yet flexible enough to support a variety of configuration parameters) as a compromise for the tradeoff between programmability and power consumption/area. In addition to fast prototyping, the additional benefits of using modern FPGAs (e.g. Xilinx Virtex 4) are the availability of highly optimized features implemented as non-standard configurable logic blocks (CLB) like phaselocked loops, low-voltage differential signal, clock data recovery, lots of internal routing resources, hardware multipliers for DSP functions, memory, programmable I/O, and microprocessor cores. These advantages simplify mapping from hierarchical blocks to FPGA resources.

The hardware design effort started with anevaluation of architectures presentlyavailable for base band SDR processingat rates of 50-100 mbps. All thesearchitectures use massive hardwareparallelism to sustain high data rate. Wealso looked at the base band processingrequirements of different wirelessstandards such as 802.11a/b, Bluetoothand WCDMA, and found that differentstages of base band processing have verydifferent hardware needs. Thus, using ageneric hardware design leads toinefficient usage of chip area and powerconsumption. As a result, we proposed a "heterogeneous block-based architecture" which would help implement SDR baseband processing in an efficient way. Anadditional feature is the ability toefficiently reconfigure blocks in a fewclock cycles to facilitate fastchangeover between multiple SDRphysical layers.

B. Heterogeneous block-based architecture

The heterogeneous-block based architecture (see Figure 1.2 below) combines a general microprocessor with special purpose hardware blocks. The microprocessor containing multiplier/accumulator units handles control intensive operations such as channel estimation, synchronization, and programming and interconnection of the heterogeneous blocks, while data intensive operations are handled by the heterogeneous blocks. The following heterogeneous-blocks have been identified:

1. Channel utilization Block: A configurable multi-stage filter used toselect a sub-band and/or decimate theinput signal for different standards
2. FFT/MWT Block: A configurablearchitecture which can handle FFToperations used in OFDM and alsohandle the modifier Walsh transformused in 802.11b.
3. Rake Block: A generic four fingerRake accelerator for channel estimation,de-spreading in DSSS and CDMA.
4. Inter leaver Block: Using a blockbasedmemory and multiplexer-basedaddress handler, a multi-modearchitecture can handle de-interleavingfor different standards.
5. Data and Channel Encoding/Decoding Block: A configurablearchitecture can handle both Viterbi (for802.11a) and Encoder/Turbo Decoder(for WCDMA). Both the Data andChannel Encoder have a similar connection pattern, but only the Data Encoder needs feedback. A commonblock is proposed which can beconfigured in one clock cycle to perform either of the twofunctionalities.
6. Detection and Estimation Block: Common interference detection block.

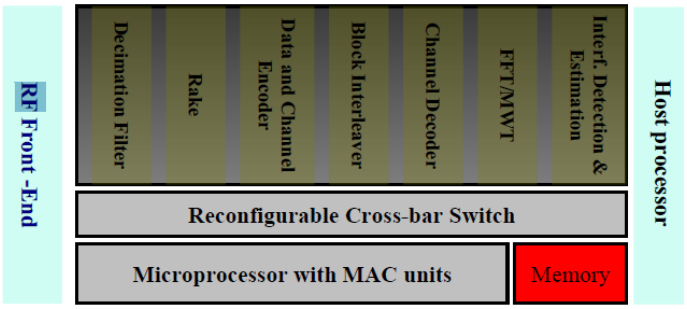


Figure 1.2 - Heterogeneous Blocks based Base band Processor Architecture

The hardware design effort started with an evaluation of architectures presently available for base band SDR processing at rates of 50-100 mbps. All these architectures use massive hardware parallelism to sustain high data rate. We also looked at the base band processing requirements of different wireless standards such as 802.11a/b, Bluetooth and WCDMA, and found that different stages of base band processing have very different hardware needs. Thus, using a generic hardware design leads to inefficient usage of chip area and power consumption. As a result, we proposed a "heterogeneous block-based architecture" which would help implement SDR base band processing in an efficient way. An additional feature is the ability to efficiently reconfigure blocks in a few clock cycles to facilitate fast changeover between multiple SDR physical layers.

Ongoing work is aimed at creating animplementation of the above SDR design usingavailable FPGA boards and conductingevaluations on flexibility and performance. The packet processing engine's architecture will alsobe considered during the remainder of thisreporting year. The goal is to have both SDRand packet processor FPGA implementationstested and evaluated by the end of 2005.

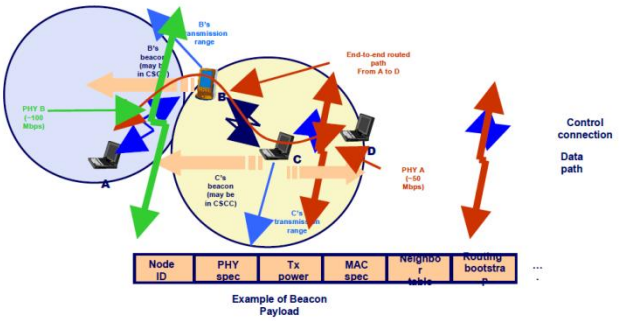
II. Spectrum Scanning Algorithms

An important aspect of the cognitive radioplatform is its ability to opportunistically useportions of the spectrum that are not being used,which requires the ability to efficiently scanspectrum usage. Furthermore, it is veryimportant to detect and identify types ofinterference that the platform is facing. Thisbecomes increasingly difficult for arbitrary radiosystems. Thus we can focus on an OFDM radioplatform because it allows a simplecharacterization of interference in terms of theOFDM sub carriers. A project on spectrum detection algorithms was carried out in order to understand the computational complexity and response times for the scanning receiver. In order to solve this detection and estimation problem, we used an eigen value decomposition of the sample covariance matrix of the received signal. This analysis was performed using

computer simulations for two common sources of interference: a microwave oven and a Bluetooth radio. Simulations carried out show that the
influence of an interfering signal on the OFDM system depends on the power of the interfering signal and the data rate in the OFDM system (this system supports the following data rates: 6, 9, 12, 18, 24, 36, 48 and 54 Mbps). As expected, the BER of the system increases with the increasing power of the interfering signal and increasing data rate of the OFDM system. In the presence of the microwave oven signal, only one of the 64 eigen values of the covariance matrix is affected. In the presence of the Bluetooth radio interference, several eigen values will be affected. The number of affected eigen values in this case is proportional to the power of the interfering signal. In the future work, we will examine how multiple radios can collaborate in the detection of interferers, including the
development of protocols for the exchange and aggregation of measurements.

III. Adaptive Network Protocols

In parallel to SDR and packet processor designwork described above, a project has been startedon adaptive network protocols and relatedalgorithms. In particular, we are studying theconcept of an adaptive wireless network
bootstrapped from the CSCC etiquette protocolpreviously developed at WINLAB. The CSCCprotocol (which uses a broadcast beaconmechanism to inform neighboring radios ofsignal properties) is being extended to includeinformation necessary for self-organization intoa collaborative network of cognitive radios.Information on transmit power, PHY speeds,channel quality and aggregated routinginformation is added to the beacon to facilitateself-organization. This concept is shown in



below Figure 1.3
Figure 1.3 - Concept for CSCC-based selforganization
In a cognitive radio network
A preliminary evaluation of the protocol concepts is planned for year 2 of the project using a GNU radio extension to the ORBIT radio grid test bed. A GNU radio kit has been procured and an RF front end module is being developed for subsequent use as softwaredefined ORBIT radio node extension.

IV. Security

One of the factors which should be considered during design process of CRN emergency network is security of the network infrastructure and security of transmitted information. Without proper network security terrorists responsible for the disaster would be able to eavesdrop emergency information and utilize it for future attacks. Moreover the some of the possible methods of attacks on CRN and ways of prevention:

Licensed user emulation attack: Because cognitive radios cannot be completely sure whether a licensed spectrum is free and available for transmission they simply defer from licensed bands and utilize other non-licensed parts of the band if they are not sure if it is really free. Suppose that attacker knows in which specific area CRN works. Knowing which licensed bands CRN might use attacker can simply transmit signal in the licensed band emulating real transmission and thus limiting overall CRN capacity. Until now we don't know any method of prevention against this attack.

Common control channel jamming*:* Oneof the possible solutions for commoncontrol channeldeployment is the UWB. In this casepotential attacker can simply transmit
periodical pulses whichhave the same spectrum as common control channel of CRN but with higherpower than legitimateusers. Throughout jamming of just onechannel attacker blocks the possibility ofcommunicationbetween all CR nodes. This is the reasonfor building sophisticated UWBtransmission methods forcontrol channels utilizing UWB. It has tobe underlined that a need for special careof control channel isthe same for any type of approach
(dedicated channel, channel hopping etc.).

Attacks on spectrum managers:We cannot allow having one central spectrum manager responsible for assigning frequency bands for nodes (see paragraph 2.3) because it constitutes a single point of attack. Whenever the spectrum manager is not available for CR nodes the communication process becomes impossible. That is whyinformation about spectrum availabilityshould be as distributed andreplicated as possible. This constraint is inline with the requirement for moreaccurate measurements
of spectrum availability (see paragraph2.3). One of the preventing ways for thisattack is to use specific pilot channel innetwork elements due to their poor securitycould become a target of attack itself. Becausecognitive radio constitute a new approach forbuilding wireless networks it simultaneouslyopens a door for new methods of attacks ontheir physical structure. Below we outline each license band. It would inform secondary users about the reservation of
the nodes.

Eavesdropping: Usually in the infrastructure-based corporate WLAN it was assumed that signal will not leave building due to his short distance and will be limited to eavesdropping and sniffing. However cognitive radios are allowed to work in the bands lower than UNII and ISM. This means that they can perform longer transmission distances with the same powers. It also allows foreasy physical data collection from locations far distancedfrom CRN location where attackers invisible to emergency services. This yields a need for strong dataencryption at the physical level. Frequent leaving and joining the emergency

network must be preceded by authentication process. It is open for discussion which layer should be responsible for this step. Currently the most possible approach is that application layer willperform all the necessary authentication procedures. Moreover the entire WEP infrastructure should be the basis for authentication procedures in CRNs.

VIII. Conclusions

The rapidly changing radio environment, more radio channels to utilize, number of parameters to choose during decisions taken by MAC and routing protocols, etc. makes design of CRNs very challenging. In this deliverable we have outlined some specific parameters and constraints which have to be taken into consideration while designing protocols for layers above PHY. Many protocols have the same design requirements (like robustness, no clock synchronization or localizing capabilities) which simplify design by small fraction. Moreover we can state that UWB as a common control channel might become a good solution for realizing certain functions outlined in this document. We also outline that cooperation between physical and link layer is essential for accurate operation of CRN. We have to emphasize that new requirements might occur during design process so this document will be constantly updated.

V. References

1) Josef Hausner, Integrated Circuits for Next Generation Wireless System European Solid-State Circuits Conference, 2001
2) Linkopings University Programmable Base band Processor Website http://www.da.isy.liu.se/research/bp/bbp1.html
3) Cavallaro, J.R.; Vaya, M.; Viturbo: a reconfigurable architecture for Viterbi and turbo decoding; Proceedings of
4) IEEE International Conference on Acoustics, Speech, and Signal Processing, 2003. (ICASSP ' 03). Volume: 2, 6-10 April 2003 Pages: II - 497-500
5) Eric Tell, Olle Segeroch, Dake Liu; A Converged Hardware Solution for FFT, DCT and Walsh Transform; Proc. of the International Symposium on Signal Processing and its Applications (ISSPA), Paris, France, Vol. I, pp. 609 - 612, July 2003
6) Eric Tell, Dake Liu; A Hardware Architecture for a Multi Mode Block Interleaver; International Conference on Circuits and Systems for Communications (ICCSC), Moscow, Russia, June 2004
7) Simon Leung, Adam Postula, Ahmed Hemani; Customized Reconfigurable Block-based Architecture for Base band Data Processing in Telecommunication Applications. International Conference on Chip Design Automation (ICDA 2000), Beijing, China, Aug. 2000
8) Sridhar Rajgopal, Joseph R. Cavallaro; A Programmable Base band Processor Design for Software Defined Radios.
9) IEEE Mid West Conference on Circuit and Systems, Tulsa, USA, August 2002
10) Hui Zhang, Jan M. Rabaey, et. al.; A 1V Heterogeneous Reconfigurable Processor IC for Base band WirelessApplications. IEEE International Solid-State Circuits Conference, February2002

Conceptual Clustering Of RNA Sequences With Codon Usage Model

GJCST Classification
J.3,H.3.3

Barilee B. Baridam[1], Olumide Owolabi[2]

***Abstract*-This paper proposes a conceptual clustering approachfor RNA sequences using codons. It is shown thatemploying the codons (codon usage model) in the conceptualclustering of RNA sequences has high efficiency and robustnesscompared to conventional clustering methods. In cases wherethere are hidden structural patterns, homology search algorithmsare inefficient in locating similar sequences and as a result arenot reliable in the task of biological sequence clustering. As isshown by empirical results in this paper, conceptual clusteringusing the codons is able to discover similar sequences in adatabase of sequences with hidden structural homologues. Thecodon usage and cohesiveness model introduced in this papercan be efficiently employed in clustering biological sequence datawhere conventional homology search algorithms fail.**

Keywords- Conceptual clustering, cohesiveness, codon usage,formal concept analysis, RNA sequences.

I. Introduction

Conventional Data analysis employs context-free similarity measures, that is, similarity based on the properties of the objects without considering the environment where the objects are found. On the other hand, contextsensitive similarity measures are not only based on the properties of the objects but also the properties of the surrounding environment. All these similarity measures (context-free andcontext-sensitive) are concept-free. Similarity search based on a set of concepts describing objects, and not just on properties and environment, are what is employed in this paper.

Although biological data can be clustered using context-free similarity measures (Lee & Crawford 2005), the clustering of biological sequence data with context-sensitive similarity measures may not be appropriate. This is because the environment has little or no effect on already sequenced biological data. However, context-free homology searches can only yield less than 60% found genes and only a few of the searches can result in assigning the correct structure of the genes (Math´e, Peresetsky, D´ehais, Van Montagu & Rouz´e 1999). Therefore, biological clustering using conceptual clustering, clustering based on sets of concepts, by employing the codon usage (CU) model becomes appropriate to cluster sequences with hidden biological patterns.

Conceptual clustering is employed in this paper for the task of clustering RNA sequences. The goal is to employ codons,otherwise referred to as the CU model, and the cohesiveness model (the degree of codon cohesion) in clustering RNA sequences. Conceptual cohesiveness, from which codon cohesiveness is derived, is a measure of similarity between two points based on a set of concepts available for describing the two points (Michalski & Stepp 1986). The method has the ability to cluster sequences which would not ordinarily be clustered with conventional categorical clustering methods like CLUSEQ - CLUstering for SEQuences, ED - Edit Distance, and EDBO - Edit Distance with Block Operations (Yang & Wang 2003), (Levenshtein 1965), (Lopresti & Tomkins 1997).

The remainder of this paper is arranged as follows: A brief look at formal concept analysis followed by related work, themethods employed in this paper for the clustering of biologicalsequence data, followed by some experimental results, andlastly conclusions and future research.

B. B. Baridam is with the Department of Computer Science, University of Pretoria, South Africa, 0083. E-mail: bbaridam@cs.up.ac.za
O. Owolabi is the Director of Computer Science Centre, University of Abuja, Nigeria. E-mail: olumideo@uniabuja.edu.ng

II. Conceptual Clustering

Conceptual clustering is a machine-learning paradigm forunsupervised classification that aims at generating a conceptdescription for each generated class. This section considers
formal concept analysis (FCA) and the Galois or conceptlattice.

A. Formal Concept Analysis

FCA aims at the automatic derivation of ontology based on a collection of objects and their properties. FCA, introduced byRudolf Wille and his students in 1984, is a direct applicationof the applied lattice and order theory developed by Birkhoffand others in the 1930s (Birkhoff 1930). FCA attempts tofind all the natural clusters of properties and all the naturalclusters of objects in the input data. The set of all objects thatshare a common subset of properties or attributes is referredto as a natural object cluster, while the set of all propertiesor attributes shared by one of the natural object clusters isreferred to as a natural property cluster.

i. Concepts Definition

From the description of FCA, conceptanalysis employs a set of objects and a set of propertiesor attributes belonging to all or some of the objects. For everyset of objects O, set of properties P and an indication of whichobject has which attribute, a concept can be defined to be a pair(Oi; Pi) such that the following conditions hold(Vinner 1983):

1) $O_i \subseteq O$
2) $P_i \subseteq P$

1) Every object in $O_i$has every attribute in Pi
2) For every object in O that is not in O_i, there is an attribute in Pi that the object does not have
3) For every object in P that is not in P_i, there is an attribute in O_i that does not have that attribute.

From the definition above, it can be said that a concept isa pair containing both a natural property cluster and its correspondingobject cluster. The mathematical axioms defining

TABLE I
CONCEPT REPRESENTATION WITH NUCLEOTIDES

	A	C	G	U
Tyrosine	×	×		×
Cysteine		×	×	×
Tryptophan			×	×
Histidine	×	×		×
Glutamine	×	×	×	
Methionine	×		×	×
Asparagine	×	×		×
Lysine	×		×	
Aspartic acid		×	×	×
Glutamic acid	×		×	
Arginine	×		×	

A lattice based on these concepts are referred to as concept lattice or as a general term, Galois lattice.

2) The Concept (or Galois) Lattice: The concept lattice can be described using the concepts (O_i, P_i). Partially ordering these concepts by inclusion, it is obtained that: if (O_i, P_i) and (O_j, P_j) are concepts, a partial order $\leq$ can be defined that $(O_i, P_i) \leq (O_j, P_j)$ whenever $O_i \subseteq O_j$. It follows, therefore, that $(O_i, P_i) \leq (O_j, P_j)$ whenever $P_j \subseteq P_i$. There exists a unique greatest lower bound (*meet*) and a unique least upper bound (*join*) in every pair of concepts in this partial order which makes it satisfy the axioms defining a lattice. The concepts with objects $O_i \cap O_j$ are inclusive in the greatest lower bound of (O_i, P_i) and (O_j, P_j) with its attributes as $P_i \cup P_j$ and any additional attributes common to objects in $O_i \cap O_j$. Symmetrically, therefore, the least upper bound of (O_i, P_i) and (O_j, P_j) is the concepts with attributes $P_i \cap P_j$ with its objects as $O_i \cup O_j$ inclusive of additional objects with all the attributes in $P_i \cap P_j$ (Mephu-Nguifo 1994), (Wille 1992).

Biological sequence clustering, using conceptual clustering based on the CC model, becomes appropriate, therefore, to capture hidden biological (structural) pattern in sequence data.Following the rule for conceptual clustering, the objects andtheir attributes (properties) are derived as explained below.The objects are derived from the nucleotides in peptideformation during RNA translation using the basic RNA nucleotides- A, C, G and U. The nucleotides are the attributes.These peptides are Tyrosine, Cysteine, Tryptophan, Histidine,Glutamine, Methionine, Asparagine, Lysine, Aspartic acid,Glutamic acid and Arginine.

A tabular representation of these peptides showing their properties (attributes) based on their nucleotide formation, is given in Table I. A cross (X) in the cells indicates the presence of an attribute, while a space indicates none. Note that the bases are in triplets, referred to as a codon, and that several contiguous bases (codons) may form a particular peptide and so a base can be repeated twice or three times, depending on the peptide involved, e.g. Lysine and Arginine with AAA, AAG and AGA, AGG, respectively.

Table I serves as a guide in the clustering of nucleic acidsequences. In the clustering task, sequences are represented asobjects while peptides are the attributes.

III. Related Work

Several algorithms have been proposed for conceptual clusteringsince the idea was developed in the 1980s. Carpinetoand Romano (Carpineto & Romano 1993), introduced GALOISwhich is an order-theoretic approach to conceptualclustering. From experimental results presented, Carpineto andRomano argued that GALOIS performs better than other methods.Michalski and Stepp (Michalski & Stepp 1986) developedthe conjunctive conceptual clustering program CLUSTER/2in which the predefined concept class consists of conjunctivestatements involving relations on selected object attributes.The method was experimented on a large collection of Spanishfolk songs. The result proved the efficiency of CLUSTER/2in the clustering task. Kolodner (Kolodner 1983) proposedthe CYRUS algorithm, which was also an improvement onexisting methods. An earlier paper by Michalski (Michalski1980) introduced the idea of partitioning data into conjunctiveconcepts to handle knowledge acquisition through conceptualclustering. Furthermore, Lebowitz (Lebowitz 1987) proposedthe UNIMEM algorithm for incremental concept formation inconceptual clustering problems as a system that learns from

observation by noticing regularities among examples and organizingthem into a generalization hierarchy. In the same year,Fisher (Fisher 1987) came up with the COBWEB algorithm forknowledge acquisition via incremental conceptual clustering.The most recent algorithms in this field were proposed byJonyer et al. (Jonyer, Cook & Holder 2001) and Talavera andB´ejar (Talavera & B´ejar 2001), namely SUBDUE and GCF,respectively. Talavera and Bjar employed probabilistic conceptsin performing a generality-based conceptual clustering.Despite the successful implementation of conceptual clusteringin data analysis (Kuminek & Kazman 1997),(Ketterlin,Ganc¸arski & Korczak 1995), it has not been employed as muchin the field of bioinformatics to date. The most recent workon the application of conceptual clustering in the clustering ofbiological data is the work done by McClean et al. (McClean,Scotney & Robinson 2001) on the conceptual clustering ofheterogeneous gene expression sequences. Other work thatmay look like conceptual clustering, though not explicitlystated, was done by Math´e et al. (Math´e et al. 1999). In theclassification of Arabidopsis thalianagene sequences, codonusage was employed by Math´e et al. in the classificationof coding sequences into two groups. The result was animprovement in the quality of gene prediction

compared toexisting methods.It is important to note that other than the work presentedby Math´e et al. (Math´e et al. 1999) none of the methodsmentioned above considered the application of conceptualclustering in the clustering of biological sequences, althoughthe work presented by Math´e et al. is limited to a particularset of gene sequences.

IV. The Codon Cohesiveness Model

The codon cohesiveness model employs what is referredto here as codon usage in determining the frequency of each codon in a given sequence. The codon usage (CU) of a given

TABLE II
CLUSTERS GENERATED BY CLUSTAL

Cluster	Sequence
1	7,16,5,15,3,6,1
2	13,20,12,2,17,4
3	14,11,9,19,10,18,8

sequence is defined as:

$$CU = \frac{f_c}{S_l} F_l \qquad (1)$$

where f_c= the relative codon frequencies, S_l = the sequence length and F_l = the feature (codon) length. The feature lengthis a constant and is equals 3, since there are just three basesthat form a codon.

The codon cohesiveness (CC) or the degree of cohesion is now defined based on the CU as follows:

$$CC = \sum_{i=0}^{N} \frac{f_{c_i}}{S_l} . F_l \quad = \sum_{i=0}^{N} CU_i \qquad (2)$$

The values of CU and CC are between 0 and 1. CCdetermines to what extent the sequence to be clustered is closeto the peptide group - the attribute.Codon cohesiveness is used to group similar sequencesbased on the occurrence of codons. Sequences with higheroccurrence of a peptide group are grouped in the same cluster.

V. Experimental Results

The method was tested on 20 Rickettsia typhi str. sequences from the Wilmington complete genome. Patternelement-wise search was used in detecting available codonsin the sequences. When the edit distance was employed inthe search, it was found that none of the sequences was atleast 60% similar, based on the homology principle (Claverie& Notredame 2007), and so the clustering result was notuseful. Also, clustering Rickettsia typhi str. sequences with edit distance violates the rule that nucleic acid sequences canonly be considered homologue if and only if they are or morethan 70% similar (Claverie & Notredame 2007).

Overlaps are encountered with this clustering technique. The solution used to overcome the problem of overlaps is the CC model. In the result obtained in Table IV, sequences with at least 30% amino acid occurrence are grouped based on their CC values. When this was done, 6 clusters were generated as indicated in Table II using the peptide formation grouping.Of all the sequences clustered, sequences 1, 2, 4, 6, 15 and 17 have some similarities. However, they could not be grouped based on the values of the CU model. The CU values and the resultant CC values for these sequences are less than 20%.However, they cannot be considered as outliers since they manifest some measure of similarity. Recall that the highest CU or CC values renders a sequence clusterable. However,sequence 3 could not be grouped although it has the highest CU and CC values. The method employed here reveals that sequence 3 has a STOP signal. This makes it different from the rest of the sequences tested. It will not be out of place to consider sequence 3 outlier.

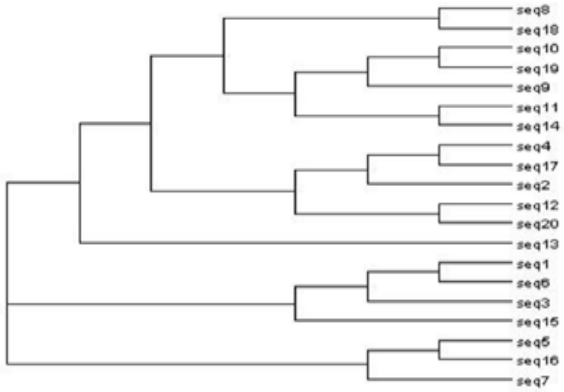


Fig. 1. Generated phylogenetic tree of the sequences

With crisp clustering (sequences belong to one and only one cluster), six clusters were generated as indicated in Table IV.From the results it is evident that the method employed in this paper produces clusters of even shape based on their codons.CLUSTAL produced three clusters with crisp clustering. The result of CLUSTAL clustering is indicated in Table II.Employing fuzzy clustering, Table III produces more clusters of sequences 11 and 14; 11, 13 and 18; 9, 10 and 19; 8,10 and 13; 5, 11 and 16; 12 and 20; 5, 7 and 16, forming separated clusters.The result was compared with a constructed phylogenetic tree of the sequences. A phylogenetic tree (Figure V) is used to show how related the sequences are based on their genetic composition, thus defining or at the very least, giving the idea of the composition of clusters that may be formed by any clustering or similarity search algorithm. Note that phylogenetic trees are constructed mostly using multiple-alignment algorithms. Note also that alignment algorithms introduce gaps to achieve sequence alignments (Corpet 1988), (Gondro & Kinghorn 2007), (Notredame & Higgins 1995). To prove the inefficiency of such methods, gaps are penalized. The clustering done in this paper does not consider the introductionof gaps, hence, the result is somewhat different and better than the one achieved with other methods that use aligned sequences.

VI. Conclusion

Conceptual clustering is successfully employed in this paper

to cluster RNA sequences through the application of the geneticcode triplet bases arrangement referred to as codon. Themethod is a strong deviation from popular clustering methods.The result obtained from the method is promising and couldbe extended to other areas of biological sequence clustering.Further research on this work could involve the clustering ofother biological sequences, for example amino acids.

VII. References

1) Birkhoff, G. D. (1930), _Formal theory of irregular linear difference equations‘, Acta Mathematica 54(1), 205–246.
2) Carpineto, C. & Romano, G. (1993), Galois: An order-theoretic approach to conceptual clustering, in _Proceedings of10th International Conference on Machine Learning‘, Amherst, pp. 33–40.
3) Claverie, J. & Notredame, C. (2007), Bioinformatics for dummies, 2nd edn,Wiley, Indiana.
4) Corpet, F. (1988), _Multiple sequence alignment with hierarchical clustering‘,Nucleic Acids Research 16(22), 10881–10890.
5) Fisher, D. H. (1987), _Knowledge acquisition via incremental concept clustering‘,Machine Learning 2, 139–172.
6) Gondro, C. & Kinghorn, B. P. (2007), _A simple genetic algorithm for multiplesequence alignment‘, Genetics and Molecular Research 6, 964–982.
7) Jonyer, I., Cook, D. J. & Holder, L. B. (2001), _Graph-based hierarchicalconceptual clustering‘, Journal of Machine Learning Research 2, 19–43.
8) Ketterlin, A., Ganc¸arski, P. & Korczak, J. J. (1995), Conceptual clustering instructured databases: A practical approach, in _Proceedings of KDD‘,pp. 180–185.
9) Kolodner, J. L. (1983), _Reconstructive memory: A computer model‘, CognitiveScience 7, 281–328.
10) Kuminek, J. & Kazman, R. (1997), Accessing multimedia through conceptclustering, in _Proceedings of ACM CHI‘, pp. 19–26.
11) Lebowitz, M. (1987), _Experiments with incremental concept formation‘,Machine Learning 2, 103–138.
12) Lee, S. & Crawford, M. M. (2005), _Unsupervised multistage image classificationusing hierarchical clustering with a Bayesian similarity measure‘,IEEE Transactions on Image Processing 14(3), 312–320.
13) Levenshtein, V. I. (1965), _Binary codes capable of correcting deletions, insertions, and reversals‘, Doklady Akademii Nauk SSSR 163(4), 845–848.
14) Lopresti, D. & Tomkins, A. (1997), _Block edit models for approximate stringmatching‘, Theoretical Computer Science 181, 159–179.
15) Math´e, C., Peresetsky, A., D´ehais, P., Van Montagu, M. & Rouz´e, P. (1999),_Classification of Arabidopsis thaliana gene sequences: Clustering ofcoding sequences into two groups according to codon usage improvesgene prediction‘, Journal of Molecular Biology 285, 1977–1991.
16) McClean, S., Scotney, B. & Robinson, S. (2001), _Conceptual clustering ofheterogeneous gene expression sequences‘, Artificial Intelligence Review20, 53–73.
17) Mephu-Nguifo, E. (1994), Galois lattice: a framework for concept learning.design,evaluation and refinement, in _Proceedings of Sixth International Conference on Tools with Artificial Intelligence‘, New Orleans, LA,USA, pp. 461–467.
18) Michalski, R. S. (1980), _Knowledge acquisition through conceptual clustering:A theoretical framework and an algorithm for partitioning datainto conjunctive concepts‘, International Journal of Policy Analysis andInformation Systems 4, 219–244.
19) Michalski, R. S. & Stepp, R. E. (1986), Learning from observation: Conceptualclustering, in R. S. Michalski, J. G. Carbonell & T. M. Mitchell,eds, _Machine learning - An artificial intelligence approach‘, MorganKaufmann, Los Altos, CA, pp. 471–498.
20) Notredame, C. & Higgins, D. G. (1995), _SAGA a genetic algorithm for multiple sequence alignment‘, Nucleic Acids Research 174, 1515.
21) Talavera, L. & B´ejar, J. (2001), Generality-based conceptual clustering withprobabilistic concepts, in _IEEE Transactions on Pattern Analysis andMachine Intelligence‘, Vol. 23, Amherst, pp. 196–206.
22) Vinner, S. (1983), _Concept definition, concept image and the notion of function‘, International Journal of Mathematical Education in Science and Technology 14(3), 293–305.
23) Wille, R. (1992), _Concept lattices and conceptual knowledge systems‘,Computers and Mathematics with Applications 23(6–9), 493–515.
24) Yang, J. & Wang, W. (2003), CLUSEQ: efficient and effective sequenceclustering, in _Proceeding of 19th International Conference Data Engineering‘,pp. 101–1125.

TABLE IIICALCULATED CC OF SEQUENCES

Sequence	A	Sequence	R	Sequence	G	Sequence	K	Sequence	F	Sequence	P	Sequence	S
5	0.30	11	0.65	5	0.30	5	0.30	9	0.35	8	0.40	12	0.35
11	0.65	14	0.50	7	0.30	16	0.30	10	0.35	10	0.55	20	0.35
14	0.45			11	0.45			19	0.30	13	0.40		
16	0.30			13	0.40								
18	0.30			16	0.30								
				18	0.45								

A = Alanine(GCU, GCC, GCA, GCG); R = Arginine(CGU, CGC, CGA, CGG); G = Glycine(GGU, GGC, GGA, GGG);
K = Lysine(AAA, AAG); F = Phenylatanine(UUU, UUC); P = Proline(CCU, CCC, CCA, CCG); S = Serine(UCU, UCC, UCA, UCG)

TABLE IV CLUSTERS GENERATED BASED ON CC VALUES

CLUSTER 1		CLUSTER 2		CLUSTER 3		CLUSTER 4		CLUSTER 5		CLUSTER 6	
Sequence	A	Sequence	R	Sequence	G	Sequence	F	Sequence	P	Sequence	S
5	0.30	11	0.65	7	0.30	9	0.35	8	0.40	12	0.35
16	0.30	14	0.50	13	0.40	19	0.30	10	0.55	20	0.35
				18	0.45						

Vehicle Counting And Classification Using Kalman Filter And Pixel Scanner Technique And Its Verification With Optical Flow Estimation

GJCST Classification
I.3.8,1.3.m

H.S. Mohana[1], Aswatha Kumar. M [2] and G. Shivakumar[3]
[1,3]Malnad College of Engineering, Hassan, Karnataka
[2]MS Ramaiah Institute of Technology, Bangalore, Karnataka
hsm@mcehassan.ac.in, maswatha@yahoo.com,gs@mcehassan.ac.in

***Abstract*-Vehicle tracking is important in traffic monitoring systems. The behaviors of regions of moving vehicles are complicated, since the regions may combine or break during the tracking due to mistakes in vehicle detection and tracking or vehicles' overlapping with each other, and as a result, region matching simply according to similarities between successive frames is not enough to achieve reliable results. This paper proposes a novel tracking strategy that can robustly track and classify the objects within a fixed environment. We define a robust model-based tracker and classifier using kalman filtering combined with pixel scanner. The tracking is done by fitting successively more elaborate models on the tracked region and the segmentation is done by extracting the regions of the image that are consistent with the computed model of the target. We adopt a competitive and efficient dynamic Kalman filtering to adaptively update the object model by adding new stable features as well as deleting inactive features. In the next stage we need to check each and every frame for object recognition. This work introduce a diagonal pixel scanner to identify the objects. The result is verified further by implementing optical flow analysis. The tracking, counting and classification of object/vehicle have produced very consistent result. The average accuracy with short length video clipping is greater than 98%.**

Keywords-Kalman filter, pixel scanner, object classification and object counting.

I. INTRODUCTION

Traffic on roads may consist of pedestrians, ridden or herded animals, vehicles, streetcars and other conveyances, either singly or together, while using the public way for purposes of travel. Traffic is often classified by type: heavy motor vehicle (e.g., car, truck); other vehicle (e.g., moped, bicycle); and pedestrian. Computer vision is concerned with the theory for building artificial systems that obtain information from images. The image data can take many forms, such as a video sequence and /or views from multiple cameras.

The Kalman filter produces estimates of the true values of measurements and their associated calculated values by predicting a value, estimating the uncertainty of the predicted value, and computing a weighted average of the predicted value and the measured value. The most weight is given to the value with the least uncertainty. The estimates produced by the method tend to be closer to the true values than the original measurements because the weighted average has a better estimated uncertainty than either of the values that went into the weighted average.

Optical flow is the distribution of apparent velocities of movement of brightness patterns in an image. Optical flow can arise from relative motion of objects and the viewer. Consequently the optical flow can give important information about the spatial arrangement of the objects viewed and the rate of change of this arrangement. Discontinuities in the optical flow can help in segmenting images into regions that correspond to different objects. Attempts have been made to perform such segmentation using differences between successive image frames.

Several papers address the problem of recovering the motions of objects relative to the viewer from the optical flow. Some recent papers provide a clear exposition of this enterprise. The mathematics can be made rather difficult, by the way, by choosing an inconvenient coordinate system. In some cases information about the shape of an object may also be recovered. It is assumed that the optical flow has already been determined. Although some reference has been made to schemes for computing the flow from successive views of a scene, the specifics of a scheme for determining the flow from the image have not been described. Related work has been done in an attempt to formulate a model for the short range motion detection processes in human vision .The pixel recursive equations of Netravali and Robbins designed a method for coding motion in television signals. This bear some similarity to the iterative equations developed in this paper. A recent review of computational techniques for the analysis of image sequences contains over 150 references. It suggests that the optical flow cannot be computed at a point in the image independently of neighboring points without introducing additional constraints, because the velocity field at each image point has two components while the change in image brightness at a point in the image plane due to motion yields only one constraint.

Velocity is a vector quantity which refers to "the rate at which an object changes its position." Imagine a person moving rapidly - one step forward and one step back - always returning to the original starting position. While this might result in a frenzy of activity, it would result in a zero velocity. Because the person always returns to the original position, the motion would never result in a change in position. Since velocity is defined as the rate at which the

position changes, this motion results in zero velocity. If a person in motion wishes to maximize their velocity, then that person must make every effort to maximize the amount that they are displaced from their original position. Every step must go into moving that person further from where he or she started. For certain, the person should never change directions and begin to return to the starting position.

Considering a patch of pattern where brightness varies as a function of one image coordinate but not the other. Movement of the pattern in one direction alters the brightness at a particular point, but motion in the other direction yields no change. Thus components of movement in the latter direction cannot be determined locally.

II. Related Work

After referring some of the technical papers under Traffic analysis resulted in novel idea to reach the objective. Some of the papers referred are presented here. Discussion on referred paper provides the limitations of those methods and how our approach seems to be advantageous over them. Reference [1] presents algorithms for vision-based detection and classification of vehicles in monocular image sequences of traffic scenes recorded by a stationary camera. Processing is done at three levels: raw images, region level and vehicle level. It is observed that data acquisition of monocular image sequence is a very tedious task. The information gathered is more than required as it covers the region level information as well. the present method incorporates .avi standard sequences which can be easily manipulated and worked upon. The computational time and memory requirement is much less than compared to the above method. In [2] a study on a stand-alone image tracking system for automatic traffic monitoring is presented. The proposed image tracker consists of three parts: an edge detection module, an image tracking module and a traffic monitoring module. The above paper uses a tracking system which automatically does the monitoring system with no manual interference in real time. It consists of edge detection, image tracking and monitoring the traffic. A novel tracking strategy is proposed in [3] that can robustly track an object within a fixed environment. Authors define a robust model-based tracker using Kalman filtering combined with recursive least squares. It uses a tracking done by fitting successively more elaborate models on the tracked region and the segmentation is done by extracting the regions of the image that are consistent with the computed model of the target. But the present work adopts a competitive and efficient dynamic Kalman filtering to adaptively update the object model by adding new stable features as well as deleting inactive features. Reference [4] reads real

time monitoring video from communications department and converts it into images. After that, we change them into corresponding gray images and carry out image binarization with dynamic multiple thresholds method which selects thresholds depending on pixel, grayscale and pixel position. Here the system updates the background periodically background refreshing method. We also put forward an adaptive background subtraction method, which can remove noise, to identify the moving objects and get total movement in a given time.

A new approach is developed in [5], in order to track the vehicles, which is known as region processing. The regions may combine or break during the tracking due to mistakes in vehicle detection and tracking or vehicles overlapping with each other, so a method to overcome this effect is developed and accomplished. In this paper, a vehicle tracking method is proposed to reduce mistake in spatial segmentation. “Temporary vehicle”, “confirmed vehicle” and the corresponding judging rules are presented. A fuzzy judgment is proposed to determine whether vehicle overlapping occurs or not. Reference [6] presents a practical real-time traffic monitoring system based on object detection and tracking for measuring traffic parameters such as speed and volume. In the proposed system, background is modeled by using edge information and this model is used for extracting foreground moving objects. The advantage of using edge information to model the background is that it is more robust to the lighting variation. The extracted moving objects are then tracked by using Lukas-Kanade (Pyramid) optical flow algorithm. Only the successfully tracked vehicle will be considered for retrieving traffic information. In [7] a real time video surveillance is presented for traffic monitoring of vehicle volume on major highways. This paper deals with the determination of traffic volume automatically in real time to dynamically plan their trips more efficiently. A new method known as the virtual line analyzer detects vehicles as they cross the virtual boundary. The goal of this paper is to provide real time and accurate vehicle counter when using stationary web cams, fixed highways and lanes, and deterministic vehicle characteristics.

A real time system for pedestrian tracking in sequences of grayscale images acquired by a stationary camera is presented in [8]. The proposed scheme is also useful for the detection of several diverse tracking objects of interest. Blob tracking is modeled as a graph optimization problem. Pedestrians are modeled as dynamic rectangular patches. Kalman filtering is used in order to estimate pedestrian parameters. Disadvantage is that this system assumes that all objects in the scene are pedestrians. This means that if another object /vehicle appear into the scene, it will be treated as group of pedestrians.

A computer vision based approach for event detection and data collection at traffic intersections is proposed in [9]. It implements a robust tracking algorithm for targets through combination of multiple uses and multiple motion models. Also, event detection system using results of a switching Kalman filter in combination with some simple rules is implemented. The estimation is that the detected events are very simple based on simple rules for detection. The system makes no distinction between a target moving and stopped vehicle in the scene.

III. IMPLEMENTATION

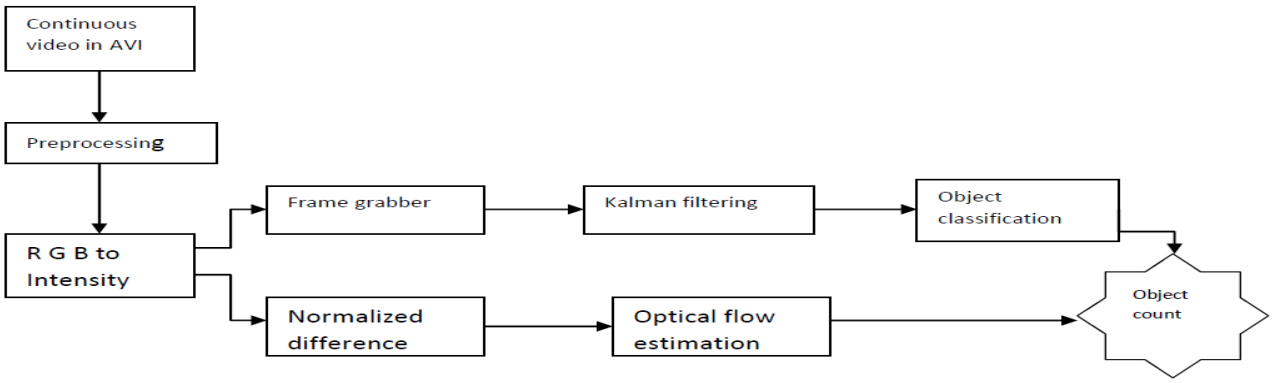


Fig.1: Block diagram representation of the developed system.

The methodology described above is followed and the computation is done .The whole procedure is represented by a block diagram as shown in Fig.1. The input to the system is video sequence which is in MPEG2 format.The video sequences are then converted into AVI format with the help of software. Then this is converted into frame vise using frame grabber software. Then a frame with no vehicle is taken and this is said to be a reference image which is then used for background subtraction. Continuous frames are sent so that the subtraction takes place within the reference image and the current image. Thus we accomplish the background subtraction via which we determine the object segmentation which is useful in classification of vehicles. Next this is passed through the Kalman filter. The state of the object is upgraded and thus it helps in the classification of vehicles. Pixel scanner is just acting like asensor. Initially while fixing pixel scanner, each and every pixels having different RGB values for different frames. Basically a pixel scanner line consisting of more than 100 pixels, once an object enters into the frame and when it passes through pixel scanner, there will be drastic changes in RGB values of the pixel until the object is in contact with the pixel scanner.

IV. OPTICAL FLOW

First the video is selected which is in avi format. then it is subjected to intensity form by converting its RGB into its respective intensity. Then this intensity is next converted into single image format where white pixel representation is obtained. To this the optical flow technique is implemented with which we get the velocity. The optical flow method used here is the Horn-schunk[10] method where the horizontal and vertical components are taken into consideration and the difference between them are calculated so that the velocity is determined. This velocity is then subjected to thresholding and median filtering where morphological features are extracted. This results with the motion vector. Thus the determination of optical flow is implemented. Further, the result is used for counting and classification of vehicles.

V. OBJECT RECOGNITION BY USING KALMAN FILTER

Here we need to maintain separate data base for each and every object, and it is totally depending upon your camera position that's related to your road. Object data base will vary according to distance between camera and main road, so accordingly we need to maintain an object data base.

Take an example: Two-wheeler

Distance between camera and road ==5m

Overall road width==10m

Total from camera position==15m

Suppose bike travelling in 10m distance from camera,

Assume that height==5cm

Width==7cm (by using keen observation)

Find area now,

Area A== (1/2)*height*width==17.5cm/sq

Now construct a rectangle of area between 15-20cm/sq by using kalman filter.

It means in between 15-20 we should suppose to maintain 10 or more than 10 rectangle areas in our background database. Then apply Kalman filter to each and every frames, find object areas and compare with backgrounds present in our data base, when it matches (not 100 percent) almost, then you can easily recognize a given object. Similarly you can do it for four-wheeler and heavy objects also. For object display operation we have taken a frame which is having much change in their almost all pixels RGB values which are all present in the pixel scanner line, and then algorithm can read that frame easily.

By using velocity vectors in optical flow, we can easily find out vehicle count by using pixel scanner line. Green value will increase once velocity vector reaches pixel scanner line.

VI. DIFFERENCE FILTER

1. Compute I_x and I_y using the kernel $[-1 \quad 8 \quad 0 \quad -8 \quad 1]/12$ and its transposed form.
   If you are working with fixed-point data types, the kernel values are signed fixed-point values with word length equal to 16 and fraction length equal to 15.
2. Compute I_t between images 1 and 2 using the $[-1 \quad 1]$ kernel.
3. Smooth the gradient components, I_x, I_y, and I_t, using a separable and isotropic 5-by-5 element kernel whose effective 1-D coefficients are $[1 \quad 4 \quad 6 \quad 4 \quad 1]/16$. If you are working with fixed-point data types, the kernel values are unsigned fixed-point values with word length equal to 8 and fraction length equal to 7.
4. Solve the 2-by-2 linear equations for each pixel using the following method:

- If $A = \begin{bmatrix} a & b \\ b & c \end{bmatrix} = \begin{bmatrix} \sum W^2 I_x^2 & \sum W^2 I_x I_y \\ \sum W^2 I_y I_x & \sum W^2 I_y^2 \end{bmatrix}$

Then the eigen values of A are $\lambda_i = \frac{a+c}{2} \pm \frac{\sqrt{4b^2 + (a-c)^2}}{2}; i = 1,2$

In the fixed-point diagrams, $\frac{a+c}{2}, Q = \frac{\sqrt{4b^2 + (a-c)^2}}{2}$

When the block finds the eigen values,it compares them to the threshold,that corresponds to the value you enter for the Threshold for noise reduction parameter. The results fall into one of the following cases: The Compute optical flow between, N, and Velocity output parameters are described in Horn-Schunck Method. Use the Threshold for noise reduction parameter to eliminate the effect of small movements between frames. The higher the number, the less small movements impact the optical flow calculation.

Case 1: $\lambda_1 \geq \tau$ and $\lambda_2 \geq \tau$

A is nonsingular, so the block solves the system of equations using Cramer's rule.

Case 2: $\lambda_1 \geq \tau$ and $\lambda_2 < \tau$

A is singular (noninvertible), so the block normalizes the gradient flow to calculate *u* and *v*.

Case 3: $\lambda_1 < \tau$ and $\lambda_2 < \tau$

The optical flow, *u* and *v*, is 0.

The Compute optical flow between, N, and Velocity output parameters are described in Horn-Schunck Method. Use the Threshold for noise reduction parameter to eliminate the effect of small movements between frames. The higher the number, the less small movements impact the optical flow calculation.

VII. DERIVATIVE OF GAUSSIAN

If you set the Temporal gradient filter parameter to Derivative of Gaussian, the block solves for *u* and*v* using the following steps. You can see the flow chart for this process at the end of this section:

i. Compute I_x and I_y using the following steps:
   a. Use a Gaussian filter to perform temporal filtering. Specify the temporal filter characteristics such as the standard deviation and number of filter coefficients using the Number of frames to buffer for temporal smoothing parameter.
   b. Use a Gaussian filter and the derivative of a Gaussian filter to smooth the image using spatial filtering. Specify the standard deviation and length of the image smoothing filter using the Standard deviation for image smoothing filter parameter.

ii. Compute I_t between images 1 and 2 using the following steps:
   a. Use the derivative of a Gaussian filter to perform temporal filtering. Specify the temporal filter characteristics such as the standard deviation and number of filter coefficients using the Number of frames to buffer for temporal smoothing parameter.
   b. Use the filter described in step 1b to perform spatial filtering on the output of the temporal filter.

iii. Smooth the gradient components, I_x, I_y, and I_t using a gradient smoothing filter. Us
Standard deviation for gradient smoothing filter parameter to specify the standard de
the number of filter coefficients for the gradient smoothing filter.

iv. Solve the 2-by-2 linear equations for each pixel using the following method:

If $$A=\begin{bmatrix} a & b \\ b & c \end{bmatrix}=\begin{bmatrix} \sum W^2 I_x^2 & \sum W^2 I_x I_y \\ \sum W^2 I_y I_x & \sum W^2 I_y^2 \end{bmatrix}$$

Then the eigenvalues of A are

$$\lambda_i = \frac{a+c}{2} \pm \frac{\sqrt{4b^2+(a-c)^2}}{2}; i=1,2$$

When the block finds the eigenvalues, it compares them to the threshold, that corresponds to the value you enter for the Threshold for noise reduction parameter. The results fall into one of the following cases:

Case 1: $\lambda_1 \geq \tau$ and $\lambda_2 \geq \tau$

A is nonsingular, so the block solves the system of equations using Cramer's rule.

Case 2: $\lambda_1 \geq \tau$ and $\lambda_2 < \tau$

A is singular (noninvertible), so the block normalizes the gradient flow to calculate *u* and *v*.

Case 3: $\lambda_1 < \tau$ and $\lambda_2 < \tau$

The optical flow, *u* and *v*, is 0.

Select the Discard normal flow estimates when constraint equation is ill-conditioned check box if it is required that the block to set the motion vector to zero when the optical flow constraint equation is ill-conditioned. The block calculates these motion vectors on a pixel-by-pixel basis.
Select the Output image corresponding to motion vectors (accounts for block delay) check box if required that the block to output the image that corresponds to the motion vector being output by the block.

VIII. ALGORITHM

Initially algorithm will read continuous movie in AVI format by using MATLAB, then we will separate out the frames by using frame grabber. In the next stage we need to check each and every frame for object recognition. So we can introduce a diagonal pixel scanner to identify the objects. Pixel scanner is just acting like a sensor. Initially while fixing pixel scanner, each and every pixels having different RGB values for different frames. Basically a pixel scanner line consisting of more than 100 pixels, once an object enters into the frame and when it passes through pixel scanner, there will be drastic changes in RGB values of the pixel until the object is in contact with the pixel scanner. Now we can consider output of pixel scanner lines, I mean RGB values of each and every pixels present in the pixel scanner.

Following are the steps involved:

i. Pixel 1: initial RGB value=30, 20, 10….when there is no object present in the scene
ii. Changed R1G1B1 values= 220, 110, 80….presence of object in the scene.
iii. Subtract RGB from R1G1B1
iv. Initialize counter……c==0
v. If (R1G1B1-RGB) is greater than or equal to (10,10,10)====increment count
Count ==c+1:
Else
Count==c:
End
vi. Display the result of object counting.

Object Recognition By Using Kalman Filter

At this level of analysis it is needed to maintain separate data base for each and every object, and it's totally depending upon your camera position that's related to your road. Object data base will vary according to distance between camera and main road, so accordingly we need to maintain an object data base.

Specific Identifier

Two-wheeler
Distance between camera and road ==5m
Overall road width==10m
Total from camera position==15m
Suppose bike travelling in 10m distance from camera,
Assume that height==5cm
Width==7cm (by using keen observation)
Find area now,
Area A== (1/2)*height*width==17.5cm/sq
Now construct a rectangle of area between 15-20cm/sq by using Kalman filter.
It means in between 15-20 we should suppose to maintain 10 or more than 10 rectangle areas in our background database. Then apply Kalman filter to each andevery frames, find object areas and compare with backgrounds present in our data base, when it matches (not 100 percent) almost, then you can easily recognize a given object. Similarly you can do it for four-wheeler and heavy objects also.
For object display operation we have taken a frame which is having much changes in their almost all pixels RGB values which are all present in the pixel scanner line, then you can read that frame easily.
By using velocity vectors in optical flow, we can easily find out vehicle count by using pixel scanner line. Green value will increase once velocity vector reaches pixel scanner line.

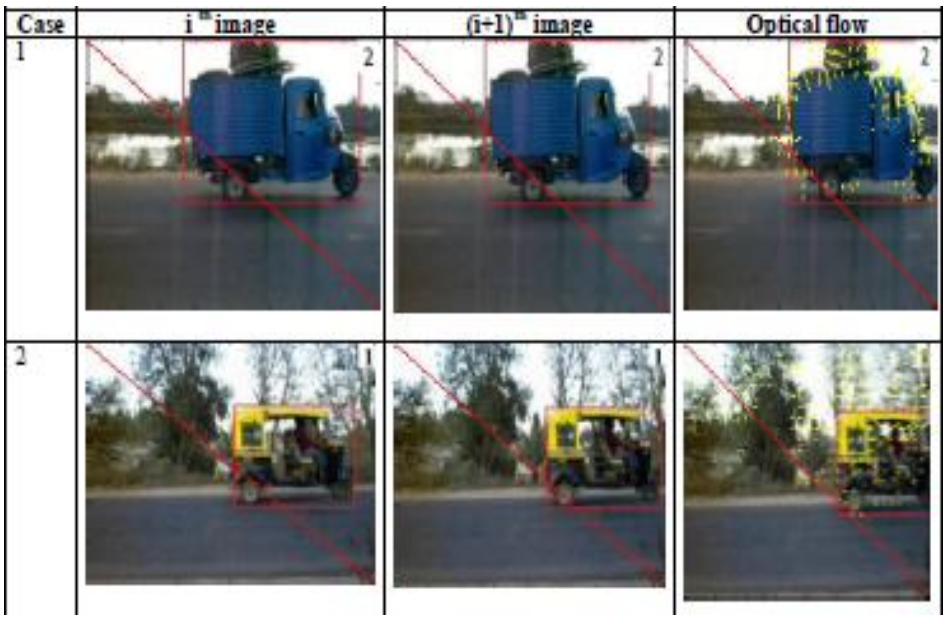
Table 1: Tabulates results achieved for different natural video steams

	Actual Classification	Count	Estimated Classification	Count	Error	Accuracy
Case1	Two wheeler	1	Two wheeler	1	0	100%
	Four wheeler	4	Four wheeler	4	0	100%
	Heavy vehicles	3	Heavy vehicles	3	0	100%
	Total	8	Total	8	0	100%
Case2	Two wheeler	4	Two wheeler	1	0	100%
	Four wheeler	4	Four wheeler	1	0	100%
	Heavy vehicles	1	Heavy vehicles	1	0	100%
	Total	9	Total	9	0	100%
Case3	Two wheeler	7	Two wheeler	6	0	85.71%
	Four wheeler	5	Four wheeler	5	0	100%
	Heavy vehicles	2	Heavy vehicles	2	0	100%
	Total	14	Total	13	0	95.12%
Case 4	Two wheeler	4	Two wheeler	0	0	100%
	Four wheeler	3	Four wheeler	3	1	100%
	Heavy vehicles	2	Heavy vehicles	6	0	100%
	Total	9	Total	9	1	100%
Average					**1.6**	**98.78%**

IX. PRESENTATION OF RESULTS

In order to test the proposed algorithm, several sets of natural image sequences have been used. Real image sequences, recorded in MPEG2 format have been used with camera, in fixed position to capture the aerial view of the road. Different natural traffic videos are taken in situations where obstacles are found in the line of view, vehicle shadows, building shadows in the path and oblique view of the traffic. The first set of images is taken in order to establish the reference images under different illumination condition from morning till evening. Four such reference frames have been identified for experimentation.

In the present work, a platform has been created so that complete automation of dynamic and intelligent traffic control devoid the human intervention. Monocular camera with fixed resolution of 1024X1024 with a frame rate of 30 is used to acquire the data. The present algorithm translates image size 1024X1024 to 200X200 in order to reduce the computational complexity. Table.1 showcases the result established through the implementation of the present algorithm.



Optical Flow Estimation

Fig.2-Display of results of optical flow needle diagram for different vehicles

Display of results of optical flow needle diagram for different vehicles is as shown in Fig.2. The needle diagram clearly indicates the direction of movement of the vehicle. Hence, bidirectional vehicular movement analysis is achieved apart from counting and classification of vehicles..

Reslts Presentation: Object Counting By Using Kalman Filter

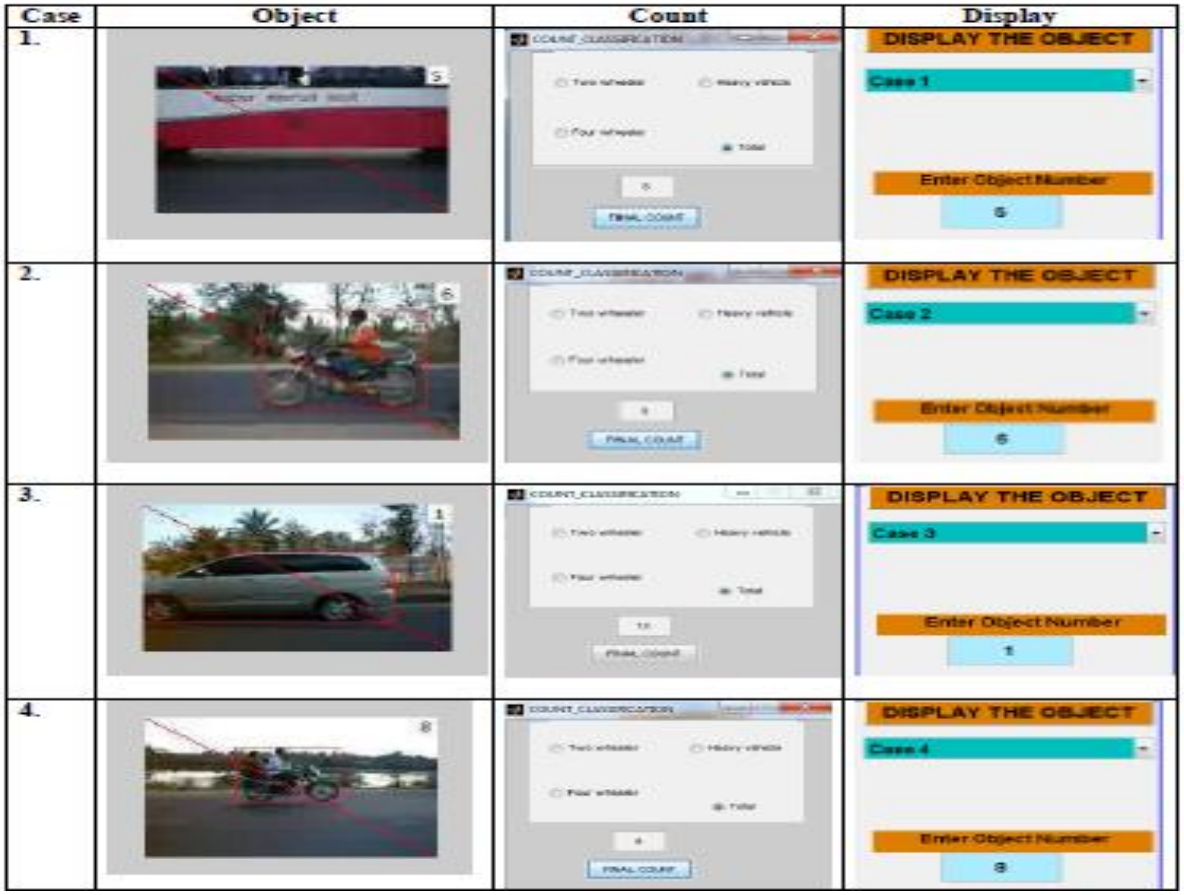


Fig.3

Display of results of Kalman filter for different vehicles.

The classification of vehicles based on Kalman filter is showcased in Fig.3. The result presentation consists of the vehicle count, its sequence of appearance and type. It also provides the insight to the frame number at which each vehicle passed though the geometric center of the frame.

X. Conclusion

The result established is consistent with good repeatability. The system developed consider output of pixel scanner lines, it means that RGB values of each and every pixels present in the pixel scanner. We also notice that the proposed method fails if the traffic is too congested, because in this case, vehicles may overlap from the beginning to the end, or more than two vehicles are overlapped with each other, so it is difficult to distinguish each of the vehicles. The Optical Flow block estimates the direction and speed of object motion from one image to another or from one video frame to another using either the Horn-Schunck or the Lucas-Kanade method in order to verify the result.

XI. References

1) Ching-Po Lin, Jen-.Chao Tai and Kai-Tai Song, "Traffic Monitoring Based On Real Time Image Tracking", IEEE International Conference on Robotics and automation,pp2091-96,2003.
2) Feng Yi-wei, Guo Ge ,Zhu Chao-qun, "Object Tracking By Kalman Filtering And ecursive Least Squares based On 2D Image Motion", IEEE International Conference on Computational Intelligence and Design,pp106-109,2008.
3) Gang-Yi Jiang, Mei Yu, Sheng-Nan Wang, Rang-Ding Wang, "New Approach To Vehicle Tracking Based On Region Processing", IEEE International Conference on Machine learning and Cybernetics, pp5028-33,2005.
4) Kiratiratanapruk K. and Supakorn Siddhichai, "Practical Application for Vision-Based Traffic Monitoring System", 978-1-4244-3388-9,2009.
5) Fei Zhu, " A Video-Based Traffic Congestion Monitoring System Using Adaptive Background

Subtraction", Second International Symposium on Electronic Commerce and Security, pp73-77,2009.

6) Belle L. Tseng, Ching-Yung Lin and John R. Smith, "Real-Time Video Surveillance For Traffic Monitoring Using Virtual Line Analysis", IEEE 0-7803-7309-9, pp541-544,2002.
7) R. Cucchiara, M. Piccardi, and P. Mello, "Image analysis and rule-based reasoning for a traffic monitoring system," IEEE Transactions on Intelligent Transportation System., vol. 1, no. 2, pp. 119–130, Jun. 2000.
8) Osama Masoud and Nikolas P.Papanikolopoulos, "A Novel method for tracking and counting pedestrians in Real time using a single camera", IEEE Transactions on Vehicular Technology ,Volume 50, no.5,sept 2001.
9) Harini Veeraraghavan, Paul Schrater and Nikolas Papanikolopoulos, "Switching Kalman filter-Based approach for Tracking and Event Detection at Traffic Intersection", IEEEInternational conference on control and Automation , pp. 1167-1172, 2005.
10) B.K.P. Horn and B.G. Schunck, " Determining optical flow", Artificial Intelligence, 17; 185-203,1981.

HybridAlgorithm Approach To Job Shop Scheduling Problem

Ye Li[1], [2], Yan Chen[2]

GJCST Classification
D.4.1

[1]Electronic and Information College, Dalian University of Technology, Dalian,China 116026
[2.] Transportation Management College, Dalian Maritime University, Dalian,China 116026
liye_dlmu@sohu.com

***Abstract*- In this paper, we analyze the characteristics of the dynamic job shop scheduling problem when machine breakdown and new job arrivals occur. A hybrid approach involving neural networks(NNs) and geneticalgorithm(GA) is presented to solve the dynamic job shop scheduling problem as a static scheduling problem. The objective of this kind of job shop scheduling problem is minimizing the completion time of all the jobs, called the makespan, subject to the constraints.The result shows that the hybrid methodology which has been successfully applied to the static shop scheduling problems can be also applied to solve the dynamic shop scheduling problem efficiency.**

Keywords- dynamic job shop, neural network, genetic algorithm, hybrid methodology, makespan

I. INTRODUCTION

Job shop scheduling(JSP) is usually a strongly NP complete problem of combinatorial optimization problems and is the most typical one of the production scheduling problems[1,2].Unfortunately, most publication in shop scheduling area focuses on the static shop scheduling. Very few of them suggest a comprehensive model and solution to the dynamically job shop problem[3,4].To deal with dynamic scheduling, most researches usually partition the scheduling process into two phases. In Phase 1, they consider the optimization of makespan under idealized conditions; then in Phase 2, they simply deal with reactive scheduling based on some scheduling rules, in case of accidental disturbance. Muhleman et al analyzed the periodic scheduling policy in a dynamic and stochastic job shop system. Their experiments indicated that more frequent revision was needed to obtain better scheduling performance[5]. Church and Uzsoy considered periodic and event-driven rescheduling approaches in a single machine production system with dynamic job arrivals. Their result indicated that the performance of periodic scheduling deteriorate as the length of rescheduling period increased and event-driven methods achieved a reasonably good performance[6]. Subramaniam et al demonstrated that significant improvements to the performance of dispatching in a dynamic job shop could be achieved easily through the use of simple machine selection rules[7].SQ. Liu et al presented a framework to model dynamic shop scheduling problem. Using the proposed framework, a metaheuristic was proposed to solve dynamic shop problem. The result showed that the metaheuristic methodology which had been applied to solve dynamic shop scheduling problem efficiently[8]. Borstjan andPeter proposed an alternativeway to avoid infeasibility by incorporating a repairing technique into the mechanism for applying moves to aschedule. Whenever an infeasible move was being applied, a repairing mechanism rearranged the underlying schedule insuch a way that the feasibility of the move was restored. The possibility of reaching infeasible solutions was, therefore,eliminated on the lowest possible conceptual level[9]. Hiroshi and Toshihiro considered the jobshop scheduling problem of minimizing the total holding cost of completed andin-process products subject to no tardy jobs. A heuristic algorithm based on the shifting bottleneck procedure waspropose for solving the minimum total holding cost problem subject to no tardy jobs. Several benchmark problemswhich were commonly used for job-shop scheduling problems of minimizing the makespanwere solved by the proposedmethod and the results were reported[10].

Recently, much attention has been paid to applying neural networks or genetic algorithms et al to production scheduling problems. Haibin Yu et al presented neural network and genetic algorithm to solve the expand job shop problem. The GA was used for optimization of sequence and NN was used for optimization of operation start times with a fixed sequence. New type of neurons were defined to construct neural network(CNN). The neurons can represent processing restrictions and resolve constraint conflicts. Combining gradient CNN with GA for sequence optimization, a hybrid approach was put forward. The approach had been tested by a large number of simulation cases and practical applications. It had been shown that the hybrid approach was powerful for complex JSP[11]. Shengxiang Yang et al presented a new adaptive neural network and heuristics hybrid approach for job shop scheduling. One heuristic was used to accelerate the solving process of neural network and guarantee its convergence; the other heuristic was used to obtain non-delay schedules from the feasible solutions gained by neural network. Computer simulations had shown that the proposed hybrid approach was of high speed and efficiency[12]. Hong Zhou and Yuncheng Feng proposed a hybrid heuristics method for $n/m/G/C_{\max}$, where the scheduling rules, such as shortest processing time(SPT) and MWKR, were integrated into the process of genetic evolution. In addition, the neighborhood search technique was adopted as an auxiliary

procedure to improve the solution performance[13]. Byung developed an efficient method based on genetic algorithm to address JSP. The scheduling method based on single genetic algorithm and parallel genetic algorithm was designed. In the scheduling method, the initial population was generated through integrating representation and G&T algorithm, the new genetic operators and selection method were designed to better transmit the temporal relationships in the chromosome, and island model PGA were proposed[14]. Dirk and Christian considered a job shop scheduling problems with release and due-dates, as well as various tardiness objectives. The genetic algorithm can be applied to solve this kind of problem. The heuristic reduction of search space can help the algorithm to find better solution in a shorter computation time[15]. Jose presented a hybrid genetic algorithm for job shop scheduling problem. The chromosome representation of the problem was based on random keys. The schedules were constructed using a priority rule in which the priorities were defined by the genetic algorithm. Schedules were constructed using a procedure that generates parameterized active schedules. After a schedule was obtained a local search heuristic that was applied to improve the solution[16]. Guo proposed a universal mathematic model of the JSP problem for apparel assembly process. The objective of this model was to minimize the total penalties of earliness and tardiness by deciding when to start each order‘s production and how to assign the operations to machine. A genetic optimization process was then presented to solve this model. In which a new chromosome representation, a heuristic initialization process and modified crossover and mutation operators were proposed[17]. Masato and Kenichiproposed the modified geneticalgorithm with search area adaptation (mGSA) for solving the jobshop scheduling problem. To show the effectiveness of the proposed method that conducted numerical experiments by using two benchmark problems. It was shown that this method had betterperformance than existing GAs[18].Young Su Yun proposed a new genetic algorithm (GA) with fuzzy logic controller (FLC) for dealing withpreemptive job-shop scheduling problems (p-JSP) and non-preemptive job-shop scheduling problems (np-JSP).The proposed algorithm considered the preemptive cases of activities among jobs under single machine schedulingproblems. For thesepreemptive cases, they first used constraint programming and secondly developed a new generepresentation method, a new crossover and mutation operators in the proposed algorithm[19].

In those papers, most publications in job shop scheduling area focus on the static shop scheduling problems and seldom takes into account the dynamic disturbance such as machine breakdown and new job arrivals. In this paper, a university mathematical model for dynamic job shop scheduling problem is constructed. The objective of this model is to minimize makespan. In order to solve this mixed- and multi-product scheduling problem, a combinationof a genetic algorithm and a neural network is used to find the optimal solution. The Back-Propagation Neural Network(BPNN) is designed to describe machine breakdown and new job arrivals etc, detecting whether constraints are satisfied and resolving the conflicts by their feedback adjustments. Then the BPNN can generate a feasible solution for the JSP. For sequence optimization and makespan, a GA is employed. The algorithm will then be used to solve the JSP problem of 10 working procedure and10 machines. Though the simulation, it is shown that the approach can be used to model real production scheduling problems and to efficiency find an optimal solution.

II. MODELING THE JOB-SHOP SCHEDULING PROBLEM

In a JSP we have a set N of jobs, $N = \{1,...,n\}$, that have to be processed in a set M of stages, $M = \{1,...,m\}$. At each stage i, $i \in M$ we have a set $M_i = \{1,...,m_i\}$ of unrelated parallel machines that can process the jobs where $m_i \geq 1$. We consider the dynamic job shop case where stages might be skipped. Every job is a chain of operations and every operation has to be processed on a given machine for a given time. The task is to find the completion time of the very last operation is minimal. The chain order of each job has to be maintained and each machine can only process one job at the same time. Once an operation starts, it must be completed; two operations of a job can not be processed at the same time; no more than one job can be handled on a machine at the same time; the same priority level at each operation; there is no setup and idle time; the money value is not considered. The following additional definitions and notations will help in formulating the problem:

i. i : number ofmachines, $i \in \{1, 2, \ldots, m\}$;

ii. j_i : number of operations of machine i, $j \in \{1,2,\ldots,n\}$;

iii. p_{ij} : processing time of operation j on machine i; $i \in \{1, 2,\ldots, m\}$, $j \in \{1,2,\ldots,n\}$;

iv. o_j : sequence and technique restriction of job j ,such as job j passing though machine sequence = $(o_{j1}, o_{j2}, \cdots, o_{jn})$, $o_{ij} \in \{1,2,\cdots,m\}$, $i \in \{1, 2, \cdots, m\}$, $j \in \{1, 2, \cdots, n\}$;

v. t_{ij} : starting time of operation j on machine i;

vi. t_j : completion time of operation j.

vii. $$X_{ijk} = \begin{cases} 1 & \text{if operation } j \text{ precedes operation } k \\ 0 & \text{otherwise} \end{cases}$$

viii. $$z_{ij} = \begin{cases} 1 & \text{if operation } j \text{ is allocated on machine } i \\ 0 & \text{otherwise} \end{cases}$$

ix. C_{ij} : the completion time of operation j on machine i

x. $C_{\max}$: makespan, at the end of the production step, is thus of its final operation o_j .

According to above suggestion, parameter and decision variable of problem, the mathematical model is identified as followed:

$$\min C_{\max}$$

$$s.t$$

$$\sum_{j=1}^{n} z_{ij} = 1$$

$$\sum_{j=1, j\neq k}^{n} \sum_{i=1}^{m} X_{ijk} = 1$$

$$t_{ij} + p_{ij} \leq t_{i+1,j}$$

$$t_{ij} + p_{ij} \leq t_{ik} + (1 - X_{ijk})M$$

$$\sum_{i=1}^{m} \sum_{j=1}^{n} (X_{ijk} + X_{ikj}) \leq 1$$

The objective function is to minimize the maximum completion time (makespan). In a job shop environment, how should the jobs be scheduled and how should they be rescheduled when dynamic events occur, so that the makespan is dynamically minimize? In this study, we restrict our attention to two dynamic factors, the machine breakdown and new job arrivals only.

III. BPNN MODEL

Artificial neural networks are parallel computationaldevices consisting of groups of highlyinterconnected processing elements called neurons. Neurons are basic elements of BPNN. Acommon neural cell or neuron is defined by linearly weighted summation of its input signals, and serially connected non-linear activity function $F(T_i)$.

$$T_i = \sum_{j=1}^{n} (W_{ij} X_j) \; Y_i = F(T_i) \; T_i(k+1) = T_i(k) + Y_i(k)$$

where W_{ij} is the connection weight of the j th input signal X_j and the i th neuron. T_i is the weighted summation of the i th neuron. $F(T_i)$ is the activity function and Y_i is the output of the i th neuron.Links among neurons are through their weights. They represent the scheduling restriction. They also reflect the adaptation or adjustment to resolve constraint conflicts through proper feedback links, when restrictions are not met. The working orderand start time etc are used as input nodes, and the feedback represents iterative adjustment, and the breakdown and new job arrivals etc are used as output nodes.

In the event of machine breakdown, two scenarios should be resume or the entire job to be taken out from the schedule. For the first case, the unfinished operation usually has priority to be processed first when the machine has been repaired, considering the set up time or other realistic. For the second case, the affected job should be taken out either to be discarded or processed offline. We consider the first case.

To solve the job shop scheduling problem, the BPNN is adopted that can generate a feasible solution. x_1 represents input node, and y_1 represents output node. For example, $x_1 = 0$ represents that all machines are working order, otherwise $x_1 = 1$. $x_2 = 0$ represents that the start time of each operation is above or equal to 0, otherwise $x_2 = 1$. $x_3 = 0$ represents that all the job is processed, otherwise $x_3 = 1$. $y_1 = 0$ represents that new job arrivals don't occur, otherwise $y_1 = 1$. $y_2 = 0$ represents that the machine don't break down, otherwise $y_2 = 1$. $y_3 = 0$ represents that due dates isn't tardiness, otherwise $y_3 = 1$. $y_4 = 0$ represents X_{ijk}, otherwise $y_4 = 1$. $y_5 = 0$ represents z_{ij}, otherwise $y_4 = 1$.

According to built BPNN, it has three input neurons and five output neurons and six hidden neurons. The training sample is as table 1.

Table 1: some BPNN training sample

Sample number	input			output				
	x1	x2	x3	y1	y2	y3	y4	y5
1	0	1	0	0	0	1	0	0
2	0	0	0	1	0	0	0	0
3	1	0	0	0	0	0	0	0
4	0	0	1	0	0	0	0	1

IV. DESCRIPTION OF GA AND BPNN MODEL

This section first gives out the description of two models, which are used to improve the performance of job shop scheduling problem. One is BPNN that is used to accelerate the solving process of JSP and guarantee feasible solution, the other is GA that is used to obtain the global optimal solution from feasible solution with determined order of operations. The BPNN model is set three levels, which I_i is

The $i's$ input ofinput layer and H_i is output of hidden layer and O_i is output of output layer. So WIH_{ij} is weight between input layer and hidden layer and WHO_{ji} is weight between hidden layer and output layer. Secondly the algorithm of hybrid approach of BPNN and GA for job shop scheduling problem is presented as follows:

Step 1-Initialization population P is generated, which is include probability of crossover P_c andprobability of mutation P_m and initializing WIH_{ij} and WHO_{ji}. Real coding is adopted, and initial population is 30.

```
for i=1:10
L=M(i,:);
for j=1:10
L(j)=L(j)+1;
end
M(i,:)=L;
end
NIND=40;
MAXGEN=        200;
GGAP=0.9;
XOVR=0.8;
MUTR=0.6;
[R,Q]=size(P);
[S2,Q]=size(O);
S1=6;
S=R*S1+S1*S2+S1+S2;
```

Step 2-The fitness is defined and sort order, and network individual is selected as the following probability

$$p = f_i / \sum_{i=1}^{N} f_i$$

Then f_i is adaptive value of individual i, and evaluated by error sum of squares.

$$f(i) = 1/E(i) \qquad E(i) = \sum_p \sum_k (V_k - T_k)^2$$

```
FitnV=ranking(ObjV);
SelCh=select('sus', Chrom, FitnV, GGAP);
SelCh=across(SelCh,NIND*GGAP,XOVR,WNumber);
SelCh=aberrance(SelCh,NIND*GGAP,M
      UTR,WNumber); disp_fqre=100;
      max_epoch=3000;err_goal=0.002;lr
      =0.01;
TP=[disp_fqre max_epoch err_goal
lr];[W1,B1,W2,B2,te,tr]=trainbp(W1,B1,'tansig',W2,B2,'pur
      elin',P,O,TP);
```

Step 3-The crossover is operated in the population G_i *and* G_{i+1} according to probability of crossover Pc, so the offspring G_i' *and* G_{i+1}' are generated.

Step 4-The individual G_j is selected randomly according to probability of mutation Pm, so the offspring G_j' is generated.

```
[PVal                                  ObjVSel
N]=cal(SelCh,NIND*GGAP,T,M,PNumber,MNumber,WP
Number);      [Chrom ObjV] =reins(Chrom, SelCh,1, 1,
ObjV, ObjVSel);
[PVal                                  ObjVl
N]=cal(Chrom,NIND,T,M,PNumber,MNumber,WPNumber
);
```

Step 5-

```
if gen==1
   Val1=PVal;
   Val2=N;
   MinVal=min(ObjV);
   end
```

Step 6-If the optimal solution is obtained, stopping the program and the best solution is output, otherwisegoing back to step3.

V. SIMULATION STUDY

We take the benchmark $10/10/J/C_{\max}$ problem. The simulation is finished under Matlab environment. Through 200 epochs searching, the fitness goes stabilization. The sum squared error and fitness curve are showed in figure 1.

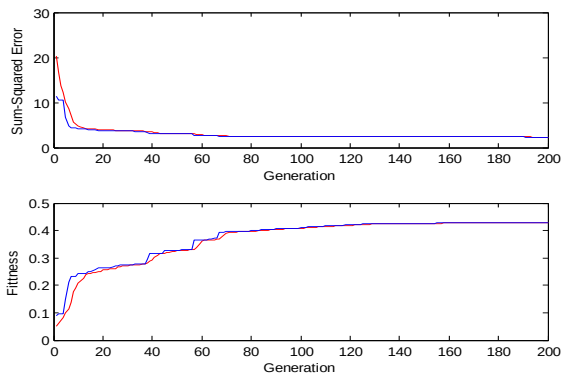


Figure 1:sum-squared error and fitness curve

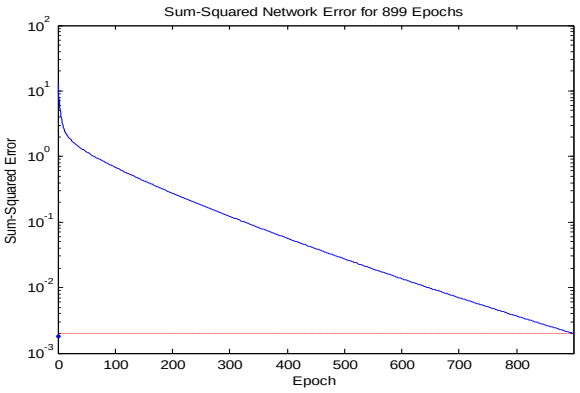


Figure 2: sum-squared network error of BP algorithm

The result of simulation is as follows:[0.0004,0.9930,0.0054,0.0015;0.0013, -0.0036,0.0008,0.0011;0.9998,0.0110,-0.0074,-0.0032;0.0006,-0.0302,0.0230,0.0069;-0.0015, 0.0123, -0.0080,0.9973]. So the idea output is [0 1 0 0;0 0 0 0;1 0 0 0;0 0 0 0;0 0 0 1], and the runtime is 10.6750 seconds.

The sum-squared network error of BP algorithm is showed in figure 2.The error objective is 0.002, and learn rate is 0.01.From the figure, the error objective is convergence to 0.02 when the BPNN algorithm run 899 epochs and the runtime is 13.690000 seconds.

Although the idea result is gotten by weight ofNN that is trained by GA from the above comparing, it takes longtime comparing with BPNN algorithm. Because GA is convergence by heuristic searching such as method of exhaustion, in addition, the complexity of network structure anda large amount of calculated data. For example, the weight of BPNN and threshold number is 58, and the thirty populations are 1740.Such number will be coding, decoding, crossover and mutation, and the dealt data is much greatness. So the searching time is longer. Considering the BPNN is accuracy to seek optimal solution, but it traps into local optimizationeasily. The GA has global searching capacity, and we could combine the GA with BPNN, which show each advantage.

A. Ga-Bp Algorithm

The principle of GA-BP algorithm is the optimal initial value is inherited by GA that focuses at the random position firstly, which is as the initial weight of BPNN. Secondly, it is trained by BPNN.

i. The algorithm of hybrid approach for job shop scheduling problem is presented as follows:

Step 1- 5: The same as above, which is NN that is trained by GA

Step 6: The sum squared error is calculated. If the predetermined value(εGA) is obtained, going to step 7, otherwise going back to step 3

Step 7: The optimal initial value is inherited as the initial weight of BPNNby GA. It is trained by BPNN till the predetermined precision $\varepsilon_{BP}(\varepsilon_{BP}<\varepsilon_{GA})$ is gotten.

B. Experiment result

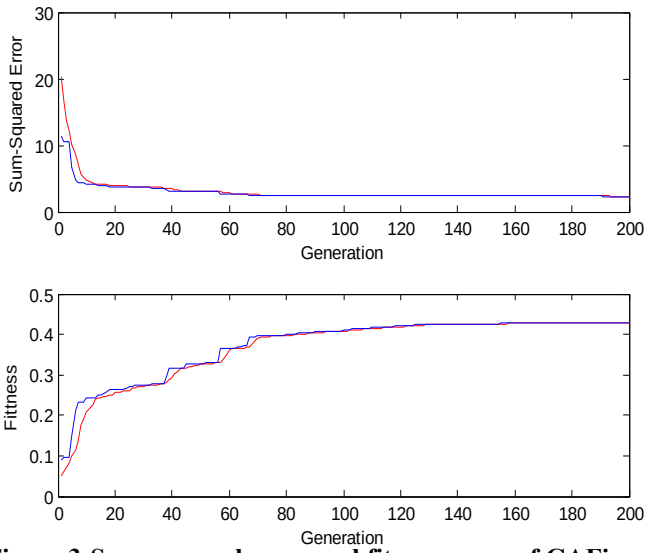


Figure 3:Sum-squared error and fitness curve of GA

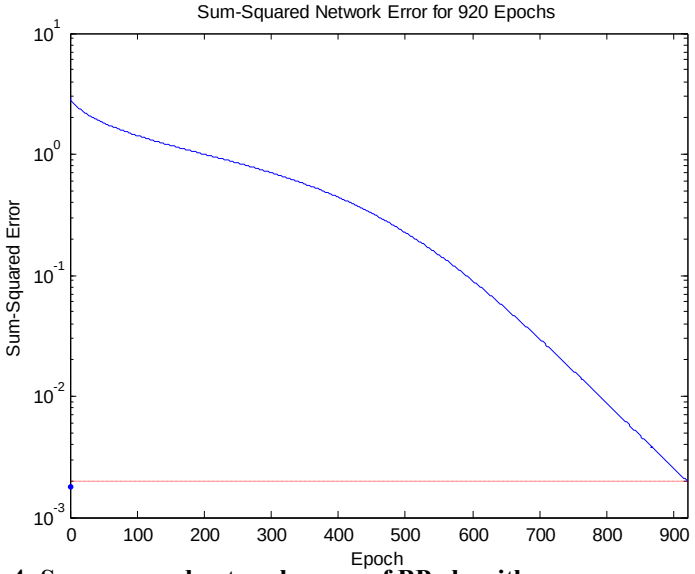


Figure 4: Sum-squared network error of BP algorithm

The sum squared error and fitness curve of GA are showedfrom figure 3, and the training objective of BPNN is showed from figure 4. We set initial population of GA is 30, and predetermined value is 5. The result of simulation is as follows:[0.0115,0.9647,0.0097,0.0114;0.0039,-0.0018,0.0007,0.0034;1.0025,-0.0076,-0.0034,0.0042;-0.0007,-0.008,0.0041,0.0037;-0.0073, 0.0081, -0.0059,1.0039]. So the idea output is [0 1 0 0;0 0 0 0;1 0 0 0;0 0 0 0;0 0 0 1], and the runtime is 5.739000 seconds.

The objective value is obtained through 80 epochs by GA, and the predetermined precision is convergence by 920 epochs. The run time is 18.326. It is obviously that the GA-BP algorithm is better than BP algorithm that is in convergence rate andRuntime.

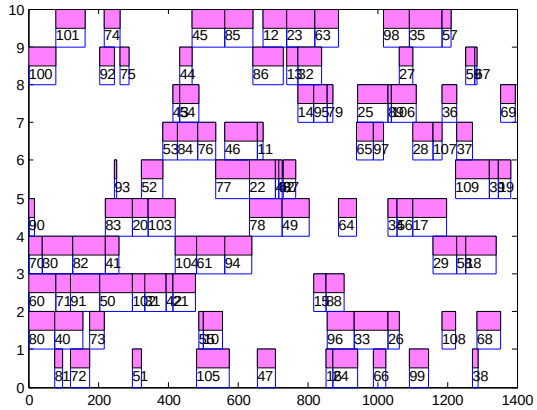


Figure 5: Gantts chart of JSP

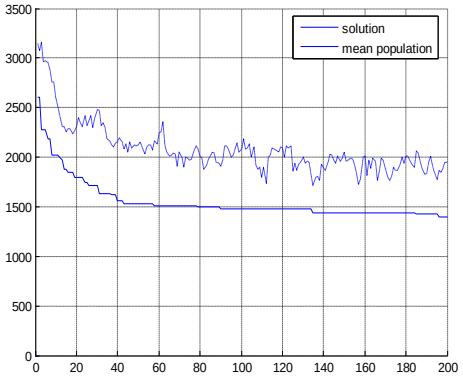


Figure 6:The solution and population curve

The result shows the sequence of each job, and makespan is 1395 from figure 5. The makespan is attained 1395, when the iterative number is 80, and the mean population is randomfrom the figure

VI. . Conclusion

In this paper, we analyze the characteristics of the dynamic job shop scheduling problem, and present a new hybrid approach, combining the BPNN with GA for solving when machine breakdown and new job arrivals occur.The BPNN is used to obtain feasible solution during the iterations. In order to overcome the shortcomings that BP algorithm is usually trapped to a local optimum and it has a low speed of convergence weights. The GA is adapted to the globe optimal searching. This algorithm can effectively and reliably be used in JSP problem. Simulation has shown that the proposed hybrid approach for JSP has excellent performance with respect to the quality of solution and speed of calculation.

VII. Reference

1) HeinzGroflin,Andreas Klinkert. Feasible insertions in job shop scheduling,Short-cycles and stable sets. European Journal of Operational Research, 177(2),2007: 763–785
2) Gerhard J. Woeginger. Inapproximability results for no-wait job shop scheduling. Operations Research Letters, 32(4), 2004: 320–325
3) Liu SQ, Ong HL. A comparative study of algorithms for the flowshop scheduling problems. Asia-Pacific J Operation Research, 19(2),2002: 205-222
4) Wein LM, Chevalier PB. A broader view of the job shop scheduling problem. The Institute of ManagementSciences, 38(7), 1992: 1018-1033
5) Muhleman AP, Lockett AG, Farn CK. Job shop scheduling heuristics and frequency of scheduling. *Int J Production Research*, 20(2), 1982: 227-241
6) Church LK, Uzsoy R. Analysis of periodic and event-driven rescheduling policies in dynamic shops.*Int J Computer Integrated Manufacturing*, 5(3), 1992:153-163
7) Subramaniam V, Lee GK et al. Machine selection rules in a dynamic shop. Int J Advanced Manufacturing Technology, 16(1), 2000:902-908
8) SQ Liu, HL Ong, KM Ng. Metaheuristics for minimizing the makespan of the dynamic shop scheduling problem. Advances in Engineering Software, 36(3), 2005: 199-205
9) Bortjan Murovec, Peter Suhel. A repairing technique for the local searchof the job-shop problem.European Journal of Operational Research, 153(1), 2004:220-238
10) Hiroshi Ohta, Toshihiro Nakatani. A heuristic job-shop scheduling algorithm to minimize thetotal holding cost of completed and in-process productssubject to no tardy jobs. International Journal Production Economics,101(1), 2006:19–29
11) Habin Yu, Wei Liang. Neural network and genetic algorithm-based hybrid approach to expanded job-shop scheduling.Computers & Industrial Engineering, 39(3-4), 2001: 337-356
12) Shengxiang Yang, Dingwei Wang. A new adaptive neural network and heuristics hybrid approach for job-shopscheduling. Computer & Operations Research, 28(10), 2001: 955-971
13) Hong Zhou, Yuncheng Feng, Limin Han. The hybrid heuristic genetic algorithm for job shop scheduling.Computers & Industrial Engineering, 40(3), 2001: 191-200
14) Byung Joo Park, Hyung Rim Choi, Hyun Soo Kim. A hybrid genetic algorithm for the job shop scheduling problem.*Computers & Industrial Engineering*, 45(4), 2003:597-613
15) Dirk C. Mattfeld, Christian Bierwirth. An Efficient Genetic Algorithm for Job Shop Scheduling with Tardiness Objectives. European Journal of Operational Research, 155(3), 2004: 616-630
16) Jose Fernando Goncalves, Jorge Mendes, Mauricio Resende. A Hybrid Genetic Algorithm for the Job Shop Scheduling Problem. *European Journal of Operational Research*, 167(1), 2005: 77-95

17) Z.X Guo, W.K Wong, S.Y Leung et al. Mathematical Model and Genetic Optimization for the Job Shop Scheduling Problem in a Mixed- and Multi-Product Assembly Environment: A Case Study Based on the Apparel Industry. Computers & Industrial Engineering, 50(3), 2006:202-219
18) Masato Watanabea, Kenichi Ida, Mitsuo Gen. A genetic algorithm with modified crossover operator and searcharea adaptation for the job-shop scheduling problem. *Computers & Industrial Engineering*, 48(4), 2005: 743-752
19) Young Su Yun. Genetic algorithm with fuzzy logic controller for preemptive andnon-preemptive job-shop scheduling problems.Computers & Industrial Engineering, 43(3), 2002: 623-644

Security Provision For Mobile Ad-Hoc Networks Using Ntp & Fuzzy Logic Techniques

GJCST Classification
C.2.1.I.2.3

[1]Suresh Kumar [2]Machha.Narender, [3]G.N.Ramesh

[1]Assistant Professor MLEngg College. Sureshkumar1239@gmail.com
[2]Assistant Professor HITS College of Engg,machha.narender@gmail.com.
[3]Assistant Professor Bhoj Reddy Engg College, noya.ramesh@gmail.com.

***Abstract*-Ad-hoc Networks are a new generation of networks offeringunrestricted mobility without any underlying infrastructure.Primary applications of Ad-hoc networks are in military, tacticaland other security sensitive operations, where the environment ishostile. Hence, security is a critical issue. Due to the nature of Adhocnetworks, conventional security measures cannot be used.New techniques of security measures are essential for highsurvivability networks. The performance of the network will beseverely affected, in the presence of compromised nodes, whichcause undetermined and unpredictable complex failures. Thisproject is mainly to identify the misbehaviors caused by somemalicious node for NTP (Node Transition Probability) protocol,and eliminate them from the network. The performance analysis isdone based upon two cases .In first case the complete networktopology is studied and based upon it a threshold value is fixed todetect the malicious activity and eliminate it. In the second case afuzzy model is introduced so that automation of threshold can bedone for anomaly detection of malicious nodes in network withvarying topology. In contrast to the case one -- intrusion detectionmodels for ad hoc networks we have implemented an efficient andbandwidth-conscious framework that takes into distributed natureof ad hoc wireless network management and decision policies.**

Keywords- NTP, MAL, REMAL, PURGE packets, IDM, IRM, Crisp value, Security.

I. INTRODUCTION

Ad-hoc networks demand a protocol completely different from those used for wired and infrastructured wireless networks. Ad-hoc networks have their own requirements and constraints and require a protocol that takes into account these issuesand provide reliable communication under such constraints. This section explains the protocol aspects for ad-hoc mobile networks. In particular, it reveals what are the problems associated with routing in such networks. Although several routing schemes have been proposed, most of them are modified extensions of existing link-state or distance-vector based routing protocols. However, in an ad-hoc mobile network where mobile hosts are acting as routers and have both power and bandwidth constraints, conventionalprotocols that employ periodic broadcast are unlikelyto be suitable. A novel routing scheme is required toprovide efficient and high throughput communicationamong mobile adhoc networks (MANET).

The newrouting protocol-NTP that was proposed determinesroutes based on the probability that the nodes lie within the host node‘s proximity for a longer timethereby improving the stability of the route. Theobjective is to enhance the security issues of the NTPprotocol.

II. NTP

The proposed a new routing scheme called NodeTransition Probability (NTP) based routing, whichuses less control packets to determine the routesbetween two nodes. The proposed algorithm adaptsquickly to routing changes when host movement isfrequent. NTP based routing algorithm, whichdetermines route using the received power at aparticular node from all other nodes. In thisalgorithm, a node floods a control packet only if thereis no neighbor table and has data to send. Theneighbor table is computed based on the receivedreplies and we choose the node, which is replied withmaximum power for more times as neighbor. Bychoosing the neighbor table route table is computedfor the Source-Destination pair. The performance ofthis algorithm is studied for various scenarios andcompared their performance such as throughput,control over head and end to end delay with anexisting routing protocol. The performance resultshows that this algorithm maximizes the bandwidthduring heavy traffic with less overhead.

A. The Fuzzy Approach

In this paper the traffic pattern of the Node transition based probability protocol is to be established in terms of fuzzy logic parameters. For fuzzification process ‗mamdani‘ method is used and for defuzzification process ‗Mirror rule‘ is applied. We define the traffic levels to be low level, medium level and high level based upon the crisp value of the fuzzy security model. Intrusion detection is an important but complex task for an adhoc network. Many Artificial intelligent techniques have been widely used in intrusion detection systems. There are two main reasons for introducing fuzzy logic for intrusion detection. First, many quantitative features are involved in intrusion detection. Fuzzy set theory provides a reasonable and efficient way to categorize these quantitative features in order to establish highlevel patterns. Second, security itself is fuzzy. For quantitative features, there is no sharp delineation between normal operations and anomalies. Fuzzy episode rules allow one to create the high-level sequential patterns representing

[1]Suresh Kumar MLEngg College. Sureshkumar1239@gmail.com
[2]*Machha.Narender HITS College of Engg,machha.narender@gmail.com*
[3]G.N.Ramesh Bhoj Reddy Engg College, noya.ramesh@gmail.com.

normal behavior. With fuzzy spaces, fuzzy logic allows an object to belong to different classes at the same time. This concept is helpful when the difference between classes is not well defined. This is the case in theintrusion detection task, where the differences between the normal and abnormal classes are notwell defined. Thus the intrusion detection problem(IDP) is a two-class classification problem: the goalis to classify patterns of the system behavior in twocategories (normal and abnormal), using patterns ofknown attacks, which belongs to the abnormal class,and patterns of normal behavior. In fuzzy logic, fuzzysets define the linguistic notions, and membershipfunctions define the truth-value of such linguisticexpressions.

B. Fuzzy Algorithm

We can determine the crisp value for the differenttraffic range of the mobile nodes based upon thequality of service parameters for the given Node
Transition Probability protocol [6]
Input (1) --------- Queue length (QL)
Input (2) --------- Data rate (DR)
Input (3) --------- Item size (IT)
Range of the Input levels
Now based upon the input levelsselected the _Rule base' is sorted output for varioustraffic levels. Membership graph for the three levelsof input is shown in the figure 2.5.1.

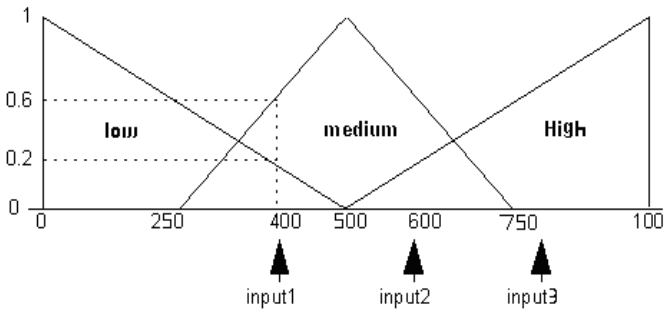


Figure: 2.2.1: Membership graph for the three levels of input.

Rule base:
With respect to the different levels of input traffic therule base for the fuzzy model is framed as low-level,medium-level and high-level and is shown in table2.5.1, 2.5.2 and 2.5.3 respectively.

Low level:

Rules	Queue length	Data rate	Item size	Traffic range
Rule1	Low	Low	Low	Low
Rule2	Low	Low	High	Low
Rule3	Low	Low	Medium	Low
Rule4	Low	Medium	High	Low
Rule5	Low	High	Low	Low
Rule6	Low	Medium	Low	Low
Rule7	Low	High	Medium	Low
Rule8	High	Low	Low	Low
Rule9	Medium	Low	Low	Low

Table: 2.2.1 Rule Base for low level range

Medium Level

Rules	Queue length	Data rate	Item size	Traffic range
Rule10	Medium	Medium	Medium	Medium
Rule11	Medium	Medium	Low	Medium
Rule12	Medium	Medium	High	Medium
Rule13	Medium	Low	High	Medium
Rule14	Medium	Low	Medium	Medium
Rule15	Medium	High	Medium	Medium
Rule16	Medium	High	Low	Medium
Rule17	Low	Medium	Medium	Medium
Rule18	High	Medium	Medium	Medium

Table: 2.2.2 Rule Base for Medium level range

High level

Rules	Queue length	Data rate	Item size	Traffic range
Rule19	High	High	High	High
Rule20	High	High	Low	High
Rule21	High	High	Medium	High
Rule22	High	Medium	Low	High
Rule23	High	Low	High	High
Rule24	High	Medium	High	High
Rule25	High	Low	Medium	High
Rule26	Low	High	High	High
Rule27	Medium	High	High	High

Table: 2.2.3 Rule Base for High level range

Thus for the three input parameters quelength, datarate and the packet size we have framed 27 rules fordetermining the crisp value. Now based upon thecrisp value output the threshold parameter associatedwith respect to the traffic pattern in any routingprotocol can be changed to achieve desired flow
control. The Intrusion detection model and theintrusion response model can be improved using this_crisp value' to reduce the malicious node activity inthe given _MANET'.The fuzzy logic parameters canbe selected as the packet size, queue length of thedata packets, data rate, power margin of nodes, andmobility range of nodes etc., In this paper queuelength, data rate, packet size are taken as the fuzzyparameters, a rule base is formed based upon these
parameters. The rule base has three level of rangesbased upon the fuzzy parameters selected todetermine the crisp value of the traffic range for thegiven Node Transition Probability model. Now, thisfuzzy approach for security enhancement of NTPprotocol is the main source for the IDM& IRMmodel.

C. Algorithm For Intrusion Detection Model

The node sends to neighboring node an intrusion (oranomaly) state request. Each node (including theinitiation node) then propagates the state information,indicating the likelihood of an intrusion or anomaly,to its immediate neighbors. Each node thendetermines whether the majority of the receivedreports indicate an intrusion or anomaly; if yes, thenit concludes that the network is under attack.

Anynode that detects an intrusion to the network can theninitiate the response procedure.

A node identifies that another node is compromised,when its malcount exceeds the crisp value of thefuzzy approach or threshold value as for (case-1) forallegedly compromised node. In such cases, itpropagates this information to the entire network bytransmitting a Mal packet. If other nodes also suspectthat the node, which has been detected, iscompromised, it reports its suspicion to the networkby transmitting a ReMal packet.

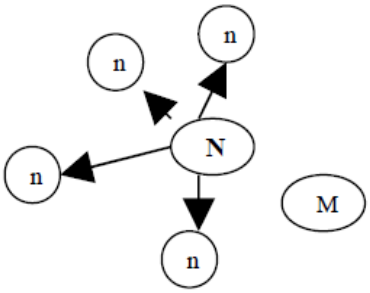


Figure: 2.6.1 Generation of mal Packets

The rationales behind this scheme are as follows.Audit data from other nodes cannot be trusted andshould not be used because the compromised nodescan send falsified data. However, the compromisednodes have no incentives to send reports of intrusion,anomaly because the intrusion response may result intheir expulsion from the network. Therefore, unlessthe majority of the nodes are compromised, in whichcase one of the legitimate nodes will probably be ableto detect the intrusion with strong evidence and willrespond, the above scheme can detect intrusion evenwhen the evidence at individual nodes is weak.

D. Algorithm For Intrusion Response Model

The following steps are taken after a purge packet issend to all nodes regarding the malicious node:

i. All the nodes in the network are made awareof the malicious node.
ii. All the data, control packets from the purgednode is dropped.
iii. A signal for route table entry modification issend to all the nodes.
iv. The purged node is deleted from theneighbor table and seen table for theneighbor nodes.

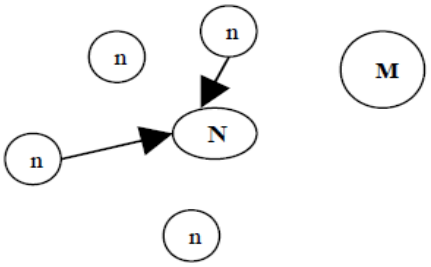


Figure: 2.8.1. Generation of Re-Mal packet by the nodes

E. Implementation

The proposed security measures were implementedusing GloMoSim as the simulator. Theimplementation part consists of following steps:

i. Creation of Malicious Nodes

Out of N nodes in the network 20% of the nodes weremade malicious. In the network the malicious nodesare the nodes, which generate more of RouteRequests than the normal value [3]. These nodeswere selected randomly. Normally the nodes generateroute requests when data is present in their buffer anda proper route to the destination is not known. Therandomly selected nodes were made to generate morenumber of route requests irrespective of their bufferand route discovery status. Each malicious node inthe network generates a variable number of routerequests to another randomly. The above said IDSIRSoperations are done cooperatively by a group ofnodes when the confidence percentage level is verylow. When the confidence level is very high thealleged node is directly purged from the networkincreasing the efficiency of the model and thereby decreasing the time taken for the detection andresponse modules incorporated. Thus the mal nodesare identified through the proposed security model.

III. PERFORMANCE METRICS

A. Control Overhead

The number of control packets transmitted for everydata packet is noted down. Each hop of the routingpacket is treated as a packet. The following graphshows that the malicious nodes increase the routingload of the network as they generate the false routerequests and there by increasing the number ofcontrol packets for each data packet transmitted.After implementing the proposed security model, itconsiderably decreases the routing load byidentifying the malicious nodes and eliminating themfrom the network and bringing the network near tonormal NTP protocol. The performance metrics ofcontrol overhead Vs Pause Time is shown in thefigure 3.1.

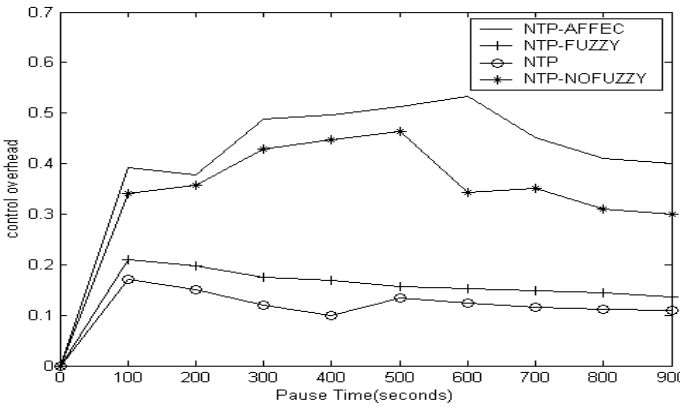


Figure 3.1: Control Overhead Vs Pause Time

B. Packet Delivery Fraction

This is the ratio of CBR packets delivered to thatgenerated and is measured as throughput. Fordifferent pairs of the source destination paircorresponding throughput is noted down. Thethroughputs for the NTP affected with malicious nodes are less when compared with ordinary NTPprotocol. After incorporating the fuzzy approach thethroughput is getting increased. Thus we prove thatfuzzy approach is better than direct assignment ofthreshold for anomaly detection. The performancemetrics of throughput Vs Source-Destination Pair isshown in the figure 3.2.

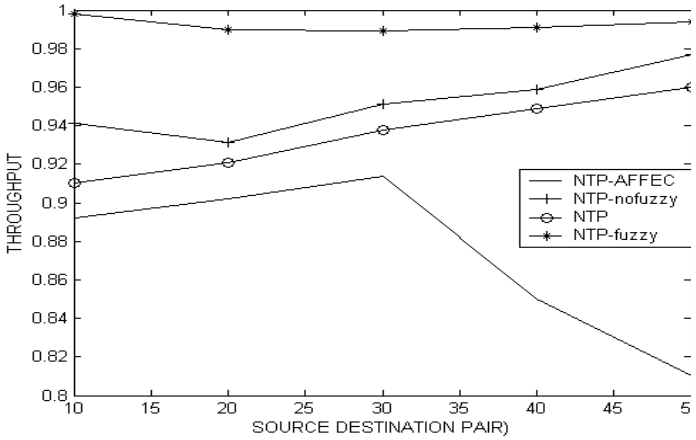


Figure 3.2: Throughput Vs Source-Destination Pair

C. Mobility

For different ranges of mobility the graph is plotted.The system performance has been observed in thepresence of malicious nodes and measured. Theperformance enhancement is due to the implementedmodel. In the simulation misbehaving node generatesfalse route requests. So the corresponding packetdelivery decreases for it. The performance metrics ofPacket delivery Vs Mobility is shown in the figure3.3.

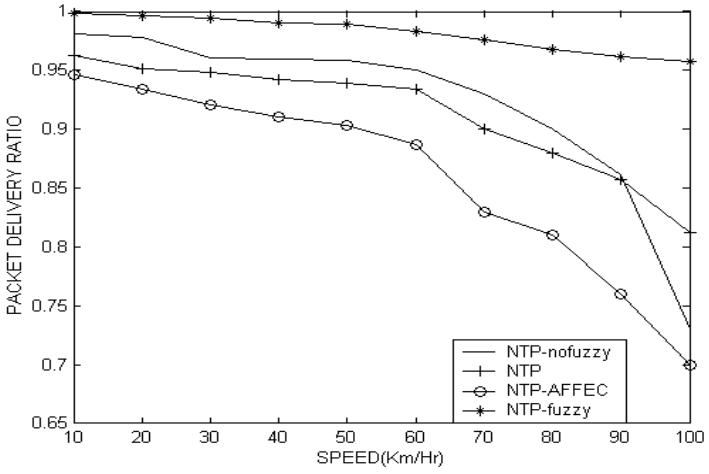


Figure 3.3: Packet Delivery ratio Vs Mobility

D. Average End To End Delay

This is the average of delays incurred by all packetsthat are successfully transmitted. The following graphshows that the malicious nodes in the network hasphenomenally increased the end-to-end delay of thenetwork compared to the normal network as thenodes forward the false RREQs to other nodes andthereby increasing the overall time to process the control packets. The performance metrics of delay VsPause Time is shown in the figure 3.4.

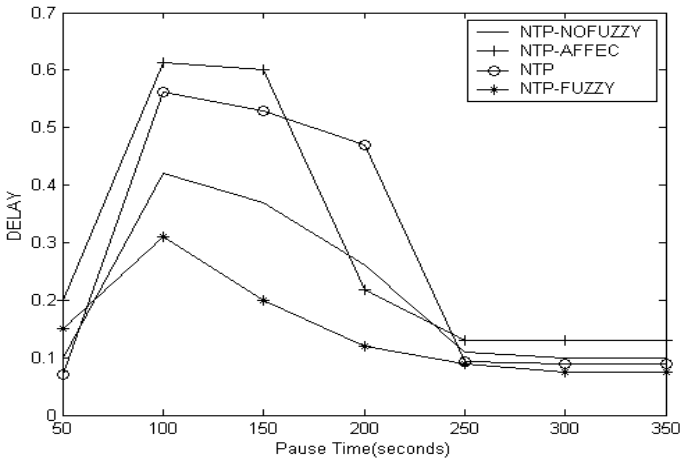


Figure 3.4: Delay Vs Pause Time

After incorporating the fuzzy security scheme theend-to-end delay is brought down to near normalnetwork as intruder nodes are identified and thereactivities are restricted and intruder nodes areeliminated from the network.

IV. Conclusion

The distributed false route request problem increases end-to-end delay, routing overhead and decreasingthe throughput and overall efficiency of the network.Our solution to this problem as successfullyeliminated the intruder nodes and has brought thenetwork performance near to the normalcy. Theperformance characteristics of network depicted inthe graphs prove this statement.

V. Future Work

The future work of the paper is to extend the fuzzy automation for the security enhancement of the NTP protocol in terms of power margin and Noise margin.

VI. References

1) Charles E Perkins, Introduction to Adhoc networking, Addision Wesley, Dec 2001.
2) SankararajanRadha and sethu shanmugavel —Implementation of Node Transition Probability Based Algorithm for MANET and performance analysis using different mobility models"IEEEProc, VOL5, NO.3.sept2003

3) Sonali Bhargava, Dharma P.Agarwal Security enhancement in AODV protocol for wireless Ad Hoc networks, IEEE 2001.
4) Ross, Timothy. Fuzzy Logic with Engineering Applications. McGraw-Hill, New York, NY, 1995.
5) Ibrahim, Ahmad. Fuzzy Logic for Embedded Systems Applications. Elsevier Science, Burlington, MA, 2004.
6) Miller, Byron. The Design and Development of Fuzzy Logic Controllers. Impatiens Publications, Minneapolis, 1997.
7) Yongguang Zhang and Wenke Lee. Intrusion detection in wireless ad hoc networks. In the 6th international conference in mobile computing and networking (MOBICOMM'00), pages 275-283, June 2000.
8) Sergio Marti, T.J. Giuli, Kevin Lai, and Mary Baker. Mitigating routing misbehaviour in mobile ad hoc networks. In 6th International Conference onmobile computing and networking (MOBICOM'00),pages 255-265, August 2000.
9) GloMoSim User Manual, http://pcl.cs.ucla.edu/projects/domains.

Performance Analysis of Wired and Wireless LAN Using Soft Computing Techniques- A Review

Dr. R K Bansal[1], Vikas Gupta[2], Rahul Malhotra[3]

Abstract— **The wired Computer Networks provide a secure and faster means of connectivity but the need of mobility i.e. anywhere, anytime and anyone access is tilting the network users towards wireless technology. In this paper, an overview of the current research literature, in the field of Wired and wireless networks, has been presented. The network simulators provide an ease in predicting and estimating the performance of networks. Among the various network simulators available, OPNET gains an edge in analysing the performance of the networks through simulations. The metrics like throughput, delay and retransmission attempts have been overviewed for performance analysis of the wireless and wired computer networks using soft computing techniques like simulation through OPNET.**

Keywords—IEEE 802.11, RTS/CTS, OPNET, Wired LAN, Wireless LAN.

I. INTRODUCTION

Networks have grown like weed over the past few decades providing a pace to the means of accessing network resources. For example, the use of Internet is gaining importance with the adoption of network technologies for purposes like education, business, banking and defence. These interconnected set of computer system permits interactive resource sharing between connected pair of systems. Rapid advances have taken place in the field of Wired and Wireless Networks. Several network models have been modelled by various researchers, using network simulators, to find out the most feasible ones. Investigations of these network models have been performed using the simulation techniques that reduce the cost of prediction, estimation and implementation of the network models. Among the various network simulators available like NetSim, NS-2, GloMoSim etc., OPNET provides the industry's leading environment for network modelling and simulation. It allows to design and study communication networks, devices, protocols, and applications with flexibility and scalability. It provides object oriented modelling approach and graphical editors that mirror the structure of actual networks and network components. It provides support for modelling both the wired and wireless LANs. Though the wired networks have provided the high speed connectivity but due to the drawbacks like extensive cabling and immobility etc., the WLAN gained momentum. The computer networks today are not only wired but wireless too, depending on the type of circumstances like need of mobility, rough terrains, or secure networks.

About[1]- Giani Zail Singh College of Engineering & Technology, Bathinda
hodecegzscet@yahoo.com
About[2&3]- Adesh Institute of Engineering and Technology, Faridkot
vikas_gupta81@yahoo.co.in
blessurahul@gmail.com

Open system interconnection (OSI) reference model divides the Data Link Control (DLC) layer into Logical Link Control (LLC) and Medium Access Control (MAC) sub layers. The LLC layer is independently specified for all 802 LANs, wireless or wired. Like IEEE 802.3 (Ethernet), IEEE 802.5 (Token Ring), IEEE 802.11 (WLANs) standard also focuses on the above mentioned two layers [1]. Our study has focused on performance analysis of IEEE 802.3 (Ethernet) based Wired LANs and IEEE 802.11b based Wireless LANs using soft computing techniques like network simulators. This paper has been organised as follows: Part I deals with Introduction, Part II deals with the Literature Overview, Part III and IV deals with the brief description of IEEE 802.11 and IEEE 802.3, Part V deals with the performance metrics being focused upon and in the last section the paper has been concluded.

II. LITERATURE REVIEW

A wireless communication is flexible data communication system implemented as an extension to or as an alternative for a wired communication. It has overshadowed the wired technology over a span of time and is a rapidly growing segment of the communications industry, with a potential to provide high-speed, high quality information exchange between the portable devices located anywhere in the world. Wireless Local Area Networks (WLANs) have been developed to provide users in a limited geographical area with high bandwidth and similar services supported by the wired Local Area Network (LAN). Unlike wired networks, WLANs, which uses IEEE 802.11 standards, to transmit and receive radio waves through the air medium between a wireless client and an Access Point (AP), as well as among two or more wireless clients within a certain range of each other. A WLAN basically consists of one or more wireless devices connected to each others in a peer-to-peer manner or through APs, which in turn are connected to the backbone network providing wireless connectivity to the covered area. In [8], the authors worked on improving the performance of WLANs using Access points. They investigated and estimated the traffic load on an access point, which can help determine the number of access point to be employed in a network. The effect of enabling Point Coordination Function (PCF) on network stations and also the number of PCF stations that can be deployed per access point was also investigated. Correctly setting the number of PCF stations will help tune the performance of these nodes as well as the overall network performance. In [20], also the author introduced a wireless LAN design framework for optimal placements of access points at suitable locations to satisfy the coverage and capacity requirements of the users. Optimal planning of WLANs can result in improved Quality of Services, efficient use of resources, minimizing

interference and reduced deployment cost. The performance of WLANs depends on the RF conditions in which they operate. Randomized optimization algorithms were used, to solve the AP placement and channel allocation problems like coverage, traffic, Redundancy, channel interference and wiring cost. Then the output of this algorithm was validated using OPNET.

Another important issue is the Bandwidth of wireless networks. The bandwidth of wireless local area networks is limited as compared to that of wired local area networks which provide a large bandwidth. This limitation is due to the error prone physical medium (air). The methods like tuning the physical layer related parameters [6], tuning the IEEE 802.11 parameters and using enhanced link layer (media access control) protocol were used to improve the performance of WLANs.

The IEEE 802.11 standard operates far from theoretical throughput limit depending on the network configuration [7]. An analytical model was proposed to achieve maximum protocol capacity (theoretical throughput limit), by tuning the window size of the IEEE 802.11 back-off algorithms. The main reason why the capacity of the standard protocol is often far from theoretical limit is that during the overload conditions, a station experiences a large number of collisions before its window has a size which gives a low collision probability. It was cited that proper appropriate tuning of the back-off algorithm can derive the IEEE 802.11 protocol close to the theoretical throughput limit.

The identification time is another critical indicator for the performance enhancement of RIFD in wireless systems. In [12], the authors proposed a Rician fading channel model to highlight the fading effect in Radio frequency Identification (RIFD) System, using the statistics of Bit Error Rate (BER) and Signal-to-noise Ratio (SNR). This model was employed in addition to the existing RIFD system and was used to calculate the identification time to reflect the influence of channel situation on tag identification. The simulation showed that the Fading channel effect increased the Identification time as BER varies. It was also analyzed that the wireless channel has strong effect on the identification time.

The throughput performance of WLANs is affected by the mobility of the users [19]. The wireless data connections have high bit error rates, low bandwidth and long delays. The physical and MAC layer were fine tuned to improve the performance of WLAN. The performance metrics like slot time, short Inter-frame spacing (SIFS), minimum contention window (CW_{min}), Fragmentation Threshold (FTS) and Request to send (RTS) thresholds were focused upon to reduce collisions and media access delay. Hence an increase in throughput and channel utilization occurs, which can improve the performance of Wireless networks under heavy load conditions (high BER values). The effectiveness of optional RTS/CTS handshake mechanism on the performance of IEEE 802.11 based wireless local area networks (WLANs) using OPNET was also evaluated in [21]. The impact of parameters like throughput, packet loss rate, round trip time (RTT) for packets, retransmission rate and collision count on the performance metrics like retransmissions, throughput, media access delay was presented.. It was cited that handshake mechanism is useful where hidden node problem exists, but the unnecessary use of RTS/CTS mechanism increases the overhead of RTS/CTS packets. The parameters like RTS/CTS threshold, fragmentation threshold and data rate impact the performance of wireless LAN. In [3], also the authors proposed the wireless network performance optimization using OPNET Modeler. The model was simulated and the results indicated that fine tuning of these parameters can help to improve the performance of WLANs.

THE IMPACT OF LOAD, NUMBER OF NODES, RTS/CTS, FTS AND DATA RATE ON PERFORMANCE METRICS LIKE END-TO END THROUGHPUT AND AVERAGE DELAY WAS ANALYZED BY MEANS OF SIMULATION. THE SIMULATION STUDY OF IEEE 802.11B WIRELESS LAN USING OPNET IT GURU ACADEMIC EDITION 9.1 FOR IMPROVEMENT IN THE THROUGHPUT BY FINE TUNING THE ATTRIBUTES LIKE FRAGMENTATION THRESHOLD AND RTS THRESHOLD [1].

In the literature, discussed above the performance analysis of wireless LANs has been surveyed but the use of wireless technology doesn't mean an end to the wired technology. The following literature survey provides scope of improvement in the wired technology too.

In order to deal with burst data transmission the 100Mbps Ethernet is preferable to ensure communication performance [18]. The features of conventional protection system, including current differential protection and distance protection were analysed by the author. The disadvantages of complex power systems were pointed out. The comparative investigation of three wide area protection System (WAPS) architectures, i.e. centralized, distributed and networked using OPNET, revealed that networked structure is considered to be best due to its fast response time in terms of lesser delay or transfer time. The architecture and communication network of WAPS was investigated to utilize global information instead of local information to achieve better performance.

The load on the network server increases with increase in the user activity. An increased number of users increase the network load and degrades the performance. An effort was made to improve the performance by load balancing. Various probabilistic methods to study network performance [2] had been proposed during the research. The significance of using discrete-event simulation, as a methodology to confront network design and fine-tuning its parameters was also highlighted.

Another major problem exists in the form of network congestion. To overcome the problem of congestion, Fiber Distributed Data Interface and Asynchronous Transfer Mode type high-performance networks along with the bucket congestion control mechanism were modeled and simulated [4]. The effect of variation in attributes like traffic load on the performance metrics like end-to-end delay and throughput was analyzed.

The increase in traffic load effects the network performance In [5], a network model with switched Ethernet subnets and Gigabit Ethernet backbone under typical load conditions and also for time-sensitive applications such as voice over IP

was modeled and simulated. The simulations were carried out to study the impact of increase in traffic load on the performance metrics like delays was analyzed.

The type of routing technique used in the network is an important consideration to study the network performance. Three technologies – Internet protocol (IP), Asynchronous Transfer Mode (ATM) and Multiprotocol Label Switching (MPLS) were compared in terms of their routing capability [9]. Different performance metrics like end-to-end Delay, throughput, Channel Utilization, FTP download response time and normalized delivered traffic were analyzed using OPNET simulator. The results indicated that ATM and MPLS outperform IP (without modification) in terms of delay and response time to the exposed data. Another comparison of the performance of Gigabit Ethernet and ATM network technologies using modeling and simulation was done. Real-time voice and video conferencing type traffic were used to compare the network technologies in terms of response times and packet end-to-end delays. While ATM is a 53-byte frame connection-oriented technology, Gigabit Ethernet is a 512-byte frame (minimum) connectionless technology. The performance analysis indicated that the performance of ATM network is still very good [14]. But it does not keep up with the Gigabit Ethernets small delay time. Hence Gigabit Ethernet provides better performance than ATM as a backbone network, even in networks that require the transmission of delay sensitive traffic such as video and voice.

A new operational model called "AMP model" and an improved ack-regulation scheme called SAD to explain and improve the performance of TCP/IP over wireless networks was presented. The use of link –sharing schedulers with just two queues (ack and packet queues, with SAD implemented on ack queues) to support bidirectional traffic was also proposed. In [10], the authors analyzed TCP performance in asymmetric networks, where throughput significantly depends on the reverse direction and packet loss.

The queuing disciplines are implemented for resource allocation mechanisms. The queuing disciplines used are First-in-first out (FIFO) queuing, priority Queuing (PQ) and weighted Fair Queuing (WFQ). A comparison of different queuing disciplines for different scenarios using simulation was presented for performance evaluation [11]. By varying the queuing disciplines the parameters like Traffic received End-to-End Delay and Traffic received or live video streaming video were presented.

The use of network connecting devices plays an important role in the network design. Various network scenarios were designed by changing the network devices like Hub, Switch and Ethernet cables using the network simulation software – OPNET. The performance of the network was analysed using various performance metrics like Delay and collision count, Traffic sink, Traffic source and packet size. It was observed that the throughput improved and collisions decreased when the packet size is reduced [13].

The choice of network simulator is very important for accurate simulation analysis. A comparative study of two network simulators: OPNET Modeler and NS-2 for packet level analysis was presented in [15]. Both discrete events and analytical simulation methods were combined to check the performance of simulator in terms of speed while maintaining the accuracy. For performance testing of the network, different types of traffic like CBR (constant Bit Rate) and an FTP (File transfer protocol) were generated and simulated. Though both the simulators provide similar results, the "freeware" version of NS-2 makes it more attractive to a researcher but OPNET Modeler modules gain an edge by providing more features.So, OPNET can be of use in academia i.e. advanced networking education [16]. Various scenarios like VoIP, WLAN or video Streaming were designed, simulated and also analysed analytically to check accuracy. This illustrated the broader insight the OPNET software can offer in the networking technologies, simulation techniques and its impact of applications on the network performance.

III. IEEE 802.11

An 802.11 LAN is based on a cellular architecture where the system is subdivided into cells. Each cell called Basic Service Set is controlled by a Base Station called Access Point. Although a wireless LAN may be formed by a single cell, with or without a single Access Point, most installations will be formed by several cells, where the Access Points are connected through some kind of backbone called Distribution System. This backbone is typically Ethernet and, in some cases, is wireless itself as shown in Figure 1. The whole interconnected Wireless LAN, including the different cells, their respective Access Points and the Distribution System, is seen as a single 802 network to the upper layers of the OSI model and is known in the Standard as Extended Service Set. As any 802.x protocol, the 802.11 protocol covers the MAC and Physical Layer.

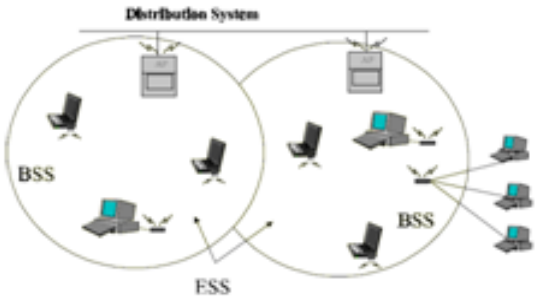


Figure 1: IEEE 802.11 LAN

The Standard currently defines a single MAC which interacts with three PHYs (running at 1 and 2Mbit/s) as Frequency Hopping Spread Spectrum (in 2.4 GHz Band), Direct Sequence Spread Spectrum (in 2.4 GHz Band), and Infrared. The MAC Layer defines two different access methods, the Distributed Coordination Function and the Point Coordination Function. The IEEE 802.11b DCF mode is based on a "listen before-talk" mechanism i.e. it may be CSMA/CA protocol – a basic two way handshaking mechanism or Virtual Carrier Sense mechanism – four way handshaking mechanisms.

IV. IEEE 802.3

Wired Local Area Networking includes several technologies such as Ethernet, token Ring, Token bus, FDDI and ATM

LAN. Some of these technologies survived for a while, but Ethernet is by far the dominant technology. Evolution from a 10Mbps Standard Ethernet to bridged Ethernet and then to a switched Ethernet paved a way for faster Ethernet. IEEE 802.3 Standard specifies CSMA/CD as the access method for first-generation 10-Mbps Ethernet, a protocol that helps devices share the bandwidth evenly without having the two devices transmit at the same time on the network medium. This CSMA/CD protocol was created to overcome the problem of collisions that occur when the packets are transmitted simultaneously from different nodes.

V. Performance Metrics

Some of the Performance metrics focused on, in the literature review, regarding wired and wireless LAN are:

Collision count: Total number of collisions encountered by this station during packet transmissions.

Data Dropped: Total number of bits that are sent by wireless node but never received by another node.

Delay: This statistic represents the end to end delay of all packets received by all the stations and forwarded to the higher layer.

Load: Total number of bits received from the higher layer. Packets arriving from the higher layer are stored in the higher layer queue. It may be measured in bits/sec or packets/sec.

Media access delay: Total time (in Seconds) that the packet is in the higher layer queue, from the arrival to the point when it is removed from the queue for transmission.

Queue Size: Represents the total number packets in MAC's transmission queue(s) (in 802.11e capable MACs, there will be a separate transmission queue for each access category).

Throughput: Total number of bits sent to the higher layer from the MAC layer. The data packets received at the physical layer are sent to the higher layer if they are destined for this destination.

Though Wireless networks, in contrary to wire networks, are relatively a new field of research, there exist some simulators to develop and test the effect of change in the input/other attributes parameters on various performance metrics.

VI. Conclusions

The aim of the paper is to highlight the research going on in the field of Wireless and wired Computer Networks. Various simulation studies were done using different types of network simulators, to study their performance comparison. An extensive literature review on wireless and wired networks using simulation has been investigated for their performance comparison by varying the attributes of network objects such as traffic load, file size, RTS/CTS, customizing the physical characteristics to vary BER, slot time, SIFS time or the contention window, to determine their impact on throughput & delay.

VII. References

1) Mohammad Hussain Ali and Manal Kadhim Odah, "*Simulation Study of802.11b DCF using OPNET Simulator*," Eng. & Tech. Journal, vol.27,No6,2009,pp:1108-1117,2009
2) Norbert Martinez, Angel A. Juan, Joan M.Marques and Javier Faulin, "Using OPNET to simulate the computer system that gives support to an on-line university Intranet," [Online]. Available: https://enterprise1.opnet.com/.
3) Sameh H. Ghwanmeh, "Wireless network performance optimization using Opnet Modeler," Information Technology Journal 5(1), pp. 18-24, 2006.
4) N. Alborz, M. Keyvani, M. Nikolic, and Lj. Trajkovic, ``Simulation of packet data networks using OPNET," OPNETWORK 2000, Washington, DC, Aug. 2000.
5) J. A. Zubairi and Mike Zuber, "SUNY Fredonia Campus Network Simulation and Performance Analysis Using OPNET" in Proc. online OPNETWORK2000, Washington DCS, Aug 2000.
6) J. Song and Lj. Trajkovic, ``Enhancements and performance evaluation of wireless local area networks," OPNETWORK 2003, Washington, DC, Aug. 2003.
7) F. Cali, M.Conti and E. Gregori, " Dynamic tuning of the 802.11 protocol to achieve a theoretical throughput limit," IEEE/ACM Transactions on networking, vol. 8, no. 6, pp. 785-799, Dec. 2000.
8) Sarah Shaban, Hesham M.El Badawy, and Attallah Hashad, "Performance Evaluation of the IEEE 802.11 Wireless LAN Standards," WCE-2008, London, U.K., vol. 1, July 2-4, 2008.
9) Hafiz M. Asif and Md. Golam Kaosar, "Performance Comparison of IP, ATM and MPLS Based Network Cores Using OPNET," in 1st IEEE International Conference on Industrial & Information Systems (ICIIS 2006), Sri Lanka, 8-11 August, 2006.
10) Dibyendu Shekhar, Hua Qin, Shivkumar Kalyanaraman, and Kalyan Kidambi, "Performance Optimization of TCP/IP over Asymmetric Wired and Wireless Links," in the proceeding of Conference on Next Generation Wireless Networks: Technologies, Protocols, Services and Applications (EW-2002), Florence, Italy, February 25-28, 2002 .
11) T. Velmurugan, Himanshu Chandra and S. Balaji, "Comparison of Queuing disciplines for Differentiated Services using OPNET," IEEE, ARTComm.2009.128, pp. 744-746, 2009.
12) Yang Dondkai and Liu Wenli, "The Wireless Channel Modeling for RFID System with OPNET," Proceedings of the IEEE communications society sponsored 5th International Conference on Wireless communications, networking and mobile computing, Beijing, China, pp. 3803-3805,Sep 2009.
13) Ikram Ud Din, Saeed Mahooz and Muhammad Adnan, "Performance Evaluation of Different

Ethernet LANs Connected by Switches and Hubs," European Journal of Scientific Research, vol. 37 No. 3, pp. 461-470, 2009.

14) Jason Schreiber, Mehradad Khodai Joopari, M.A. Rashid, "Performance of video and video conferencing over ATM and Gigabit Ethernet backbone networks," Res. Lett. Inf. Math. Sci., Vol7, pp.19-27, 2005.
15) Gilberto Flores Lucio, Macros Paredes-Farrera, Emmanuel Jammeh, Martin Fleury, Martin J. Reed, " OPNET Modeler and NS-2 : Comparing the accuracy of Network Simulators for packet level Analysis using a Network Test bed," WSEAS Transactions on Computers, pp. 700—707, 2-3,July 2003.
16) J. Theunis, B.Van den Broeck, P. Leys, J.Potemans, E. Van Lil, A. Van De Capelle, " OPNET in Advanced Networking Education," proceedings to the International Conference on Networking ICN'01, Colmar France,2001.
17) Mohd. Nazri Ismail and Abdullah Mohd Zin, "Emulation network analyzer development for campus environment and comparison between OPNET Application and Hardware Network Analyzer, " European Journal of Scientific Research, ISSN 1450-216X, Vol.24 No.2pp.270-291,2008.
18) Dahai Zhang and Yanqui Bi, "Communication Network of Wide Area Protection System using OPNET Simulator," IEEE International Symposium on Industrial Electronics (ISIE 2009),pp. 1298-1303, July 5-8,2009.
19) Walid Hneiti and Naim Ajlouni "Performance Enhancement of Wireless Local Area Networks, " Proceedings of IEEE ICTTA'06, 2nd International Conference on Information & Communication Technologies: from Theory to Applications, Damascus, Syria, vol. 2, pp. 2400-2404, April 2006.
20) Karthik Chandrashekhar and Paul Janes, "Optimal design of Wireless local Area Networks (WLANs) using simulation," Military Communications Conference, 2009, MILCOM 2009, IEEE, Boston, MA, 18-21, Oct 2009.
21) Hetal Jasani and Naseer Alaraje, "Evaluating the performance of IEEE 802.11 Network using RTS/CTS Mechanism" , in the proceedings of IEEE EIT 2007, Chicago, IL, pp. 616-621, 17-20, May 2007.

Texture Classification With High Order Local Pattern Descriptor: Local Derivative Pattern

Dr U S N Raju[1], A Sridhar Kumar[2], B Mahesh[3], Dr B Eswara Reddy[4]

GJCST Classification
I.2.10,I.3.7,1.4.7

***Abstract*-This paper proposes a novel method for texture classification using high-order local pattern descriptor: Local Derivative Pattern (LDP). LDP is used to encode directional pattern features based on local derivative variations. The nth order LDP is proposed to encode the (n-1)th order local derivative direction variations, which can capture more detailed information. The local texture information for a given pixel and its neighborhood is characterized by the texture units calculated in different ways, and the global textural aspect of an image is revealed by its texture spectrum. This paper uses the second, third and fourth order LDPs to classify the textures. For this classification, the texture images are taken from Brodatz album.**

Keywords- Local Derivative Pattern, Texture pectrum, Texture classification.

I. INTRODUCTION

Texture has long been an important topic in image processing [1,2,3,7,8,9,13,18]. Methods of texture analysis are usually divided into two major categories [8,15]. The first is the structural approach, where texture is considered as a repetition of some primitives, with a specific rule of placement. The traditional Fourier spectrum analysis and wavelet based analysis [11] are often used to determine the primitives and placement rule. Several authors have applied these methods to texture classification and texture characterization with a certain degree of success [5]. The second major approach in texture analysis is statistical method. Its aim is to characterize the stochastic properties of the spatial distribution of gray levels in an image. The gray tone co-occurrence matrix is frequently used for such characteristics. A set of textural features derived from the co-occurrence matrix is widely used to extract textural information from digital images [2,4].

Study of patterns on textures is recognized as an important step in characterization and classification of textures. Textures are classified recently by various pattern methods: preprocessed images [18], long linear patterns [10,17], and edge direction movements [6], Avoiding Complex Patterns [16], marble texture description [14]. Textures are also described and classified by using various wavelet transforms: one based on primitive patterns [19], and another based on statistical parameters [12].

[1]*Professor, Dept. of CSE, Rajeev Gandhi Memorial College of Engg. & Technology, Nandyal, Kurnool (Dt.)-518 501, A.P., India, usnraju@gmail.com*
[2]*Senior Software Engineer, Inforaise Technologies Pvt. Ltd., Hyderabad, A.P., India, a.sridhar51@gmail.com*
[3]*Senior Software Engineer, Bangalore, Karnataka, India, mahesh544@gmail.com*
[4]*Associate Professor, Dept. of CSE, JNTU College of Engineering, Anantapur, A.P, India, eswarcsejntu@gmail.com*

Recently, local descriptors have gained much attention in texture analysis for their robustness to illumination and pose variations. One of the local descriptors is local feature analysis (LFA) proposed by Penev et al. [25]. In LFA, a dense set of local-topological fields are developed to extract local features. Through discovering a description of one class objects with the derived local features, LFA is a purely second-order statistic method.

The recently proposed local binary pattern (LBP) features are originally designed for texture description [23,24,26]. The operator has been successfully applied to facial expression analysis [27], background modeling [22] and face recognition [21]. In face recognition, it achieves a much better performance than Eigenface, Bayesian and EBGM methods, providing a new way of investigating into the face representation. The idea behind using the LBP features is that a texture can be seen as a composition of micropatterns [21]. LBP in nature represents the first-order circular derivative pattern of images, a micropattern generated by the concatenation of the binary gradient directions. However, the first-order pattern fails to extract more detailed information contained in the input object. To the best of our knowledge, no high-order local pattern operator has been investigated for texture analysis. In fact, the high-order operator can capture more detailed discriminative information. A novel object descriptor, the high order Local Derivative Pattern (LDP) is proposed by Baochang Zhang et al [20]. LBP can conceptually considered as a non-directional first order local pattern, which is the binary result of the first order derivative image. The second order LDP can capture the change of derivative directions among local neighbors, and encode the turning point in a given direction.

The present paper computes the texture unit(TU) and texture spectrum by using second, third and fourth order LDPs in 00, 450, 900and 1350 on original texture images. Later a classification method has been introduced to classify and to find accuracy rate of classification. For this purpose the present paper is organized as follows. Methodology is defined in the second section while in the third section results and discussions are given. The last section deals with conclusions.

II. METHODOLOGY

Derived from a general definition of texture in a local neighborhood, LBP is defined as a grayscale invariant texture measure and is a useful tool to model texture images. The LBP operator labels the pixels of an image by thresholding the 3× 3 neighborhood of each pixel with the value of the central pixel and concatenating the results binomially to form a number. The thresholding function

forthe basic LBP can be formally represented in Fig. 1(a) and it is represented in equation 1.

$$E_i = \begin{Bmatrix} 0 \ \ if \ \ V_i < V_0 \\ 1 \ \ if \ \ V_i \geq V_0 \end{Bmatrix} \quad for \quad i = 1,2,...8 \qquad .....(1)$$

where Ei, i=1,2…8 , is an 8-neighborhood point around E0 as shown in Fig. 1. Fig. 1(b) shows an example of obtaining an LBP. The resultant LBP for this is 101001111.

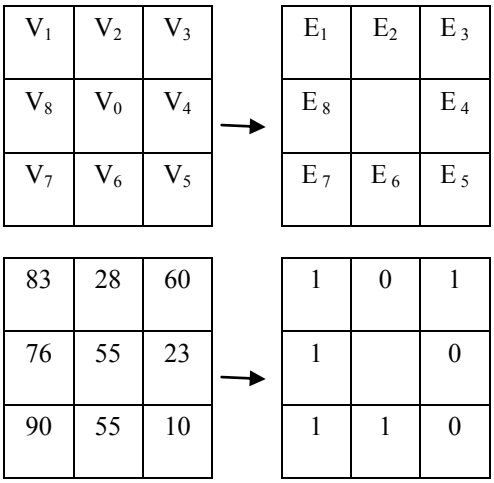


Fig. 1 (a)LBP representation(b)Example of obtaining the LBP

A. *Local Derivate Pattern (Ldp)*

Given an image *I(V)*, the first-order derivatives along 0^0, 45^0, 90^0 and 135^0 directions are denoted as $I'_\alpha(V)$where $\alpha=0^0$, 45^0, $90^0$and 135^0. Let V_0 be a point in *I(V)* , and V_i,i=1,…8 be the neighboring point around V_0 (see Fig. 1(a)). The four first-order derivatives at $V=V_0$are given in equations 2, 3, 4 and 5 for 0^0, 45^0, $90^0$and 135^0respectively[20].

$$I'_{0^0}(V_0) = I(V_0) - I(V_4) \qquad (2)$$
$$I'_{45^0}(V_0) = I(V_0) - I(V_3) \qquad (3)$$
$$I'_{90^0}(V_0) = I(V_0) - I(V_2) \qquad (4)$$
$$I'_{135^0}(V_0) = I(V_0) - I(V_1) \qquad (5)$$

The second-order directional LDP, $LDP^2_\alpha(V_0)$, in α direction at $V=V_0$ is defined as

$$LDP^2_\alpha(V_0) = \{f(I'_\alpha(V_0), I'_\alpha(V_1)), f(I'_\alpha(V_0), I'_\alpha(V_2)), \\ ...f(I'_\alpha(V_0), I'_\alpha(V_7)), f(I'_\alpha(V_0), I'_\alpha(V_8))\} \qquad (6)$$

where f(.,.) is a binary coding function determining the types of local pattern transitions. It encodes the co- occurrence of two derivative directions at different neighboring pixels as

$$f(I'_\alpha(V_0), I'_\alpha(V_i)) = \begin{cases} 0 & if \quad I'_\alpha(V_i) I'_\alpha(V_0) > 0 \\ 1 & if \quad I'_\alpha(V_i) I'_\alpha(V_0) \leq 0 \end{cases} \quad i = 1,2,...8 \quad (7)$$

Finally, the second-order Local Derivative Pattern, $LDP^2(V)$, is defined as the concatenation of the four 8-bit directional LDPs as given in equation 8.

$$LDP^2(V) = \{LDP^2_\alpha(V) \mid \alpha = 0^0, 45^0, 90^0, 135^0\} \qquad (8)$$

To calculate the third-order Local Derivative Pattern, we first compute the second-order derivatives along 0^0, 45^0, 90^0 and 135^0 directions, denoted as $I''_\alpha(V)$ where $\alpha=0^0, 45^0, 90^0, 135^0$. The third-order Local Derivative Pattern, $LDP^3_\alpha(V_0)$, in α direction at $V=V_0$ is defined as

$$LDP^3_\alpha(V_0) = \{f(I''_\alpha(V_0), I''_\alpha(V_1)), f(I''_\alpha(V_0), I''_\alpha(V_2)), \\ ...f(I''_\alpha(V_0), I''_\alpha(V_7)), f(I''_\alpha(V_0), I''_\alpha(V_8))\} \qquad (9)$$

where f(.,.) is difined as

$$f(I''_\alpha(V_0), I''_\alpha(V_i)) = \begin{cases} 0 & if \quad I''_\alpha(V_i) I''_\alpha(V_0) > 0 \\ 1 & if \quad I''_\alpha(V_i) I''_\alpha(V_0) \leq 0 \end{cases} \quad i = 1,2,...8 \quad (10)$$

$$LDP^3(V) = \{LDP^3_\alpha(V) \mid \alpha = 0^0, 45^0, 90^0, 135^0\} \qquad (11)$$

In a general formulation, the n^{th} order LDP is a binary string describing gradient trend changes in a local region of directional $(n-1)^{th}$ order derivative images $I'_\alpha(V)$as

$$LDP^n_\alpha(V_0) = \{f(I^{n-1}_\alpha(V_0), I^{n-1}_\alpha(V_1)), f(I^{n-1}_\alpha(V_0), I^{n-1}_\alpha(V_2)), \\ ...f(I^{n-1}_\alpha(V_0), I^{n-1}_\alpha(V_7)), f(I^{n-1}_\alpha(V_0), I^{n-1}_\alpha(V_8))\} \qquad (12)$$

where $I^{n-1}_\alpha(V_0)$ is the $(n-1)^{th}$ order derivative in α direction at $V= V_0$. $f(I^{n-1}_\alpha(V_0), I^{n-1}_\alpha(V_i))$is defined in (11), which encodes the $(n-1)^{th}$ -order gradient transitions into binary patterns, providing an extra order pattern information on the local region.

$$f(I^{n-1}_\alpha(V_0), I^{n-1}_\alpha(V_i)) = \begin{cases} 0 & if \quad I^{n-1}_\alpha(V_i) I^{n-1}_\alpha(V_0) > 0 \\ 1 & if \quad I^{n-1}_\alpha(V_i) I^{n-1}_\alpha(V_0) \leq 0 \end{cases} \quad i = 1,2,...8 \quad (13)$$

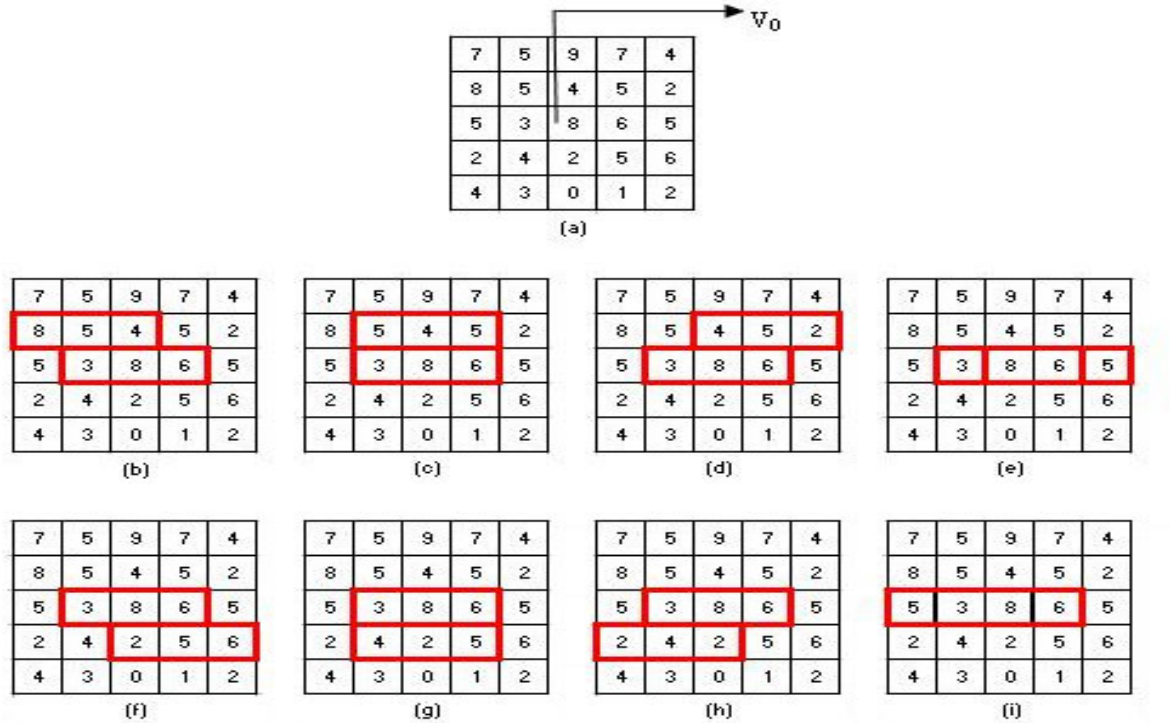


Fig. 2. Example to obtain the third order LDP(a) Original image (b) $f(I_0''(V_0), I_0''(V_1))$ ***(c)*** $f(I_0''(V_0), I_0''(V_2))$ ***(d)*** $f(I_0''(V_0), I_0''(V_3))$ ***(e)*** $f(I_0''(V_0), I_0''(V_4))$ ***(f)*** $f(I_0''(V_0), I_0''(V_5))$ ***(g)*** $f(I_0''(V_0), I_0''(V_6))$ ***(h)*** $f(I_0''(V_0), I_0''(V_7))$ ***(i)*** $f(I_0''(V_0), I_0''(V_8))$.

B. Algorithm For Evaluating Percentage Of Correct Classification On Images Using Local Derivative Pattern (LDP)

Begin

i. Take input Brodatz Textures Tk, k= 1 to 12.
ii. Subdivide the Tk , into 16 equal sized blocks. Name them as subimage TkSi, k=1 to 12 and i = 1 to 16.
iii. Select at random, a training sample sub image from each Tk, k= 1to 12 and denote it as TkSj where ‗j' is any of the sample pieces 1 to 16 of a particular Tk.
iv. Calculate the LDP and Texture Spectrum for the second, third and fourth order LDPs by moving the 3×3 matrix across the sample with overlapping (Convolving), for TkSj.
v. To obtain Texture Spectrum value of testing subimage repeat step 3 for TkSm k= 1 to 12, m=1 to 16($m \neq j$).
vi. To classify a subimage TkSm, the distance between the training set and the testing samples is measured.
vii. The tested set falls into the Class k, k= 1 to 12, such that D (k) is minimum among all the D (k), k=1to 12.
viii. w for each texture Tk, k=1 to 12, we evaluate the percentage of correct classification (PCC) and list the output in the form of table.

$$PCC_k = \frac{Number\ of\ subimages\ correctly\ classified}{Number\ of\ subimages\ considered\ for\ testing} \times 100$$

End

III. RESULTS AND DISCUSSIONS

The Table 1 shows the percentage of correct classification (PCC) on 12 Brodatz textures [28] using original images derived from the second, third and fourth order LDPs respectively. The tables clearly indicate that for second order LDP the PCC is around 92% which has decreased to 83% for third order LDP and fourth order LDP. By using second order LDP except the textures D_1, D_4, D_5 and D_9 the remaining eight textures showing a PCC of 100%. But it is little bit different for third and fourth order LDPs. The PCC is also shown with the help of a graph in Fig. 3.

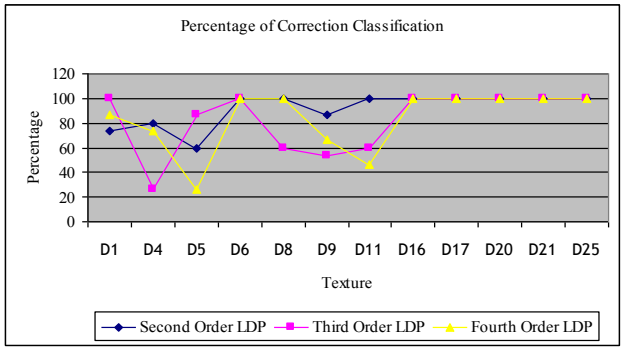


Fig. 3. Percentage of Correct Classification of Brodatz Textures

IV. Conclusions

This paper proposed a new method of texture classification using high order local patterns: Local Derivative Patterns (LDP). The second, third and fourth order LDP in the four directions i.e. 00, 450, 900 and 1350 are calculated from which texture spectrum is obtained. By using this texture spectrum the percentage of correct classification is obtained. The LDP extract high order local information by encoding various distinctive spatial relationships contained in a given local region. The experimental results clearly indicate that the percentage of correct classification for second order LDP is good when compared with third and fourth order LDP.

Table 1: Percentage of Correct Classification for the Brodatz Textures

Texture	Second Order LDP	Third Order LDP	Fourth Order LDP
D_1	73.33	100.00	86.67
D_4	80.00	26.67	73.33
D_5	60.00	86.67	26.67
D_6	100.00	100.00	100.00
D_8	100.00	60.00	100.00
D_9	86.67	53.33	66.67
D_{11}	100.00	60.00	46.67
D_{16}	100.00	100.00	100.00
D_{17}	100.00	100.00	100.00
D_{20}	100.00	100.00	100.00
D_{21}	100.00	100.00	100.00
D_{25}	100.00	100.00	100.00
Avg.	**91.67**	**82.22**	**83.33**

V. Acknowledgements

The authors would like to express their gratitude to Dr M. Santhi Ramudu, Chairman, and Mr. M Siva Ram, Managing Director Rajeev Gandhi Memorial College of Engineering and Technology for providing necessary infrastructure. Authors would like to thank Dr. Vakulabharanam Vijaya Kumar for his invaluable guidance which led to improvise the quality of this paper.

VI. References

1) Bovik, A. C., Clark, M. and Geisler, W. S. Multichannel texture analysis using localized spatial filters, IEEE Trans. Patt. Anal. Mach. Intell., 12, 1, pp. 55-73, 1990.
2) Chang. T, and Kuo, C. C. J., Texture analysis and classification with tree-structured wavelet transform, IEEE Trans. Image Processing, 2, 4, pp. 429-442, 1993.
3) Chen, J. L. and Kundu, Unsupervised texture segmentation using multi-channel decomposition and hidden Markov models, IEEE Trans. Image. Processing, 4, 5, pp. 603-620, 1995.
4) Conners, R. W. Toward a set of statistical features which measure visually perceivable qualities of texture, in Proc. Pattern Recognition Image Processing Conf., pp. 382-390, 1979.
5) D'Astous, F. and Jernigan, M. E. Texture discrimination based on detailed measures of power spectmm, in Proc. IEEE Comput. Soc. Con5 on Pattern Recogn. and Image Process., pp. 83-86, 1984.
6) Eswara Reddy, B., Nagaraja Rao, A., Suresh, A. and Vijaya Kumar, V. Texture Classification by simple patterns on edge direction movements, IJCSNS, Vol.7 No.11, pp. 220-225, 2007.
7) Haralick, R. M. et al., Texture features for image classification, IEEE Trans. Syst. Man Cybern. SMC-3, 6, pp. 610-621, 1973.
8) Haralick, R. M. Statistical and structural approaches to texture, Proc. of 4th Int. Joint Conf. Pattern Recognition, pp. 45-60, 1979.
9) He, D. C. and Wang, L. Textural filters based on the texture spectrum, Patt. Recogn. 24, 12, pp.1187-1195, 1991.
10) Krishna, V. V., Vijaya Kumar, V ., Raju, U.S.N., Saritha, B. Classification of textures based on distance function of linear patterns using mathematical morphology, Proceedings of ICEM, conducted by JNT University, India, 2005.
11) Mallat, S. Multi frequency Channel Decomposition of Images and Wavelet Models, IEEE Trans. Acoustic, Speech and Signal Processing, 37, 12, pp. 2091-2110, 1989.
12) Raju, U.S.N., Vijaya Kumar, V. , Suresh, A. and Radhika Mani, M. Texture Description using Different Wavelet Transforms Based on Statistical Parameters,proceedings of the 2nd WSEAS International Symposium on WAVELETS THEORY & APPLICATIONS in Applied Mathematics, Signal Processing & Modern Science (WAV '08), Istanbul, Turkey, pp. 174-178, 2008.
13) Salari, E. and Ling, Z. Texture segmentation using hierarchical wavelet decomposition, Patt. Recogn. 28, 12, pp.1819-1824, 1995.
14) Suresh, A., Raju, U.S.N., Nagaraja Rao, A. and Vijaya Kumar, V., An Innovative Technique of Marble Texture Description Based on Grain Components,International Journal of Computer Science and Network Security, Vol.8 No.2, pp. 122-126, 2008.
15) Van Gool, L., Dewaele, P. and Oosterlinck, A. Survey-texture analysis anno 1983, Computer Vision, Graphics Image Processing, Vol. 29, PP. 336-357, 1985.
16) Vijaya Kumar, V. , Eswara Reddy, B., Raju, U.S.N. and Suresh, A. Classification of Textures

by Avoiding Complex Patterns, Science publications, Journal of Computer Science , 2008.
17) Vijaya Kumar, V., Eswara Reddy, B. ,Raju, U.S.N. and Chandra Sekharan, K. An Innovative Technique of Texture Classification and Comparison Based on Long Linear Patterns, Journal of Computer Science 3 (8): pp.633-638, 2007.
18) Vijaya Kumar, V., Eswara Reddy, B. and Raju, U.S.N. A measure of patterns trends on various types of preprocessed images, IJCSNS, Vol.7 No.8, pp. 253-257, 2007.
19) Vijaya Kumar, V., Raju, U.S.N. , Chandra Sekaran, K. and Krishna, V. V. A New Method of Texture Classification using various Wavelet Transforms based on Primitive Patterns, ICGST International Journal on Graphics, Vision and Image Processing, GVIP, Vol.8, Issue 2, pp. 21-27, 2008.
20) Baochang Zhang, Yongsheng Gao, et. Al. ―Local Derivative Pattern Versus Local Binary Pattern: Face Recognition with High-order Local Pattern Descriptor" IEEE Trans. On Image Processing, Vol. 19, No.2, 2010.
21) Ahonen T., Hadid A., and Pietikainen M., ―Face description with local binary patterns: Application to face recognition," IEEE Trans. Pattern Anal. Mach. Intell., vol. 28, no. 12, pp. 2037-2041, 2006.
22) Heikkila M. and Pietikainen M., ―A texture-based method for modeling the background and detecting moving objects," IEEE Trans. Pattern Anal. Mach. Intell., vol. 28, no. 4, pp. 657-662, 2006.
23) Ojala T., Pietikainen M., and Harwood D., ―A comparative study of texture measures with classification based on feature distributions," Pattern Recognit., vol. 29, no. 1, pp. 51-59, 1996.
24) Ojala T., Pietikainen M., and Maenpaa T., ―Multiresolution gray-scale and rotation invariant texture classification with local binary patterns," IEEE Trans. Pattern Anal. Mach. Intell., vol. 24, no. 7, pp. 971-987, 2002.
25) Penev P. S. and Atick J. J., ―Local feature analysis: A general statistical theory for object representation," Network: Comput. Neural Syst., vol. 7, no. 3, pp. 477-500, 1996.
26) Pietikaainen M., Ojala T., and Z. Xu, ―Rotation-invariant texture classification using feature distributions," Pattern Recognit., vol. 33, no. 1, pp. 43-52, 2000.
27) Zhao G. and Pietikaainen M., ―Dynamic texture recognition using local binary patterns with an application to facial expressions," IEEE Trans. Pattern Anal. Mach. Intell., vol. 29, no. 6, pp. 915–928, Jun. 2007.
28) Brodatz, P. Textures A Photographic for Artists and Designers, Dover, NY, 1966.

Information SecurityUsingThreshold Cryptography With Paillier Algorithm

[1]Machha.Narender, [2]G.N.Ramesh [3]P.Ranganath

GJCST Classification
D.4.6,K.6.5

,

Abstract-The dynamic and cooperative nature of ad hoc networkspresent challenges in securing these networks. There arerecent research efforts in securing ad hoc networks. Amongstsecurity approaches, there are threshold cryptography andauthentication. In this paper we survey the thresholdcryptography based schemes and the authentication schemesthat have been proposed to secure ad hoc networks. Weconclude this paper and identify the challenges and openresearch areas associated with each of these approaches.The idea of threshold cryptography is to protect information(or computation) by fault-tolerantly distributing it among acluster of cooperating computers. First consider thefundamental problem of threshold cryptography, a problemof secure sharing of a secret. A secret sharing scheme allowsone to distribute a piece of secret information among severalservers in a way that meets the following requirements: (1)no group of corrupt servers (smaller than a given threshold)can figure out what the secret is, even if they cooperate; (2)when it becomes necessary that the secret information bereconstructed, a large enough number of servers (a numberlarger than the above threshold) can always do it.

I. Introduction

ThresholdCryptographyis the art of chopping asecret into little bits. Only by possessing morethan a threshold number of bits of the secret canthe secret be determined. Algorithms exist tobreak any secret up such that at least and exactlyM out of N holders of pieces of the secret mustgive approval (and their partial secret or key) inorder to compute the total secret (e.g. 3 of 5, 3 of12, 5 of 12, etc.). Removing probability has acost, though... a secret must be broken into C(N,M-1) pieces and each holder carries (NM+1)/N parts of the whole key... so '3 of 12' ismore expensive per-node than '5 of 12'. (Thesenumbers come from the pigeonhole principle andconstraints: any piece 'pK' must be found on NM+1 holders so that access to a full M secretholdersguarantees 'pK' will be known, whilstaccess to M-1 computers must guarantee thatthere is at least one piece not found, so 'pK' mustNOT be with the other M-1 computers Theminimum number of component 'pK' elements todo this is (N) Choose (M-1). Individual pKelements can be made artificially large in orderto subvert guessing of one or two missing pieces;the combinatory function needn't be straightforward appended. However, Thecomputation and storage cost of this approach ishigh, and it may do well to combine it with somestraightforward split-and-distribute as listedabove; e.g. splitting the 'require 5 of 7 pieces' to'more than 7' people is the natural extension tosplitting 'require 3 of 3 pieces' to '12 people'. Thecombined effect can avoid the massive costs ofsplitting and storing, say '5 of 20' parts (C(20,4)unique parts, every node holding ~16/20ths oftotal secret, vs. C(7,4) parts with each nodeholding 3/7ths of total secret). The mainadvantage of mixing in this algorithmic divisionapproach is in achieving better guarantees as toredundancy and survivability whilesimultaneously increasing the number of usersone must access to possess the whole secret. E.g.for the other approach, to require 5 users wouldrequire splitting the key into 5 pieces anddivvying that up among, say, 15 people; it wouldtake access to 5 people to gain the secret, and thesecret could be lost by losing 3 people. Splittingit to 5 of 7 first, then dividing the 7 chunksamong 14 people results in 2 different peoplehaving a copy of any given chunk, and the secretwon't be lost before losing 6 people (losing threewhole chunks).

As a security measure, Threshold Cryptography requires that many systems must be compromised prior to taking control of a secret,inherently including resistance to snooping orabuse by any super users of the computationresource (who would have the ability to do so ifthe secret were wholly on one system). It alsoprovides inherent redundancy of the secret... e.g.if you can guarantee that it takes at least and atmost 5 of 12 secret-holders to build the secret,you can guarantee that a failure of up to 7systems is tolerable without failure. With aprobabilistic split, you can easily calculate apercentage chance that the data is unavailable foreach loss of node... and, with intelligent split ofcomponents, you can guarantee that at least somecount of nodes must be lost before the data hasany chance of being lost.In the case of authorization to access a differentsystem (e.g. to control a power plant), securitycan be increased further by demanding that a fewparts of the approval come from –particularpeoplethat are known to still be accessible... andby changing these people at regular intervals.This makes it much more difficult to gain accesseven by compromising the systems... becauseyou can't easily know which particular systemsought to be compromised.

II. Motivation

The strongest reason for using this mechanismover straightforward encryption is that a secretmight need to be available to users that can onlyprovide a -certificate-authorizing access to a fileor service, and the primary

[1]*Machha.Narender, Assistant Professor, HITS College of Engg, machha.narender@gmail.com*
[2]*G.N.Ramesh, Assistant Professor, Bhoj Reddy Engg College , noya.ramesh@gmail.com.*
[3]P.Ranganath, Assistant Professor, Asifia Engg College, ranganathponnaboyina@gmail.com

encryption isn'tagainst any key with which individuals sharelong-term access (there is no shared key). E.g.one can use ThresholdCryptography to encryptfiles or split keys requiring, say, either 'Secret'clearance with 'Power Grid' specialization, or'Top Secret' clearance, represented as acertificate signed by a government master keynot in expiration, and any individual that canprove to M of N systems that he or she possessesthe necessary clearances will be provided thecapability to actually perform the task. Keydistribution is a difficult problem, doubly sowhen you won't trust that any one keydistribution server hasn't been compromised;ThresholdCryptography is one of the moreelegant answers to that particular problem. Avery useful extension of secret sharing isfunction sharing. Its main idea is that a highlysensitive operation, such as decryption orsigning, can be performed by a group ofcooperating servers in such a way that nominority of servers is able to perform thisoperation by themselves, nor would they be ableto prevent the other servers from performing theoperation when it is required.

In many real-life situations, we don't believe that any given person can be trusted, and we may even suspect that a big fraction of all people are dishonest, yet it is reasonable to assume that the majority of people are trustworthy. Similarly, in on-line transactions, we may doubt that a given server can be trusted, but we hope that the majority of servers are working properly. Based on this assumption, we can create trusted entities. A good example of an application whose security could be greatly improved with a threshold solution is a network Certification Authority, a trusted entity that certifies that a given public key corresponds to a given user. If we trust one server to perform this operation,then it is possible that as a result of just one break-in, no certificate can any longer be trusted.Thus it is a good idea to distribute the functionality of the certification authority between many servers, so that an adversary would need to corrupt half of them before he can forge a certificate on some public key.

Goals: In the threshold setting, we would like toimplement, via efficient protocols, the mostsecure cryptosystems and signature schemes. Wewould also like to make our protocols secure inthe strongest possible model of faults. Thefollowing are some of the various considerationswe make when modeling computer faults

A. *The Size Of The Threshold*

What fractionof the servers can be corrupted by theadversary without any harm to theservice (e.g. signature or decryption)that these servers implement?

B. *Efficiency Considerations*

How muchcommunication, storage, andcomputation dothese fault-tolerantprotocols require?

C. *Model Of Communication*

How realisticare the requirements we place on it? Dowe require synchronous or partiallysynchronous communication,authenticated broadcast and secure linksbetween servers?

D. *Type Of Adversary We Tolerate*

Howdoes the adversary choose whichplayers to corrupt? Can a serversecurely erase its local data so that itcannot be retrieved by the adversaryonce the server is infiltrated?

III. PAILLIER CRYPTOSYSTEM ALGORITHM

A. *Key Generation*

i. Choose two large prime numbers p and q randomly and independently of each other such that $\gcd(pq, (p-1)(q-1)) = 1$. This property is assured if both primes are of equivalent length, i.e., $p, q \in 1||\{0,1\}^{s-1}$ for security parameter s.
Compute $n = pq$ and $\lambda = \mathrm{lcm}(p-1, q-1)$

ii. Select random integer g where $g \in \mathbb{Z}_{n^2}^*$

iii. Ensure n divides the order of g bychecking the existence of the followingmodular multiplicative inverse $\mu = (L(g^{\lambda} \mod n^2))^{-1} \mod n$

Where function L is defined as $L(u) = \frac{u-1}{n}$.

Note that the notationdoes not denote the modular multiplication of$a$ times the modular multiplicative inverse of$b$but rather the quotient of a divided by b,i.e., the largest integer value $v \geq 0$ to satisfy the relation $a \geq vb$.

a. *The Public (Encryption) Key Is (N, G).*
b. *The private (decryption) key is (λ, μ).*

If using p, q of equivalent length, a simpler variant of the above key generation steps would be to set $g = n+1, \lambda = \varphi(n)$, And $\mu = \varphi(n)^{-1} \mod n$where $\varphi(n) = (p-1)(q-1)$.

IV. ENCRYPTION

i. Let m be a message to be encryptedwhere $m \in \mathbb{Z}_n$

ii. Select random r where $r \in \mathbb{Z}_n^*$

iii. Compute cipher text as $c = g^m \cdot r^n \mod n^2$

V. DECRYPTION

i. Cipher text $c \in \mathbb{Z}_{n^2}^*$

ii. Compute message $m = L(c^{\lambda} \mod n^2) \cdot \mu \mod n$

As the original paper points out, decryption is"essentially one exponentiation modulo n^2."

VI. HOMOMORPHIC PROPERTIES

A notable feature ofthe Paillier cryptosystem isits homomorphic properties. As the encryptionfunction is additively homomorphic, thefollowing identities can be described:

A. Homomorphic Addition Of Plaintexts

The product of two cipher texts will decrypt to the sum of their corresponding plaintexts,

$$D(E(m_1, r_1) \cdot E(m_2, r_2) \mod n^2) = m_1 + m_2 \mod n.$$

The product of a cipher text with A plaintext raising g will decrypt to the sum of the corresponding plaintexts,

$$D(E(m_1, r_1) \cdot g^{m_2} \mod n^2) = m_1 + m_2 \mod n.$$

B. Homomorphic Multiplication OfPlaintexts

An encrypted plaintext raised to the power of another plaintext will decrypt to the product of the two plaintexts,

$$D(E(m_1, r_1)^{m_2} \mod n^2) = m_1 m_2 \mod n,$$
$$D(E(m_2, r_2)^{m_1} \mod n^2) = m_1 m_2 \mod n.$$

More generally, an encrypted plaintext raised to a constant *k* will decrypt to the product of the plaintext and the constant,

$$D(E(m_1, r_1)^k \mod n^2) = k m_1 \mod n.$$

However, given the Paillier encryptions of two messages there is no known way to compute an encryption of the product of these messages without knowing the private key.

VII. Semantic Security

The original cryptosystem as shown above doesprovide semantic security against chosenplaintextattacks (IND-CPA). The ability tosuccessfully distinguish the challenge cipher textessentially amounts to the ability to decidecomposite residuosity. The so-called decisionalcomposite residuosity assumption (DCRA) isbelieved to be intractable.Because of the aforementioned homomorphicproperties however, the system is malleable, andtherefore does not enjoy the highest echelon ofsemantic security that protects against adaptivechosen-cipher text attacks (IND-CCA2). Usuallyin cryptography the notion of malleability is notseen as an "advantage," but under certainapplications such as secure electronic voting andthreshold cryptosystems, this property mayindeed be necessary.Paillier and Point cheval however went on topropose an improved cryptosystem thatincorporates the combined hashing of message mwith random r. Similar in intent to the Cramer-Shoup cryptosystem, the hashing prevents anattacker, given only c, from being able to changem in a meaningful way. Through this adaptationthe improved scheme can be shown to be INDCCA2secure in the random oracle model.

VIII. Applications

A. Electronic voting

Semantic security is not the only consideration.There are situations under which malleabilitymay be desirable. The above homomorphicproperties can be utilized by secure electronicvoting systems. Consider a simple binary ("for" or "against") vote. Let m voters cast a vote of either *1* (for) or *0* (against). Each voter encryptstheir choice before casting their vote. Theelection official takes the product of the *m*encrypted votes and then decrypts the result andobtains the value*n,* which is the sum of all thevotes. The election official then knows that npeople voted for and *m-n* people voted against.The role of the random *r* ensures that twoequivalent votes will encrypt to the same valueonly with negligible likelihood, hence ensuringvoter privacy.

B. Electronic Cash

Another feature named in paper is the notion ofself-blinding. This is the ability to change onecipher text into another without changing thecontent of its decryption. This has application tothe development of electronic cash, an effortoriginally spear-headed by David Chaum.Imagine paying for an item online without thevendor needing to know your credit cardnumber, and hence your identity. The goal inboth electronic cash and electronic voting is toensure the e-coin (likewise e-vote) is valid, whileat the same time not disclosing the identity of theperson with whom it is currently associated.

IX. Conclusion

A new threshold Signing scheme is proposed in this project that when combined with Shared Paillier secret keys generation will leads us to a complete solution for the Threshold Paillier problem. The complete solution has also been implemented successfully in this project.

X. References

1) Adam Barnett and Nigel P.Smart. Mental Poker Revisited. Cryptography and Coding 2003, Springer-Verlag LNCS 2898.
2) M. Bellare and P. Rogaway. Random oracles are practical: a paradigm for Designing e_client protocols. Proc. 1st ACM Conference on Computer and Communications Security, 1993, 62–73, 1993.
3) Benaloh. Secret sharing homomorphisms:keeping shares of a secret. Advances in Cryptography - CRYPTO ‘86. Lecture notes in Computer Science,vol. 263. Springer- Verlag, New York, LNCS 263.
4) Ben-Or, M. Goldwasser and Wigderson.Completeness theorems for noncryptographicfault-tolerant distributed computation.Proceeding of the 20th Annual ACMSymposium on Theory of Computing.Chicago, 11, May 2-4. ACM,
5) D.Boneh and M. Franklin. E_client generation of shared RSA keys. Advances in Cryptography – CRYPTO ‘97, Springer-Verlag LNCS 1233, 425–439, 1997.
6) Dan Boneh and Matthew Franklin. E_cientGeneration of shared RSA Keys. J. ACM,48, 702-722, 2001.
7) Boyd. Digital Multisignatures. Cryptographyand Coding 1989. Instituteof Mathematics and its application, IMA. 241–246,Clarendon Press, 1989.

Intrusion Detection System For Adhoc Networks

[1]M.Narender, [2]B.V.Suresh Kumar,

GJCST Classification
C.2.0,D.4.6

***Abstract*-The rapid proliferation of wireless networks and mobile computing applications has changed thelandscape of network security. The recent denial of service attacks on major Internet sites have shown us, no open computer network is immunefrom intrusions. The wireless ad-hoc network is particularly vulnerable due to its featuresof open medium, dynamic changing topology, cooperative algorithms, lack of centralizedmonitoring and management point, and lack of a clear line of defense. The traditionalway of protecting networks with firewalls and encryption software is no longer sufficientand effective. Many intrusion detection techniques have been developed on fixed wirednetworks but have been turned to be inapplicable in this new environment. We need tosearch for new architecture and mechanisms to protect wireless networks and mobilecomputing application. In this paper, we examine the vulnerabilities of wireless networksand say that we must include intrusion detection in the security architecture for mobilecomputing environment. We have showed such architecture and evaluated keymechanisms in this architecture such as applying mobile agents to intrusion detection,anomaly detection and misuse detection for mobile ad-hoc networks**.

Keywords-Intrusion, firewall, Adhoc networks, Route Discovery and Route maintenance.

I. INTRODUCTION

In the last three years, the networking revolution has finallycome of age. More than ever before, we see that the Internet is changing computing, aswe know it. The possibilities and opportunities are limitless; unfortunately, so too are therisks and chances of malicious intrusions. It is very important that the securitymechanisms of a system are designed so as to prevent unauthorized access to systemresources and data. However, completely preventing breaches of security appear, atpresent, unrealistic. We can, however, try to detect these intrusion attempts so that actionmay be taken to repair the damage later. This field of research is called IntrusionDetection.

A. Computer Security And Its Role

One broad definition of a secure computer system is given by Garfinkel and Spafford asone that can be depended upon to behave as it is expected to. It is always a point of benefit to integrate security with dependability and how to obtain a dependable computing. system. Dependability is the trustworthiness of a system and can be seen as the quality of the service a system offers.Integrating security and dependability can be done in various ways. One approach is to treat security as one characteristic of dependability on the same level as availability, reliability and safety.

A narrower definition of security is the possibility for a system to protect objects with respect to confidentiality, authentication, integrity and non-repudiation.

B. Threats Of Security

Threats can be seen as potential violations of security and existbecause of vulnerabilities, i.e. weakness, in a system. There are two basic types ofthreats: accidental threats and intentional threats.

i. Accidental Threat

An accidental threat can be manifested and the result is eitheran exposure of confidential information or cause of an illegal system state to occur i.e.modification of an object. Exposures can emerge from both hardware and softwarefailures as well as from user and operational mistakes thus resulting in the violation ofconfidentiality. It can also be manifested as modification of an object, which is theviolation of object integrity. An object here can be both information and resource.

ii. Intentional Threat

An intentional threat is an action performed by an entity withthe intention to violate security. Examples of attacks are interruption, modification,interception and fabrication of data.

C. Vulnerabilities Of Mobile Wireless Networks

The nature of mobile computing environment makes it very vulnerable to an adversary'smalicious attacks.

Firstly, the use of wireless links renders the network susceptible to attacks rangingfrom passive eavesdropping to active interfering as attacks on these links can from anydirection and target at any node. This means that a wireless ad-hoc network will not have A clear line of defense, and every node has to be prepared for encounters with anadversary directly or indirectly.

Secondly, mobile nodes are autonomous units that are capable of roaming independently.Since tracking down a particular mobile node in a global scale network cannot be doneeasily, attacks by compromised node from within the network are more damaging andharder to detect.

Third, decision-making in mobile computing environment is sometimes decentralized andsome wireless networkalgorithms rely on the cooperative participation of all nodes andthe infrastructure. Furthermore, mobile

[1]*M.Narender, Asst.prof. of CSE dept, HITS college of Engg, Hyderabad. Machha.narender@gmail.com*
[2]*B.V.Suresh Kumar, Asst. prof. of IT dept, MLEC, Singarayakonda Prakasam(dt), sureshkumar1239@gmail.com*

computing has introduced new type ofcomputational and communication activities that seldom appear in fixed or wiredenvironment. Applications and services in a mobile wireless network can be a weak linkas well.

D. Need For Intrusion Detection

A computer system should provide confidentiality, integrity and assurance against denialof service. However, due to increased connectivity (especially on the Internet), and the vast spectrum of financial possibilities that are opening up, more and more systems aresubject to attack by intruders. These subversion attempts try to exploit flaws in theoperating system as well as in application programs and have resulted in spectacular incidents like the Internet Worm incident of 1988.

There are two ways to handle subversion attempts. One way is to prevent subversionitself by building a completely secure system. We could, for example, require all users to identify and authenticate themselves; we could protect data by various cryptographicmethods and very tight access control mechanisms.

The history of security research has taught us a valuable lesson – no matter how manyintrusion prevention measures are inserted in a network, there are always some weaklinks that one could exploit to break in. We thus see that we are stuck with systems thathave vulnerabilities for a while to come. If there are attacks on a system, we would like todetect them as soon as possible (preferably in real-time) and take appropriate action. This isessentially what an Intrusion Detection System (IDS) does. An IDS does not usuallytake preventive measures when an attack is detected; it is a reactive rather than pro-activeagent. It plays the role of an informant rather than a police officer.

II. Background on Intrusion Detection

In the last three years, the networking revolution has finally come of age. More than ever before, we see that the Internet is changing computing, as we know it. The possibilities and opportunities are limitless; unfortunately, so too are the risks and chances of malicious intrusions.

It is very important that the security mechanisms of a system are designed so as toprevent unauthorized access to system resources and data. However, completelypreventing breaches of security appear, at present, unrealistic. We can, however, try todetect these intrusion attempts so that action may be taken to repair the damage later.This field of research is called Intrusion Detection

A simple firewall can no longer provide enough security as in the past. Today'scorporations are drafting intricate security policies whose enforcement requires the use ofmultiple systems, both proactive and reactive (and often multi-layered and highlyredundant). The premise behind intrusion detection systems is simple: Deploy a set ofagents to inspect network traffic and look for the —signatures" of known network attacks.

However, the evolution of network computing and the awesome availability of theInternet have complicated this concept somewhat. With the advent of Distributed Denialof Service (DDOS) attacks, which are often launched from hundreds of separate sources,the traffic source no longer provides reliable temporal clues that an attack is in progress.Worse yet, the task of responding to such attacks is further complicated by the diversityof the source systems, and especially by the geographically distributed nature of mostattacks.

Intrusion detection techniques while often regarded as grossly experimental, the field ofintrusion detection has matured a great deal to the point where it has secured a space inthe network defense landscape alongside firewalls and virus protection systems. Whilethe actual implementations tend to be fairly complex, and often proprietary, the conceptbehind intrusion detection is a surprisingly simple one: Inspect all network activity (both inbound and outbound) and identify suspicious patterns that could be evidence ofA network or system attack.

A. Classification Of Intrusion Detection Systems

Intrusions can be divided into 6main types

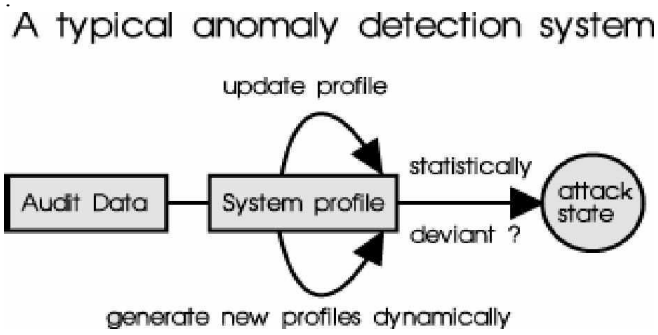
i. Attempted break-ins, which are detected by atypical behavior profiles or violations ofsecurity constraints.
ii. Masquerade attacks, which are detected by atypical behavior profiles or violations ofsecurity constraints.
iii. Penetration of the security control system, which are detected by monitoring forspecific patterns of activity.
iv. Leakage, which is detected by atypical use of system resources.
v. Denial of service, which is detected by atypical use of system resources.
vi. Malicious use, which is detected by atypical behavior profiles, violations of securityconstraints, or use of special privileges.

We can divide the techniques of intrusion detection into two main types.

B. Anomaly Detection

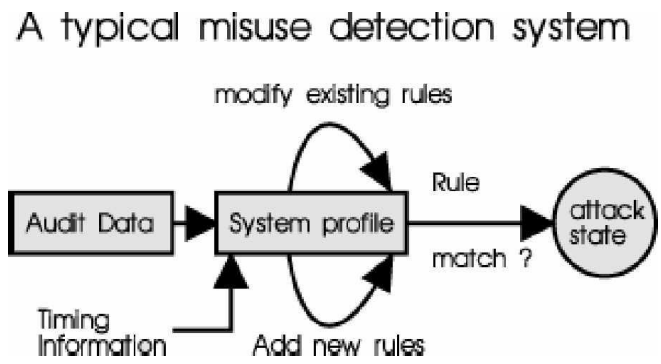
Anomaly detection techniques assume that all intrusiveactivities are necessarily anomalous. This means that if we could establish a "normalactivity profile" for a system, we could, in theory, flag all system states varying from theestablished profile by statistically significant amounts as intrusion attempts. However, ifwe consider that the set of intrusive activities only intersects the set of anomalousactivities instead of being exactly the same, we find a couple of interesting possibilities:(1) Anomalous activities that are not intrusive are flagged as intrusive. (2) Intrusiveactivities that are not anomalous result in false negatives (events are

not flagged intrusive,though they actually are). This is a dangerous problem, and is far more serious than theproblem of false positives.
The main issues in anomaly detection systems thus become the selection of thresholdlevels so that neither of the above 2 problems is unreasonably magnified, and theselection of features to monitor. Anomaly detection systems are also computationallyexpensive because of the overhead of keeping track of, and possibly updating severalsystem profile metrics. Some systems based on this technique are discussed in Section 4while a block diagram of a typical anomaly detection system is shown in Figure below



C. Misuse Detection

The concept behind misuse detection schemes is that there areways to represent attacks in the form of a pattern or a signature so that even variations ofthe same attack can be detected. This means that these systems are not unlike virus detection systems -- they can detect many or all known attack patterns, but they are oflittle use for as yet unknown attack methods. An interesting point to note is that anomaly detection systems try to detect the complement of "bad" behavior. Misuse detectionsystems try to recognize known "bad" behavior. The main issues in misuse detectionsystems are how to write a signature that encompasses all possible variations of thepertinent attack, and how to write signatures that do not also match non-intrusive activity.A block diagram of a typical misuse detection system is shown in Figure below.



D. Network Based Intrusion Detection

The most obvious location for an intrusiondetection system is right on the segment being monitored. Network-based intrusiondetectors insert themselves in the network just like any other device, except theypromiscuously examine every packet they see on the wire.

E. Host Based Intrusion Detection

While network-based intrusion detectors arestraightforward to deploy and maintain, there is a whole class of attacks closely coupledto the target system and extremely hard to fingerprint. These are the ones that exploitvulnerabilities particular to specific operating systems and application suites. Only hostbasedintrusion detection systems (the ones running as an application on a networkconnectedhost) can correlate the complex array of system-specific parameters that makeup the signature of a well-orchestrated attack.

III. Anomaly Detection Systems

There have been a few approaches to anomaly intrusion detection systems, some ofwhich are described below.

A. Statistical Approaches

In this method, initially, behavior profiles for subjects aregenerated. As the system continues running, the anomaly detector constantly generatesthe variance of the present profile from the original one. We note that, in this case, theremay be several measures that affect the behavior profile, like activity measures, CPUtime used, number of network connections in a time period, etc. In some systems, thecurrent profile and the previous profile are merged at intervals, but in some other systemsprofile generation is a one time activity.
An open issue with statistical approaches in particular, and anomaly detection systems ingeneral, is the selection of measures to monitor. It is not known exactly what the subset of all possible measures that accurately predicts intrusive activities is. Static methods ofdetermining these measures are sometimes misleading because of the unique features of A particular system. Thus, it seems that a combination of static and dynamic determinationof the set of measures should be done. Some problems associated with this techniquehave been remedied by other methods, including the method involving Predictive PatternGeneration, which takes past events into account when analyzing the data.

B. Predictive Pattern Generation

This method of intrusion detection tries to predict future events based on the events that have already occurred. Therefore, we could have A rule E1 - E2 --> (E3 = 80%, E4 = 15%, E5 = 5%) This would mean that given that events E1 and E2 have occurred, with E2 occurring after E1, there is an 80% probability that event E3 will follow, a 15% chance that event E4 will follow and a 5% probability that event E5 will follow.

Problem- The problem with this is that some intrusion scenarios that are not described bythe rules will not be

flagged intrusive. Thus, if an event sequence A - B - C exists that isintrusive, but not listed in the rule base, it will be classified as unrecognized.

Solution- The above problem can be partially solved by flagging any unknown events asintrusions (increasing the probability of false positives), or by flagging them as nonintrusive(thus increasing the probability of false negatives). In the normal case, however,an event is flagged intrusive if the left hand side of a rule is matched, but the right handside is statistically very deviant from the prediction.

C. *Neural Networks*

Another approach taken in intrusion detection systems is the useof neural networks. The idea here is to train the neural network to predict a user's nextaction or command, given the window of ‗n' previous actions or commands. The networkis trained on a set of representative user commands. After the training period, the networktries to match actual commands with the actual user profile already present in the net.Any incorrectly predicted events actually measure the deviation of the user from theestablished profile.

IV. MISUSE DETECTION SYSTEMS

There has been significant research in misuse detection systems in the recent past. Someof these systems are explained in depth in this section.

A. *Expert Systems*

These systems are modeled in such a way as to separate the rule matching phase from the action phase. The matching is done according to audit trail events. IDES follows a hybrid intrusion detection technique consisting of a misuse detection component as well as an anomaly detection component. The anomaly detector is based on the statistical approach, and it flags events as intrusive if they are largely deviant from the expected behavior. To do this, it builds user profiles based on many different criteria (more than 30 criteria, including CPU and I/O usage, commands used, local network activity, system errors etc.). These profiles are updated at periodic intervals. The expert system misuse detection component encodes known intrusion scenarios and attack patterns (bugs in old versions of send mail could be one vulnerability). The rule database can be changed for different systems.

B. *Keystroke Monitoring*

This is a very simple technique that monitors keystrokes for attack patterns. Unfortunately the system has several defects features of shells like *bash*, *ksh*, and*tcsh* in which user definable aliases are present defeat the technique unless alias expansion and semantic analysis of the commands is taken up. The method alsodoes not analyze the running of a program, only the keystrokes. This means that A malicious program cannot be flagged for intrusive activities. Operating systems do not offer much support for keystroke capturing, so the keystroke monitor should have a hook that analyses keystrokes before sending them on to their intended receiver. An improvement to this would be to monitor system calls by application programs as well, so that an analysis of the program's execution is possible.

C. *Model Based Intrusion Detection*

States that are certain scenarios are inferred bycertain other observable activities. If these activities are monitored, it is possible to findintrusion attempts by looking at activities that infer a certain intrusion scenario. Themodel-based scheme consists of three important modules. The anticipator uses the activemodels and the scenario models to try to predict the next step in the scenario that isexpected to occur. A scenario model is a knowledge base with specifications of intrusionscenarios. The planner then translates this hypothesis into a format that shows thebehavior, as it would occur in the audit trail. It uses the predicted information to planwhat to search for next. The interpreter then searches for this data in the audit trail. The
system proceeds this way, accumulating more and more evidence for an intrusion attemptuntil a threshold is crossed; at this point, it signals an intrusion attempt.

V. IDS ISSUES IN MOBILE ENVIRONMENT

Intrusion detection for traditional,wired networks has been the topic of significant research over the past few years. A problem arises, however, when taking the research for wired networks and directlyapplying it to wireless networks. Key assumptions are made when designing IDS s forwired networks, such as the difficulty for an attacker to penetrate the physical security ofthe system, the amount of network bandwidth available to the IDS, etc. Specific problemsfaced when building IDS for a mobile network are addressed below

A. *Lack of Physical Wires*

The most obvious difference when building an IDS in A wireless environment is the fact that an attacker no longer has to gain physical access tothe system in order to compromise the security of the network. Potentially, it is verysimple for someone to eavesdrop on network traffic in a wireless environment becausethey no longer have to break through any physical medium to gain access to the traffic.

B. *Bandwidth Issues*

Wireless networks have more constrained bandwidth as comparedto wired networks. This problem can manifest itself in a number of different ways whenan IDS is using wireless communication to convey information between parts of IDS onseparate nodes. An IDS in a mobile environment must be extremely careful to limit theamount of communication that takes place between nodes. A second

problem that maypossibly arise because of limited bandwidth Is erroneous behavior of the IDS due to communication delay between nodes.

C. *Difficulty of Anomaly/Normality Distinction*

Distinguishing an anomaly fromnormalcy has always been somewhat difficult for wired IDS s and wireless IDS s are nodifferent. If nodes in a network receive false or old routing information from a particularnode then it is difficult to verify if that particular node has been compromised or not. Anattacker could have taken the control of the node to send false information to other nodesin the network, or the node could just be temporarily out of sync due to fast movement orother processing requirements.

D. *Secure Communication Between Ids Agents*

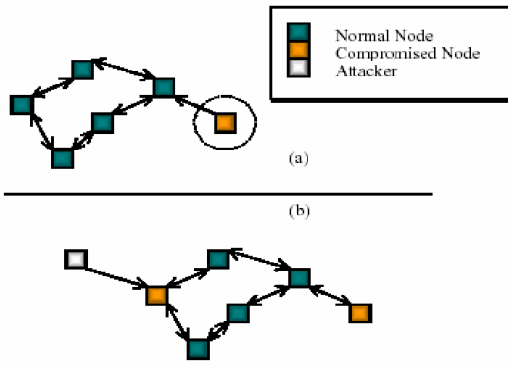
It is likely that in a wireless networkthere will have to be portions of the IDS running on each individual node in the network.Each of these IDS agents will have to communicate with other IDS agents in the networkto convey information relating to the status of the system. It is crucial that the informationbeing passed from agent to agent be encrypted as to not allow an attacker to gain accessto the communication.

E. *Lack of Centralized Access/Audit Point*

The lack of centralized audit points in adhoc networks present difficult problems for intrusion detection. Most static, wirednetworks have specific repositories where the IDS can obtain audit data for its misuse andanomaly detection(e.g. switches, routers, gateways, etc.). Without centralized auditpoints, IDS s on ad hoc networks are limited to use only the current traffic coming in andout of the node as audit data. The algorithms that the IDS uses must be distributed, andtake into account the fact that a node can only see a portion of the network traffic.

F. *Possibility Of A Node Being Compromised*

Since ad hoc networks are dynamic andnodes can move about freely, there is a possibility that one or more nodes could becaptured and compromised, especially if the network is in a hostile environment.



If the algorithms of the IDS are cooperative, it becomes important to be skeptical ofwhich nodes one can trust. IDS s on ad hoc networks have to be weary of attacks madefrom nodes in the network itself, not just attacks from outside the network.

G. *Difficulty In Obtaining Enough Audit Data*

Mobile networks do not communicateas frequently as their wired counterparts. Bandwidth issues, and other issues such asbattery life, contribute to this factor. This lack of communication can become a problemfor IDS s attempting to define rules of normality for anomaly detection. If only a smallamount of data is available to establish normal activity association rules, it is very hard todistinguish an attack from regular network use.

VI. NEW ARCHITECTURE

It is important to understand that most IDS architecturalmodels are based on static, wired networks. These models alone are insufficient to helpdesign an IDS in a mobile, ad hoc network environment. The architecture addressed is A distributed IDS, where each node on the network will have an IDS agent running on it.The IDS agents on each node in the network work together via a cooperative intrusiondetection algorithm to decide when and how the network is being attacked. Thearchitecture is divided into parts: the Mobile IDS Agents, which reside on each node inthe network, and the Stationary Secure Database, which contains global signatures ofknown misuse attacks and stores patterns of each user‘s normal activity in a non-hostile
environment.

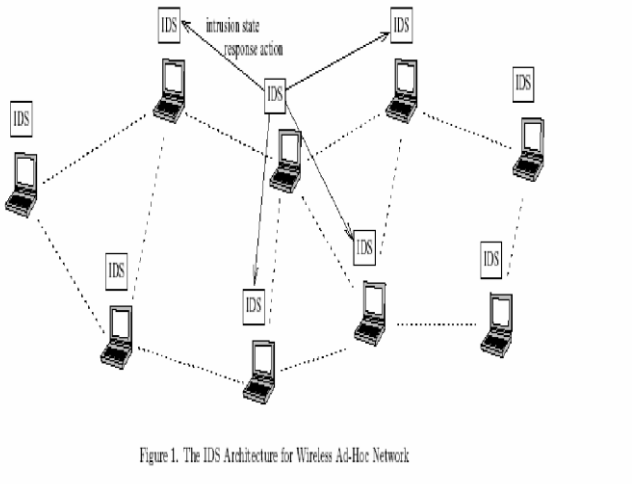


Figure 1. The IDS Architecture for Wireless Ad-Hoc Network

A. *Mobile IDS Agents*

Each node in the network will have an IDS agent running on itall times. This agent is responsible for detecting intrusions based on local audit data andparticipating in cooperative algorithms with other IDS agents to decide if the network is

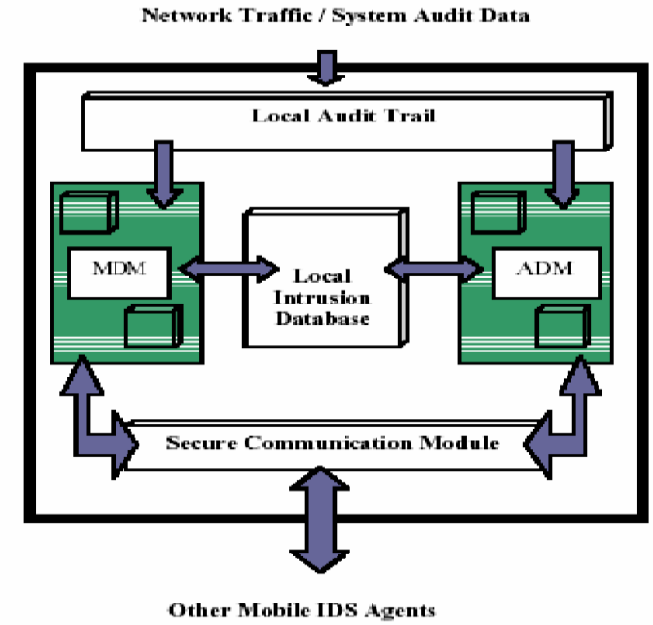
being attacked. Each agent has five parts : the Local Audit Trial, the Local IntrusionDatabase (LID), the Secure Communication Module, the Anomaly Detection Modules (ADM s), and the Misuse Detection Modules (MDM s).

i. The Local Audit Trial

Each agent must constantly check the audit data to decide thatan intrusion is not taking place. The Local Audit Trial will consist of specific items out ofthe network traffic as well as user commands to the node. The Local Audit Trial is responsible for selecting only the items it needs out of the network traffic and systemaudit data in order to minimize the size of the audit data collected. A audit data iscollected by the Local Audit Trial, it is passed to the Misuse Detection Modules and theAnomaly Detection Modules for further analysis. The Local Audit Trial is only responsible for gathering and storing audit data, not processing it.

ii. The Local Intrusion Database (LID)

The LID is a local database that warehousesall information necessary for the IDS agent, such as the signature files of known attacks,the established patterns of users on the network, and the normal traffic flow of thenetwork. The Anomaly Detection Modules and Misuse Detection Modules communicatedirectly with the LID to determine if an intrusion is taking place.



iii. The Secure Communication Module

The Secure Communication Module is necessary to enable an IDS agent to communicatewith other IDS agents on other nodes. It will allow the MDM s and ADM s to usecooperative algorithms to detect intrusions. It may also be used to initiate a globalresponse when an IDS agent or a group of IDS agents detects an intrusion. Basically, anycommunication that needs to occur from one IDS agent to another will use the SecureCommunication Module.Data communicated via the Secure Communication Module will need to be encrypted inorder to ensure that the data received by an IDS agent is accurate and has not beentampered with. The Secure Communication module is only used by IDS agents and doesnot communicate any other type of information between nodes. It must share thebandwidth that the mobile device uses for normal data transmission, so it is required to beefficient, and can only use the amount of bandwidth in needs.Also, the Secure Communication module must process information coming to the IDSagent from other agents in the network. For this reason, it must be fast and efficient, so asnot to take away from the processing time of the mobile unit.

iv. The Anomaly Detection Modules(ADM s)

Each Anomaly Detection Module isresponsible for detecting a different type of anomaly. There can be from one to manyAnomaly Detection Modules on each mobile IDS agent, each working separately orcooperatively with other ADM s. For example, one ADM might be looking for strangenetwork traffic patterns, while another ADM might be watching user input speed.

v. The Misuse Detection Modules (MDM s)

The Misuse Detection Modules functionssimilarly to the ADM s on the IDS agent. The primary difference is that MDM s onlyidentifies known patterns of attacks that are specified in the Local Intrusion Database.Like the ADM s, if the audit data available locally is enough to determine if an intrusion istaking place, the proper response can be initiated. It is also possible for a MDM to use A cooperative algorithm to identify an intrusion.

B. Stationary Secure Database

The Stationary Secure Database (SSD) in this architecture acts as a secure, trusted repository for mobile nodes to obtain information about the latest misuse signatures and to find the latest patterns of normal user activity. It is assumed that the attacker will not compromise the Stationary Secure Database, as it stored in area of high security. To ensure that the SSD will not be compromised it is kept stationary and not placed in a hostile environment where attacker attack is likely. It is also assumed that no physically compromised node will come in contact with the SSD,since the attacker will not be given physical access to the area where the SSD resides.Although these are severe restrictions, they can be accommodated through operational procedures and physical security.The mobile IDS agents will collect and store audit data while in the field, and will transfer this information when it is attached to the SSD. The SSD will then use this information for data mining of new anomaly association rules. The use of the SSD to mine new anomaly rules is beneficial to the IDS for three reasons. First, the SSD will be fixed, fast machine that is capable of mining rules much faster than on slower, mobile nodes. Secondly, the processing time used to mine the new rules of anomaly will not take away from the processing time of the mobile nodes.

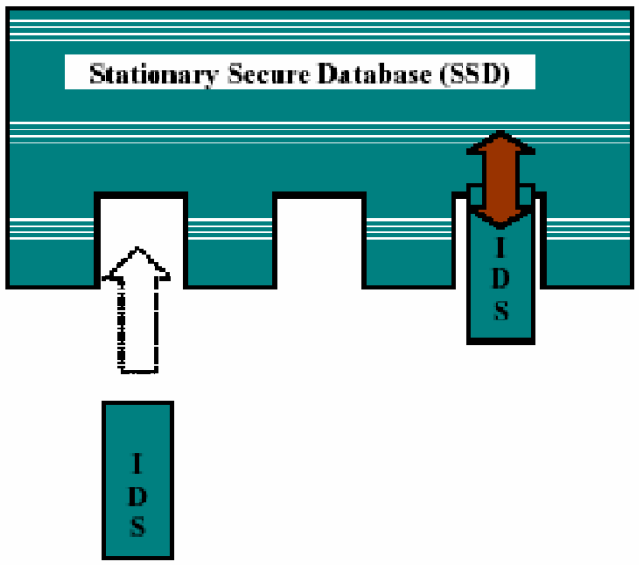


Figure: Mobile Agents Interacting with SSD

The SSD will also be the place where the system administrator can specify the newest misuse signatures. When the IDS agents are connected to SSD, they will gain access to the latest attack signatures automatically. This will make it much easier to update all the nodes in the network to keep up with the latest attacks. Instead of manually updating the attack files in the Local Intrusion Database of each individual node, or using the Secure Communication device on each node to communicate the new signatures, the SSD will be responsible for communicating the new attack signatures to each individual IDS agent.

One of the best reasons for using the SSD to communicate the new attack signatures, and establish new patterns of normalcy, is to limit the amount of communication that must take place between IDS agents in the mobile ad hoc network. As stated earlier, the IDS agents should not use very much bandwidth, because it is limited and in use by other applications on the mobile node. The use of SSD allows the IDS agents to not continually have to share information in order to update their Local Intrusion Database.Communication between the SSD and the IDS agents will be very quick and efficient, as there should be no threat of attack. By relying on the SSD to be a trusted source of update information, the IDS agent no longer has to use cooperative algorithms to determine if the information being sent is trustworthy or not.

VII. Anomaly Detection in Wire-less Ad-hoc Networks

In this section we discuss how to build an anomaly detection models for wirelessnetworks. Detection based on activities in different network layers may differ in theformat and the amount of available audit data as well as the modeling algorithms.

A. Building An Anomaly Detection Model

i. Framework

The basic premise for anomaly detection is that there is intrinsic andobservable characteristic of normal behavior that is distinct from that of abnormalbehavior. Entropy and conditional entropy are used to describe the characteristics of thenormal information flows and use the classification algorithms to build anomalydetection models. We can use a classifier trained using normal data to predict whatnormally the next event is given the previous n events. In monitoring when the actualevent is not what the classifier has predicted there is an anomaly. When constructing A classifier features with high information gain are needed.

Using this frame work we employ the following the procedure for the anomaly detection.

a. Select or partition audit data so that the normal data set has low Entropy
b. Perform appropriate data transformation according to entropy measures
c. Compute classifier using training data.
d. Apply the classifier to test it.
e. Post process alarms to produce intrusion reports.

ii. Attack Models

Route logic compromise- This type of attacks behaves by manipulating routinginformation, either externally by parsing false route messages or internally by maliciously changing routing cache information. In particular, we consider several special cases: (a)misrouting: forwarding a packet to an incorrect node; and (b) false message propagation:distributing a false route update.

Traffic pattern distortion- This type of attacks changes default/normal traffic behavior:(a) packet dropping; (b) packet generation with faked source address; (c) corruption onpacket contents; and (d) denial-of-service.

B. Areas Where Anomaly Detection Can Be Used

The two main areas where we need anomaly detection is ad-hoc networks is

· *Abnormal Updates to the routing table.*
· *Abnormal activities in other layers.*

i. Abnormal Updates to the routing table.

The two most important factors that are required for the anomaly detection are Low False positive rate High true positive rate (percentage of anomalies detected). A routing table usually contains, at the minimum the next hop to each destination node and the number of hops. The physical movement of nodes or network membership changes causes A legitimate movement in the routing table. Our objective in this study is to lead a better understanding of the important

and challenging issues in intrusion detection for ad-hoc routing protocols. First using a given set of training, testing and evaluation scenarios, and modeling algorithms, we can identify which routing protocol , with potentially all its routing information used , can result in better performing detection models.This will help Answer the question —what information should be included in the routing table to make —intrusion detection effective". This finding can be used in designing more robust protocols.

ii. Abnormal Activities In other layers

At the wireless application layer, the tracedata can use the service as the class (i.e., one class for each service), and can contain thefollowing features: for the past s seconds, the total number of requests to the sameservice, the number of different services requested, the average duration of the service,the number of nodes that requested (any) service, the total number of service errors, etc.A classifier on the trace data then describes for each service the normal behaviors of itsrequests. Many attacks generate different statistical patterns than normal requests.

VIII. IMPLEMENTED APPROACHES

Following are the some of the intrusion detection techniques used in wireless and ad hocnetworks.

A. IEEE 802.11

The IEEE 802.11 standard provides several mechanisms intended toprovide a secure operating environment. The IEEE 802.11 standard defines the physicallayers and the MAC sub layers for the wireless LANs. There are three different physicallayers. They are Frequency hopping Spread Spectrum Radio; direct sequence spreadspectrum Radio, and Base band infrared. The MAC layer is common for all these layers.

The IEEE 802.11 defines two authentication schemes:

i. Open System Authentication.
ii. Shared Key Authentication.

i. Open System Authentication

Open system authentication is the defaultauthentication protocol for 802.11. As the name implies, open system authenticationauthenticates anyone who requests authentication. A terminal announces that it wishes toassociate with an access point, and typically the access point allows the association.Essentially it provides NULL authentication process.

ii. Shared Key Authentication

Shared key authentication uses a standard challenge and response along with a shared secret key to provide authentication. The shared key Authentication requires that the Wired Equivalent privacy protocol (WEP) Algorithm be implemented on both the wireless terminal and the access point. The station wishing to authenticate, *the initiator*, sends an authentication request management frame indicating that they wish to use —shared key" authentication. The recipient of the authentication request, *the responder*, responds by sending an authentication management frame containing challenge text to the initiator. The challenge text is generated by using the WEP pseudo-random number generator (PRNG) with the —shared secret" and a random initialization vector (IV)[2] . Once the initiator receives the management frame from the responder, they copy the contents of the challenge text into a new management frame body. This new management frame body is then encrypted with WEP using the —shared secret" along with a new IV selected by the initiator. The encrypted management frame is then sent to the responder. The responder decrypts the received frame and verifies that the 32-bit CRC integrity check value (ICV) is valid, and that the challenge text matches that sent in the first message. If they do, then authentication is successful. If the authentication is successful, then the initiator and the responder switch roles and repeat the process to ensure mutual Authentication.

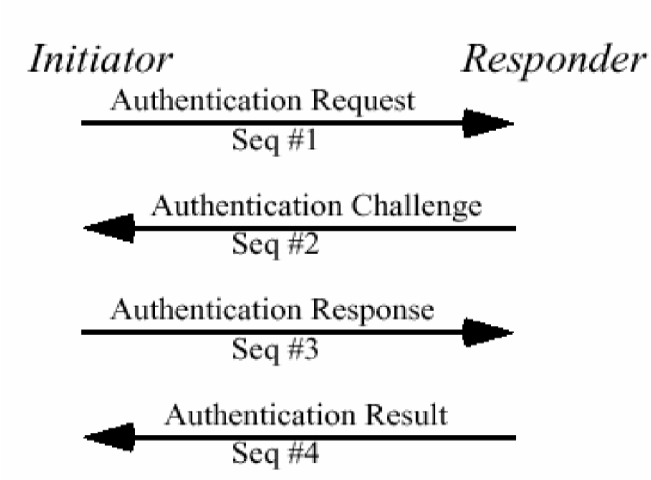


Figure: Mutual Station Authentication Using Shared Keys

Mobiles that are allowed to connect to the network use the same shared key, so thisauthentication method is only able to verify if the particular mobile belongs to the groupallowed to connect to the network, but there is no way to distinguish one mobile fromanother. Also there are no means available to authenticate the network. The IEEE 802.11does not define any key management functions. The IEEE 802.11 defines an optionalWEP mechanism to implement the confidentiality and integrity of the traffic in thenetwork. WEP is used at the station-to-station level and does not offer any end-to-endsecurity. Using, say, the playback attack, could easily fool the Shared Key Authenticationscheme. Hence, anyway an additional authentication mechanism is needed.

iii. *Secure Key Generation And Distribution*

The mobile systems have constraints like minimal computational capabilities andauthentication and the Secure key generation and distribution capability is required byany system, which contains cryptographic authentication, confidentiality andidentification. Developing faster and more powerful hardware components, which requireless Energy and changing the algorithmic and protocol design of the current systemwould be useful to meet the future needs.

iv. Current Approaches For The Key Generation

a. Key generation by the telephone manufacturer and distribution to the Service Provider via a backbone network

This requires the manufacturers and Serviceprovider to develop a special distribution channel. (b) Security of keys should be ensuredfrom the time the keys are sent to the Service provider. from the manufacturer. (c) Thisapproach is unacceptable to both the Service provider and the manufacturer.

b. Over-The-Air Phone Activation With Key Exchange

Over-the-air phone is themost preferred approach and requires a collaborative key generation and distributionbetween the mobile unit and the Service provider. The current over-the-air serviceprovisioning (OTASP) uses the Diffie-Hellman key exchange between the Serviceprovider and mobile unit to exchange a symmetric key called A-key (AuthenticationKey).

IX. Conclusion

The diligent management of network security is essential to the operation of networks, regardless of whether they have segments or not. It is important to note that absolute security is an abstract concept – it does not exist anywhere. All networks are vulnerable to insider or outsider attacks, and eavesdropping. No one wants to risk having the data exposed to the casual observer or open malicious mischief.Regardless of whether the network is wired or wirelesses, steps can and should always be taken to preserve network security and integrity.

We have said that any secure network will have vulnerabilities that an adversary could exploit. This is especially true for wireless ad-hoc networks. Intrusion Detection can compliment intrusion prevention techniques (such as encryption, authentication, secure MAC, secure routing, etc.) to improve the network security. However new techniques must be developed to make intrusion detection work better for the wireless networks. We have shown that an architecture for better intrusion detection in wireless networks should be distributed and cooperative by applying Mobile Agents to the network and given few of the implemented approaches for intrusion detection. Currently, the research is taking place in developing new architecture for wireless networks for better security.

X. References

1) Lidong Z., Zygmunt J. H., Securing ad hoc networks, IEEE Network, Vol. 13, No. 6, 1999, 24-30.
2) Sundaram A., "An Introduction to Intrusion Detection", http://www.acm.org/crossroads/xrds2-4/intrus.html
3) Marti S., Giuli T.J., Lai K. Baker M., —Mitigating Routing Misbehavior in Mobile Ad Hoc Networks",Proceedings of the Annual International Conference on Mobile Computing and Networking, MOBICOM2000, pp 255-265.
4) Arbaugh W., Shankar N., Wan Y.C.J., Your 802.11 Wireless Network Has No Clothes, Universityof Maryland, 30-Mar-2001.
5) Wenken Lee, Dong Xiang, Informatic-Theoritic Measures for Anomaly Detection.
6) Wenken Lee, Yongguang Zhang, Yi-An Huang, Intrusion Detection Techniques for Mobile wirelessnetworks.
7) Yongguang Z., Wenke L., —Intrusion Detection in Wireless Ad- Hoc Networks", Proceedings of theAnnual International Conference on Mobile Computing and Networking, MobiCom 2000, pp 275-283.
8) Andrew B.Smith, An Examination of an Intrusion Detection Architecture for Wireless Ad-HocNetworks.
9) Krugel , T.Toth. , Applying Mobile Agent Technology to Intrusion Detection
10) Kumar.S —Classification and Detection of Computer Intrusion " .

A Hybrid Reliable Data Transmission Technique for Multicasting in Mobile Ad hoc Networks

[1]M.RajanBabu
Associate Professor, ECE Department
Lendi Institute of Engineering and Technology
Jonnada, Vizianagaram, AndhraPradesh, India
rajanbabuphd@gmail.com
[2]G.Sasi Bhushana Rao
Senior Professor, E C E Department
Andhra University, Visakhapatnam

GJCST Classification
C.2.1

***Abstract*- Reliability is an important factor in multicasting in mobile ad hoc networks (MANETs), as it confirms eventual delivery of all the data to all the group members, without enforcing any particular delivery order. In this paper, we provide a hybrid reliable data transmission technique for multicasting in MANET. It uses the advantages of both Automatic Retransmission Request (ARQ) and Forward Error Correction (FEC) approaches in a controlled manner to provide a lossless non real time data to the receiver. Our technique has two phases, where in the initial phase we differentiate the data traffic as real time traffic and non-real time traffic. For both type of traffics, data is transmitted using the ARQ technique initially. In the next phase, if the traffic is non-real time, it estimates the total data loss occurred at the receivers for a given time period. If the loss is greater than a threshold value, it transmits data using FEC technique until the loss becomes less than the threshold. Thus our scheme not only controls the reliability in a network but also the overhead and scalability issues of existing ARQ and FEC techniques. By simulation results, we show that our proposed hybrid technique achieves better delivery ratio with reduced overhead when compared with existing techniques.**

Keywords- Mobile ad hoc networks (MANETs), Automatic Retransmission Request (ARQ), Forward Error Correction (FEC), hybrid reliable data transmission (HRDT), Control Overhead, Constant Bit Rate (CBR).

I. INTRODUCTION

A. *Mobile Ad Hoc Networks (Manet)*

The term —communication anytime and anywhere" has been popular due to the recent advancement in wireless transmissions and the popularity of portable computing devices available. These advancement made users to move around, while at the same time remaining touched to the rest of the world. [1] Today, the use and spread of mobile computers like laptops and palmtops are the evolution of the ideas obtained by the concept of ad hoc networking. Ad hoc networks posses nodes that are connected by wireless links and can be mobile, where all the MNs function as hosts and routers at the same time.

[1]*M.RajanBabu, Associate Professor, ECE Department,Lendi Institute of Engineering and Technology,Jonnada, Vizianagaram, AndhraPradesh, Indiarajanbabuphd@gmail.com*
[2]*G.Sasi Bhushana Rao Senior Professor, E C E Department Andhra University, Visakhapatnam*

Ad hoc networks gained its popularity due to its factors like self-organizing, rapidly deployable, and dynamic reconfigurable networks that require no fixed infrastructure. [3] In short, the MANET can be generally defined as a group of mobile computing medium using wireless links for communication without relying on any fixed infrastructure such as base stations.[2]

In MANET, two MNs communicate directly if they come under the radio transmission range of each other. . As the case of all wireless environments, radio links are not complete foolproof and they are affected by several sources of errors and interference resulting in a high and variable bit error rate. Consequently, one of the critical issues of a MANET is its radio interface. The second one is the mobility of the nodes. Even then many existing and forthcoming applications in MANETs require the association of groups of mobile users. [4]

The various application related to MANET are;

i. tactical (military) networks
ii. delay-tolerant networking
iii. disaster recovery services
iv. sensor networks
v. metropolitan/campus-area communicationnetworks
vi. enhanced cellular networks

B. *MANET Multicast*

Multicasting can be defined as the process of the parallel broadcast of the same single copy of data packets to multiple destinations which they tend to be identified by a single address. The transmitter may be one or even multiple nodes. The single transmitter is called"one to many" model and the multi transmitter is called"many to many" model. [5] Multicasting reduces the communication costs for applications that transmit the same data to multiple recipients. Instead of transmitting via multiple unicast, multicasting reduces the link bandwidth consumption, processing of sender and router, and delivery delay.

Many of the recent multicast routing protocols are proposed in a way such that it support both unicast and multicast routing. [6] The most basic and simple technique to multicast group, maintenance and creation is known as flooding. With flooding, every node that receives a packet in the network simply rebroadcasts it. [7] The need of

multicast routing protocols for MANET's are necessary because the standard protocols that are installed in fixed networks or infra-structured mobile networks cannot be used in MANET's. This is because MANET is a highly dynamic environment, so the traditional well established multicasting protocols cannot be deployed directly to it. Some modification and extension should be made while considering all the constraints, such as limited bandwidth, dynamic network topology and power. [9]

MANET Multicast routings are basically classified into two categories; tree-based protocols and mesh-based protocols. [10]

i. Tree-based schemes: It establishes a single path between any two nodes in the multicast group. These schemes need to have minimum number of copies per packet to be sent along the branches of the tree.
ii. Mesh-based schemes: It establishes a mesh of paths that connect the sources and destinations. They are more resilient to link failures as well as to mobility.

C. *Issues in MANET Multicast*

The primary challenges which are in front of multicast routing in MANETs is the need to have reliability along with, robustness, for data packets to reach completely to their destinations. Along with the above issues the problems in tree maintenance andfrequent reconfiguration during link failures, the packet losses caused by error-prone wireless media and nodal mobility also provide a major challenge. Similarly in the two protocols i.e in tree based and mesh-based protocols. In the tree-based protocols, where a tree tends to do multicast, severe packet loss occurs due to the limited connectivity of the tree. If even a single node in the tree does not receive a multicast packet, then all its downstream children cannot receive the packet too. On the other hand, mesh-based protocols overcome the problem of the tree by forwarding multicast packets with a mesh, such that a node can receive the packets from several upstream nodes. However, mesh-based protocols are inefficient in that they introduce redundant packet transmissions and nodes need to be able to distinguish previously-received packets in some way. [4,11,12]

D. *Reliable Multicast Protocols*

Reliability is the most important aspect of multicasting protocols in MANET. [9] Reliable multicast becomes a very demanding research problem due to high packet loss rate associated to MANETs. The packet losses are due to the error-prone wireless media and nodal mobility. Reliable multicast solutions proposed for wired network can not be directly ported for MANET, like [14] ;

i. link breakages
ii. concentrated retransmissions
iii. route changes
iv. concentrated retransmissions and heavy overhead

There have been many efforts to develop reliable multicasting protocols. There are three ways to provide some extent of reliability to multicast in the network layer. One is NACK-based method, the second is flooding and the third is the gossip method, which is _flooding with some limitation'. [9] Generally, the reliable multicast protocols can be classified into three categories according to the recovery mechanisms used. The categories are; Automatic Retransmission Request (ARQ) - based, gossip-based and Forward Error Correction (FEC) - based.

i. In ARQ, it provides a valuable feature for wireless networks and permits much more reliable communications across lossy wireless links. ARQ mitigates lost data packets through automatically triggered retransmissions from the original receptionist, where the recipient continuously supplies feedback (acknowledgements or negative acknowledgements) to make the transmitter know what packets have been received successfully. [15]
ii. In gossip, when a node receives a message for the first time, rather than retransmitting immediately the data like in flooding, it engages a probabilistic process to resolve whether or not to retransmit. Essentially, it retransmits each message with probability p. From a security point of view, this approach may have objectionable properties. [13]
iii. In the FEC, it transmits redundant data with the original data transmission. Thus, when errors or packet losses happen at the receptionist side, original data can be reconstructed using the ones received. Errors or losses may occur to them at the receptionist side. However, the encoder in use has a property that if any k packets out of the n packets are received, the source data can be reconstructed.

E. *Problem Identification And Proposed Solution*

In our previous papers, we have managed to provide solution to the need of congestion control and bandwidth allocation. In this paper, we provide a reliable multicast routing protocol for maintaining fault tolerance to minimize losses in the network. As discussed above the various challenges in MANET multicast routing protocol have various drawbacks and challenges. In this paper we identify the main problems in a reliable multicast MANET protocol and provide an efficient solution to overcome it.

II. RELATED WORKS

Emy E. Egbogah et.al. [16] have proposed a reliable routing protocol named Scalable Team Oriented Reliable Multicast (STORM). STORM combines individual nodes with comparable mobility patterns and speeds into teams, and builds hierarchy-based multicasts mesh structure among elected team nodes. A Unicast Acknowledgement Scheme (UAS) is developed to construct the routing structure in an efficient manner. To improve the reliability of STORM, a modified version of Reliable Adaptive Congestion controlled multicasT (ReACT) is used as a reliable transport protocol. It offers scalability as the network size, multicast groups and total number of multicast group member's

increase as well as creating and propagating control packets with reliable delivery and low memory consumption.

Bo Rong et.al. [17] have proposed a new hybrid error control scheme that combines interleaving, forward error correction (FEC), and threshold based ARQ to mitigate the error and loss effects encountered in MANETs. In particular, the threshold based ARQ is studied to shorten the transmission delay in reliable multicast. In order to work compatibly with a verity of MANET multicast routing protocols, this new scheme is based on Client/Server architecture which resides on the top of UDP layer. Moreover, they used specification and description language (SDL) to formally portray the hybrid error control scheme from a broad overview down to detailed design levels.

Mehdi EffatParvar et.al.[18] have proposed a reliable multicast algorithm with local recovery approach. By using the proposed algorithm, nodes can join to multicast group in minimum time and data delivery can be increased. The algorithm tries to accomplish fast recovery during any route breakage, so that the destination can connect to source in new route or in the same route.

Dimitrios Koutsonikolas and Y. Charlie Hu [19] have examined FEC's efficiency in wireless network by implementing four reliable schemes initially proposed for wired networks on top of On Demand Multicast Routing Protocol (ODMRP). They proved that pure FEC can offer significant improvements in terms of reliability, increasing Packet Delivery Ratio up to 100% in many cases, but it can be very inefficient regarding the number of redundant packets it transmits. Moreover, a carefully designed hybrid protocol, such as RMDP, can maintain higher reliability while improving the efficiency compared to a pure FEC scheme.

Erik M. Ferragut [20] has proposed a new erasure code as a solution to the dynamic erasure code problem. The dynamic erasure code problem is to extend the digital fountains concept to a message generator, simultaneously with the transmission (i.e., live data). Solution of this problem provides a means for robust multicasting or one-way transmission of live data on a computer network. It also gives a method for robust distributed storage of log data, or other serially generated data.

Ali Alsaih and Tariq Alahdal [21] have proposed a reliable multicast transport protocol over combined networks using sub sub-casting called RMSS. It is based on a hierarchal structure where receivers are grouped into local regions. In each local region there are special receivers, which are called designated receivers and mobile agents. Each of the receivers is responsible for retransmission of requested packets to the receivers which are in their local region. Here a sub sub-casting is used to retransmit the data only to the requested receivers.

In our previous paper [22], we have proposed an energy efficient and reliable congestion control (EERCCP) protocol for multicasting in mobile adhoc networks. Our algorithm tries to overcome the disadvantages of existing multicast congestion control protocols which depend on individual receivers to detect congestion and tries to adjust their receiving rates. Our protocol consists of three phases;

First phase - Builds a multicast tree routed at the source, by including the nodes with higher residual energy towards the receivers.

Second phase- An admission control scheme, depending on the output queue size, to analyze flow is admission or rejection

Third phase- Adjusts the multicast traffic rate at each bottleneck of a multicast tree.

III. PROPOSED SCHEME

In section 1.4, we have discussed Reliable multicast in MANET and the various protocols used. We have discussed above (section 2) various recent works related to the different protocols used in reliable multicast like the ARQ, Gossip or FEC based. These protocols have there own merits and demerits when used. [23] have proposed a hybrid method called Reliable Multicast data Distribution Protocols (RMDP) which uses the FEC encoding to improve the behaviour of the protocol in presence of large groups of receivers, and to reduce the amount of feedback from receivers. ARQ is used to deal with those cases where the default amount of redundancy does not suffice to complete reception. The RMDP method identifies the drawbacks of both FEC and ARQ method and uses the advantage of the two protocols in order to overcome the drawbacks.

The major drawback of using ARQ single handedly is that it scales very badly to large sets of receivers as well as scalability problems also exist in handling feedback from the receivers. In the same way, FEC is computationally expensive, since the entire data stream must be processed to produce the encoded packets, each one conveying information on a number (possibly as large as k) of source data packets. As in of [23] hybrid method maintains a balance between both the ARQ as well as FEC. The use of FEC techniques to drastically reduce the impact of independent losses for different receivers, which make ARQ-based protocols perform very poorly as the number of receivers grows. The protocol is well-suited to the use with mobile equipment because of its simplicity, robustness to losses, moderate demand for feedback, and scalability.

In our work, as like [23], we introduce a hybrid method of ARQ and FEC. Our method is a two phase technique, where in the initial step we differentiate the data services among the real time data services and non-real time data services. If the data service is a non-real time data services, then the next phase is executed. We use our concept of hybrid method in accordance to the data loss. In general, the service in default uses ARQ method to send data but if there exists an excessive data loss then the system changes over to FEC to send data.

A. Phase – 1

In the initial phase, we determine the data services available. We classify the data services into two major groups; the real time services and the non-real time services. The real time data services are basically those information/data which are delivered immediately after collection. There is no delay in the timeliness of the information provided. These are often

used for navigation or tracking. [24] These data needs to be sent to the receiver without any time delay even there exist a minimal loss. Therefore we can compromise the losses but the time lagging can not be compromised in the case of real time data services. Similarly the other data services are termed as non real-time services. In these services of non real-time data, the time lagging factors provide less importance but the losses in these service plays a major role. We consider the two factors of data loss and time lagging of both the services and detect between the two services. As real time data services are less prone to data losses, the information is sent in ARQ process. But in the case of non-real time services, the data loss plays a major role. So we cannot take the ARQ services in the non real-time services, if the losses are high. Thus we detect the losses and if the losses are higher than a threshold level, we shift the services from ARQ to FEC. We discuss this issue in the next section.

B. Phase - 2

As discussed above, the default services for sending the data, we consider the ARQ services. But when a non real time data is sent, we periodically determine the losses caused by the ARQ services. If the services cause a higher data loss (above a certain threshold level) in a particular time period, the default ARQ services is changed into an FEC services.

Consider a period λ in which the losses are determined for a non real time data. We analyze a data drop rate (DL) in each period λ. The probability of data loss of DL along with the number of multicast receiver (r) is given as;

$$P(DL,r)=1-(1-D_L)^r \quad (1)$$

Where,

$$DL=\frac{\text{Number of packet dropped}}{\text{Time period}} \quad (2)$$

The above equation state two factors;

i. Increase in data drop increases the probability of data loss.
ii. Increase in receivers along with data drop evolves a higher data loss.

Thus when a probability of losses increases due to either data loss or due to increase in receivers and cross a particular threshold level (P(DL, r)th), the source get informed. The source then changes the ARQ service and adopts FEC services (We evaluate the use of FEC in the next section.). The FEC service is sent throughout the section (till the next sets of data are sent). After the complete of section, the default ARQ services are resumed again. If the probability of the threshold level does not reduce, the FEC service is again resumed or else the ARQ service gets maintained.

C. FEC Service

FEC or Forward error correction is a system of error control for data transmission, whereby the sender adds carefully selected redundant data to its messages, also known as an error-correction code. Here we use Luby transform (LT) coding for the FEC service. LT codes are the first class of practical fountain codes that are near optimal erasure correcting codes which employing a particularly simple algorithm based on the exclusive or operation ($\oplus$) to encode and decode the message. [26]

The LT Coding algorithm [27] produces a virtually unlimited number of encoded blocks from some k original data blocks via logical XOR operations. The k original data blocks are obtained by partitioning the original data into k uniform segments and the creation of each encoded block, or —symbol", will require $O(\ln(\frac{k}{\delta}))$logical operations on the original blocks. To decode the original data with a 1-δ chance of success, any $k+O(\sqrt{k}\ \ln^2(\frac{k}{\delta}))$ encoded blocks should be sufficient.

The encoding process is relatively straight forward.

i. Choose some degree d for the next encoded block according to the Robust Soliton Distribution
ii. Randomly choose d different original data blocks and XOR them together to produce the encoded block.
iii. Repeat steps 1 and 2 until the desired number of encoded blocks have been produced.

It should be noted that as each encoded symbol is produced, the identities of its sources must be stored as meta-data for the decoding process.

The process ofdecoding the data is as follows

i. When an encoded block is received, XOR it with all of its neighbors in the bipartite graph which have been recovered, and remove the edges that join the XORed nodes.
ii. If the encoded block has only one remaining neighbor, then part of the original data has been recovered. Copy its data to its sole neighbor and place that data node in a queue of original nodes to process.
iii. While the queue is not empty, choose a data node from the queue. XOR each received neighbor‘s data with the data in the original node and disconnect the nodes. For each neighbor that is XORed, perform step 2.
iv. Continue receiving and processing encoded blocks until the original data has been completely recovered.

Thus our technique of hybrid usage of ARQ and FEC cumulatively produces a reduces loss based scheme which helps the non real time data to maintain loss free even if the number of receivers are increased. This increases the scalability of the network and avoids time-waste for redundancy.

Algorithm

Consider an incoming traffic flow at λ=1, where λ is a given period

i. If the flow is real-time, then

1.1 flows are transmitted using ARQ

end if

ii. if flow is non-real time, then
2.1 Flow are transmitted using ARQ
2.2 determine probability of data loss, P(DL, r)
2.3 If P(DL, r) > P(DL, r)th , then
2.3.1 Flow are transmitted using FEC
2.3.2 After FEC session complete, repeat from 1.
Else
2.3.3 Continue the transmission using ARQ
End if
End if

iii. $\lambda = \lambda + 1$,

iv. Repeat from 1

IV. Simulation Results

A. Simulation Model And Parameters Simulation Model And Parameters

We use NS2 [29] to simulate our proposed technique. The proposed hybrid reliabledata transmission (HRDT) technique is applied in our previous multicast routing protocol EERCCP [23]. In our simulation, the channel capacity of mobile hosts is set to the same value: 2 Mbps. We use the distributed coordination function (DCF) of IEEE 802.11 for wireless LANs as the MAC layer protocol. It has the functionality to notify the network layer about link breakage.

In our simulation, 50 mobile nodes move in a 1000 meter x 1000 meter region for 50 seconds simulation time. We assume each node moves independently with the same average speed. All nodes have the same transmission range of 250 meters. In our simulation, the speed of the mobile is 5 m/s. The simulated traffic is Constant Bit Rate (CBR).

Our simulation settings and parameters are summarized in table 1

Table1. Simulation Parameters

No. of Nodes	50
Area Size	1000 X 1000
Mac	802.11
Radio Range	250m
Simulation Time	50 sec
Traffic Source	CBR and VBR
Rate	0.5,1,1.5 and 2Mb
Mobility Model	Random Way Point
Speed	5m/s
Receivers	5,10,…25
Pause time	5 s
Transmit Power	0.660 w
Receiving Power	0.395 w
Idle Power	0.335 w
Initial Energy	3.1 J

B. Performance Metrics

We compare our (HRDT) technique with existing multicast AODV [28] and RMDP [24]. We evaluate mainly the performance according to the following metrics.

i. Average end-to-end Delay

The end-to-end-delay is averaged over all surviving data packets from the sources to the destination.

ii. Average Packet Delivery Ratio

It is the ratio of the No. of packets received successfully and the total no. of packets sent.

iii. Average Energy Consumption

The average energy consumed by the nodes in receiving and sending the packets are measured.

iv. Control Overhead

The control overhead is defined as the total number of routing control packets normalized by the total number of received data packets

C. Results

i. Varying the Receivers

In this experiment, we vary the group size or the number of receivers per group as 5,10…..25.

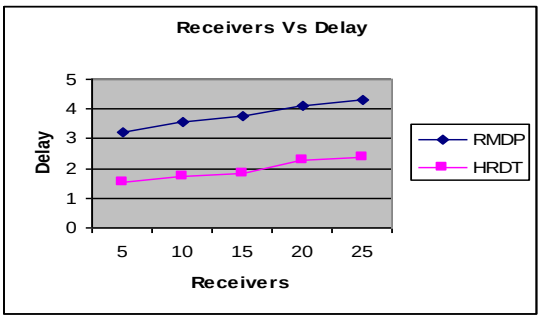


Fig. 1. Receivers Vs Delay

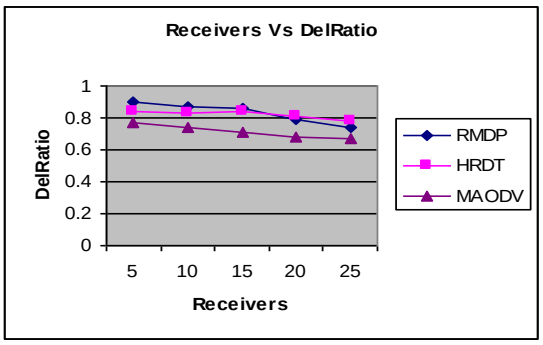


Fig. 2. Receivers Vs Delivery Ratio

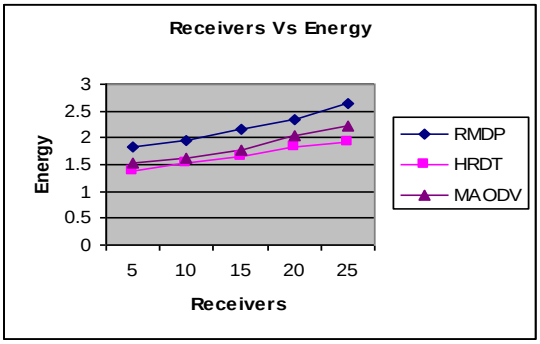


Fig. 3. Receivers Vs Energy

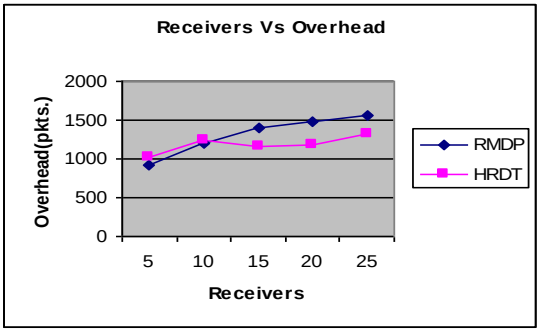


Fig. 4. Receivers Vs Overhead

When the number of receivers is increased, we observe the following results.

Fig1- shows the end-to-end delay occurred for both HRDT and RMDP. As we can see from the figure, the delay is significantly less for HRDT, when compared to RMDP. This is because, RMDP is completely FEC based resulting in high delay for encoding and decoding.

Fig2 **-**shows the packet delivery ratio for HRDT, RMDP and MAODV. As we can see from the figure, the delivery ratio is initially less for HRDT than RMDP for the receivers 5,10 and 15, since ARQ suffer from poor performance, when the receivers are increased. But when the receivers are more than 15, it changes to FEC mode, resulting in more delivery ratio than RMDP. Since MAODV does not involve any error recovery features, it has the least delivery ratio

Fig3-shows the energy consumption for HRDT, RMDP and MAODV. The energy consumption is more for RMDP compared to HRDT and MAODV, since FEC requires more energy for encoding and decoding.

Fig4- gives the overhead occurred for both HRDT and RMDP. Cleary the overhead is less in HRDT than RMDP. This is due to the fact that HRDT adaptively changes to FEC, when the receivers are more.

ii. Varying the Rate

In this experiment, we vary the data sending rate as 0.5,1,1.5 and 2Mb.

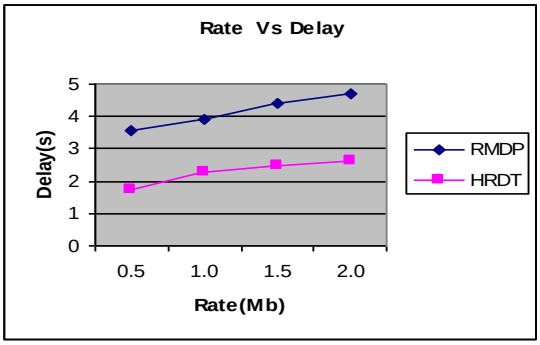


Fig.5. Rate Vs Delay

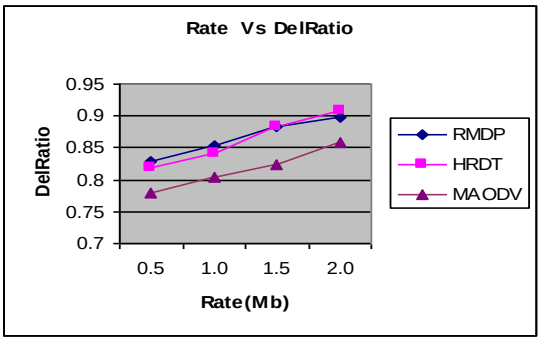


Fig. 6. Rate Vs Delivery Ratio

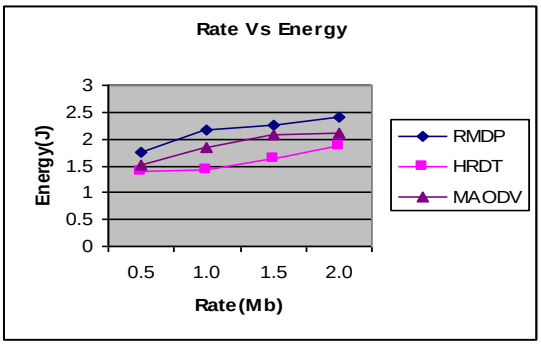


Fig. 7. Rate Vs Energy

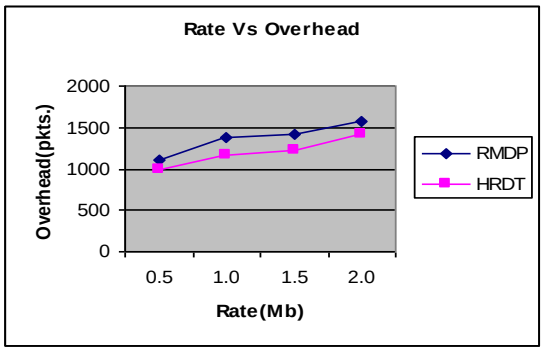


Fig. 8. Rate Vs Overhead

When the rate is increased,

Fig5- shows the end-to-end delay occurred for both HRDT and RMDP. As we can see from the figure, the delay is significantly less for HRDT, when compared to RMDP. This is because, RMDP is completely FEC based resulting in high delay for encoding and decoding.

Fig6- shows the packet delivery ratio for HRDT, RMDP and MAODV. As we can see from the figure, the delivery ratio is initially less for HRDT than RMDP for the rate 0.5Mb and 1Mb, since ARQ has more packet drops, compared to FEC. But when the rate is more than 1Mb, it changes to FEC mode, resulting in more delivery ratio than RMDP. Since MAODV does not involve any error recovery features, it has the least delivery ratio

Fig7- shows the energy consumption for HRDT, RMDP and MAODV. The energy consumption is more for RMDP compared to HRDT and MAODV, since FEC requires more energy for encoding and decoding.

Fig8-gives the overhead occurred for both the cases. Cleary the overhead is less in HRDT than RMDP. This is due to the fact that HRDT adaptively changes to FEC, when the receivers are more.

V. Conclusion

In this paper, we have provided a hybrid reliable data transmission technique (HRDT) for multicasting in MANET. It uses the advantages of both Automatic Retransmission Request (ARQ) and Forward Error Correction (FEC) approaches in a controlled manner to provide a lossless non real time data to the receiver. Our scheme is based on two phases in which the first phase determines the type of the data traffic as real time and non-real time and the second phase determines the losses. Among the two traffic services, the non real time data traffic need to be have a lower loss even if there exist a delay and the real-time traffic need minimum delay irrespective of the losses. Since ARQ involves less delay and overhead, the real-time data is transmitted completely using the ARQ technique. But for the non real-time data, the total data loss occurred at the receivers, is estimated for a give time period. If the loss is greater than a threshold value, it transmits data using FEC technique since FEC achieves more reliability than ARQ. Once the loss becomes less than the threshold, again the data is transmitted using ARQ. Thus our scheme not only controls the reliability in a network but also the overhead and scalability issues of existing ARQ and FEC techniques. By simulation results, we have shown that our proposed hybrid technique achieves better delivery ratio with reduced overhead when compared with existing techniques.

VI. References

1) Yu-chee Tseng, Wen-Hua Liao and Shih-Lin Wu, ―Handbook of Wireless Networks and Mobile Computing", John Wiley & Sons, 2002.
2) Sonmez, O.O. (2007) 'A survey on reliable multicast approaches for mobile ad hoc networks', http://pds.ewi.tudelft.nl.
3) M.Nagaratna, V.Kamakshi Prasad and C.Raghavendra Rao, ―TeamMulticasting Routing Protocol in MANETs", IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.6, June 2009
4) Moustafa and H. Labiod, "A Multicast On-demand Mesh-based Routing Protocol in Multihop Mobile Wireless Networks," IEEE 58th Vehicular Technology Conference (VTC2003), October 2003.
5) Moukhtar A. Ali, Ayman El-Sayed and Ibrahim Z. Morsi, ―A Survey of Multicast Routing Protocols for Ad-Hoc Wireless Networks", Minufiya Journal of Electronic Engineering Research (MJEER), Vol. 17, No. 2, July 2007.
6) Nen-Chung Wang and Yu-Li Su, ―AStable Power-Aware Multicast Routing Protocol for Mobile Ad Hoc", Department of Computer Science and Information Engineering, 2005.
7) K. Sambandan, G.V. Záruba, and D.Levine, "On the Reliability and Additional Overhead of Reliable On-Demand Multicast Routing Protocol for Mobile Ad Hoc Networks," Proceedings of the 2004 International Conference on Parallel and Distributed Processing Techniques and Applications PDPTA'04, Las Vegas, June 2004.
8) Zeyad M. Alfawaer, GuiWei Hua, and Noraziah Ahmed, ―ANovel Multicast Routing Protocol for Mobile Ad Hoc Networks", American Journal of Applied Sciences 4 (5): 333-338, 2007.
9) S. Yang and J. Wu, "New technologies of multicasting in MANET," in Design and Analysis of Wireless Networks, Y. Xiao and Y. Pan, Eds., Nova, Baltimore, MD, USA, 2005.
10) Pariza Kamboj and A.K.Sharma, ―Scalble Energy Efficient Location Aware
11) Multicast Protocol for MANET (SEELAMP)", Journal of computing, vol 2, issue 5, may 2010, ISSN 2151-9617.
12) Weisheng Si , Chengzhi Li, RMAC: A Reliable Multicast MAC Protocol for Wireless Ad Hoc Networks, Proceedings of the 2004 International Conference on Parallel Processing, p.494-501, August 15-18, 2004.
13) Zhiming Xu, Yu Wang and Jingguo Zhu, ―A Reliable Multicast Routing Protocol for High-speed Mobile Ad Hoc Networks: R-ODMRP", Journal of software, vol. 5, no. 1, january 2009.
14) Burmester M, Le T.V and Yasinsac, A, ―Adaptive gossip protocols: managing security and redundancy in dense ad hoc networks", Ad Hoc Networks, Volume 5, Issue 3, Pages 313-323, April 2007.
15) Beini Ouyang, Xiaoyan Hong , Yunjung Yi, "A Comparison of Reliable Multicast Protocols for Mobile Ad Hoc Networks," in the Proc. of IEEE SoutheastCon 05, Fort Lauderdale, FL, April, 2005.
16) David J. Claypool and Kevin M. McNeill, ―Automatic repeat request (ARQ) over TDMA-based mesh network", IEEE Military

Communications Conference, 2008. MILCOM 2008, p.p 1-7, San Diego, CA, 16-19 Nov. 2008.

17) Egbogah, E., Fapojuwo A.O., Viberg N., Hoople W., and Chan N. "Scalable Team-Oriented Reliable Multicast Routing Protocol for Tactical Mobile Ad Hoc Networks," IEEE Military Communication (MILCOM) Conference 2008, November 2008.
18) Bo Rong, K. Mnif, A. K. Elhakeem, and M. Kadoch, "A Hybrid Error Control Scheme for MANET Reliable Multicast," In proceeding of IEEE Canadian Conference on Electrical and Computer Engineering 2005 (CCECE 2005), Saskatoon Inn, Saskatoon, Saskatchewan Canada, May 1-4, 2005.
19) M. EffatParvar, M. Dehghan, A. Movaghar, A. Dareshorzadeh, M.R. EffatParvar "Reliable Multicast Routing with Local Recovery Approach in Ad Hoc Network," Proceedings of the Fourth Second International Conference on Access Networks(AccessNets07), IEEE, August, 2007.
20) Dimitrios Koutsonikolas and Y. Charlie Hu, ―The Case for FEC-Based Reliable Multicast in Wireless Mesh Networks", In Proceedings of the 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, p.491-501, June 25-28, 2007.
21) Erik M. Ferragut , ―ADynamic Erasure Code for Multicasting Live Data", In Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies, 2009.
22) Ali Alsaih and Tariq Alahdal, ―Non-Real Time Reliable Multicast Protocol Using Sub Sub-Casting ―,The International Arab Journal of Information Technology, Volume 4, Number 1, January 2007 .
23) Sasi Bhushana Rao and M. RajanBabu, ―An Energy Efficient and Reliable Congestion Control Protocol For Multicasting In Mobile Adhoc Networks", International Journal of Computer Science and Information Security, Vol. 7, No. 1, 2010.
24) Luigi Rizzo and Lorenzo Vicisano, ―RMDP: an FEC-based reliable multicast protocol for wireless environments", ACM SIGMOBILE Mobile Computing and Communications Review, Volume 2 , Issue 2, Pages: 23 – 31, 1998.
25) ―Real-time data" from http://en.wikipedia.org/wiki/Real-time_data
26) ―Luby transform (LT)" from http://en.wikipedia.org/wiki/Luby_Transform.
27) Uyeda, F., H. Xia, and A. Chien, Evaluation of a High Performance Erasure Code Implementation. 2004, UCSD, 2004.
28) Elizabeth M. Royer, Charles E. Perkins," Multicast Operation of the Ad-hoc On-Demand Distance Vector Routing Protocol",ACM,1999
29) Network Simulator , http://www.isi.edu/nsnam/ns

An Efficient Connection Admission Control Mechanism For IEEE 802.16 Networks

R Murali Prasad

GJCST Classification C.2.2

Abstract- **The main function of connection admission control (CAC) is to resolve whether or not to accept a new connection. The decision is made based on the aspects whether the Quality of Service (QoS) of new connection is satisfied and whether the QoS of ongoing connections is influenced after new connection is accepted. There has been no architecture that clearly describes a CAC for IEEE 802.16 networks. In this paper, we wish to design an efficient admission control mechanism for IEEE 802.16 networks to solve the above issues. Our CAC is based on the estimation of bandwidth utilization of each traffic class, with the constraint that the delay requirement of real-time flows should be satisfied. The current available bandwidth is estimated for all the nodes and for the new incoming flows, it estimates the requested bandwidth and decides to admit this new flow or not. By simulation results we show that our proposed approach reduces the blocking probability, there by increasing the throughput for all classes of traffic.**

Keywords- Quality of Service (QoS), Connection Admission control (CSC), Bandwidth based CAC, IEEE 802.16, MAC protocol.

I. INTRODUCTION

A. *WIMAX Networks*

WiMAX (Worldwide interoperability for Microwave access) or IEEE 802.16 is regarded as a standard for metropolitan area networks (MANs) [1]. It is one among the most reliable wireless access technologies for upcoming generation all-IP networks. In reality, this access technology enables obtaining high bit rate and reaching large areas with a single Base Station (BS), and because of this it provides to operators the option of supplying connectivity to end users in an economical way [2]. It is a reliable choice to offer last-mile access in wireless metropolitan area network (WMAN) together with the merits of low cost, high speed, rapid and easy deployment, such that a large number of applications can be applied also in the areas where the installation of wired infrastructure is cost-effective or technically achievable [3]. In consequence to the characteristics of WiMax, it can be widely employed in several related fields, comprising of mobile service, mobile commerce, mobile entertainment, mobile learning and mobile healthcare [4]. Fixed subscriber stations (SSs) and mobile subscriber stations (MSSs) remain in contact with BSs by means of air interfaces [1]. Even though the deployment and the utilization of this standard have begun, the exploitation of WiMAX networks is still restricted to certain situations. Research works on WiMAX access networks is still taking place, because several topics have yet to be described to permit and optimize the utilization of this technology in upcoming generation networks [2].Traffic on 4G networks namely WiMAX is heterogeneous with random mix of real and non-real time traffic with applications needing widely varying and miscellaneous QoS guarantee [5].

About-Department of Electronics and Communications :muraliprasadphd@gmail.com

B. *Connection Admission Control (CAC)*

IEEE 802.16 achieves QoS guarantee between Base Station (BS) and Subscriber Station (SS) by using connection admission control (CAC), packet scheduling, dynamic sub-carrier assignment etc, in order to keep up multimedia services. In ensuring QoS, CAC is the first stage. Also the selection of scheduling and resource allocation algorithms is controlled by the choice of CAC algorithms [7].

To resolve whether or not to accept a new connection, is the main function of CAC. The decision is made owing to two aspects

i. Whether the QoS of new connection is satisfied,
ii. Whether the QoS of ongoing connections is influenced after new connection is accepted [7].

The basic idea in CAC is to consider information from other cells in the network along with local information. The confined cell, where the new call has been requested, interacts with a set of cells called cluster that will take part in the admission process. In general, the schemes vary from each other in accordance with how the cluster is constructed, the nature of information exchanged and how this information is used. Making the choice of admission control in a decentralized manner, will be the primary idea [8].

i. *CAC schemes*

Call admission control schemes can be divided into following categories,

Local schemes- It uses local information alone (e.g. local cell load) when taking the admission decision.

Collaborative schemes- It involves more than one cell in the admission process. The cells exchange information about the ongoing sessions and about their capabilities to support these sessions [8].

Bandwidth based CAC (BW-CAC)- It admits flows as long as there is enough bandwidth to satisfy the incoming request, but it does not consider the deadline constraints of the connections. The BW-CAC receives all the DSA/DSC/DSD requests and updates the available bandwidth after admitting new connection or deleting an outgoing connection or honoring bandwidth change request of a connection [9].

QoS based CAC (QoS-CAC)- It services the UGS connection queue first, followed by RTPS and then by

NRTPS queues. Thus, it provides highest priority to UGS connections requests followed by RTPS and NRTPS connection requests. There is no need for Admission Control to Best-Effort connections since it does not require any guarantees [9].

ii. Issues in CAC

The presented admission control strategies can handle the resource management in homogeneous wireless networks only but not the issues in heterogeneous wireless environment. In mobile communication environment, the mobility of the terminals makes the resource allocation, a difficult task at what time the resources are always insufficient. This contradicting situation can be handled by efficient call admission control policies which optimize the resource utilization [8].

The CAC mechanism deals with the advent of a new call in the connection-oriented systems and decides whether the system accept a new connection or not. CAC should verify that the new call does not affect the QoS of present connections and also the system can offer the QoS requirements of the new call before taking a decision. The ongoing calls of present cell might be handed over to another cell because of user mobility. Due to the network overload or aggressive channel conditions, the receiving cell might have scarce resources. Consequently, it may start dropping calls or decline handoff attempts if the arrival rate of new or handoff calls exceeds the capability of a cell [10].

In IEEE 802.16 networks, there has been no clear structure described for CAC. Although a few authors have recommended implicit conventional bandwidth based CAC, such simple CAC cannot guarantee QoS to application services. Consequently such ancient CAC may make the execution uncooperative as well as inappropriate for application using diverse services of 802.16 [9].

II. Related Work

Ke Yu et al [7] have proposed a statistical CAC mechanism for IEEE 802.16 network. In order to avoid the QoS degradation, their proposed CAC mechanism considers the traffic variability and overflow. Furthermore, a model of traffic and air interface capacity is provided to make their CAC mechanism easy to be implemented. They also proposed a performance analysis model based on Markov chains.

Ramesh Babu H.S et al [8] have proposed an optimal call admission control algorithm to reduce call blocking probability in Next generation wireless network (NGWN) and provided optimal QoS to the mobile users. In their proposed algorithm they have considered three classes of traffic having different QoS requirements which are complementary in nature with respect to their QoS requirements are considered.

Sarat Chandra and Anirudha Sahoo [9] have presented an efficient CAC algorithm which not only provides bandwidth guarantee, but also ensures QoS guarantees to connections as per their service types.

Prasun Chowdhury et al [11] have focused on the integration of Call Admission Control (CAC) and Uplink Packet Scheduling (UPS) mechanism to identify quantitative measurement of some QoS parameters like delay, loss rate, throughput, connection acceptance probabilities and bandwidth utilization of the system. Reservation based Prioritized CAC with degradation (RPCAC- Deg) and Non Reservation based Prioritized

CAC with degradation (NRP-CAC-Deg) schemes along with the two delay models maintaining delay guarantee have been evaluated by their integrated Markov Chain model.

Anas Majeed et al [12] have described a problem in the mesh network Relay station that how to serve the mobile stations (MSs) which are out of the Relay station coverage. They also proposed a solution for mobile stations out of the coverage of the WIMAX Relay stations mesh Network. Therefore they defined Ad-hoc network as a solution by using its admission control scheme and apply it on the mobiles inside and outside the Relay station coverage.

III. Efficient Admission Control Mechanism

A. System Model and Overview

We consider a wireless metropolitan area mesh network in which the infrastructure/backbone is built using IEEE 802.16 technology. The mesh network consists of fixed wireless mesh routers and end mobile clients. The wireless mesh routers form a multi-hop wireless backbone to relay traffic to and from mobile clients. An IEEE 802.16 cell consists of a base station and one or more mobile stations based on point-to-multipoint (PMP) network topology. Wireless mesh routers also serve as base stations to mobile stations within their coverage area.

We describe an IEEE 802.16-based wireless mesh network as a set of nodes N = {1, ...,N} that includes all the mobile clients and mesh routers and a set of wireless links L = {1, ...,L} that includes all the backhaul links as well as the links between mobile stations and base stations. Assume the bandwidth requirement for the new arrival is REQbw. Each node and each link along the chosen route must have at least MIAbw units of bandwidth available for the new connection.

Our CAC is based on the estimation of bandwidth utilization of each traffic class, with the constraint that the delay requirement of real-time flows should be satisfied. The principle of our CAC algorithm is:

i. First, system calculates the current available bandwidth.
ii. Second, for new incoming flows, system estimates the bandwidth it will take and the system will decide to grant this new flow or not.

B. Available Bandwidth Estimation

The area within transmission range is defined as the direct range, and the area between transmission range and interference range is defined as the indirect range. The total numbers of these two areas denotes the number of

competitive nodes. Therefore; each node maintains two tables, the Direct Range Members (DRM) and Indirect Range Members (IRM) tables. DRM is found from the first hop nodes and IRM may be found from two or more hops nodes or hidden nodes. A node wishing to transmit data should consider both its local bandwidth and the bandwidth of all interference range nodes. In our proposed system, each node sends out a special signal with double power at a predefined interval, and collects all the signals from its neighboring nodes and updates its DRM and IRM tables.
The local bandwidth and neighboring nodes' bandwidth are determined as below.
Since bandwidth is shared among neighboring nodes, a node listens to the channel and estimates bandwidth based on the ratio of idle and busy times for a predefined interval.
The local bandwidth LBW is estimated as follows:

$$L_{BW} = C_{BW} X \frac{idle_t}{\text{int}_t} \qquad (1)$$

where C_{BW} denotes the channel capacity, $idle_t$denotes the idle time in a predefined interval $int_{t.}$
The neighboring nodes bandwidth is given by NMBW which is collected from the neighboring nodes.
So the residual bandwidth R_{BW} is calculated as

$$BW_{res} = NM_{BW} - L_{BW} \qquad (2)$$

C. Estimating Requested Bandwidth

Let Nand $F_L$be the session duration and frame length respectively. Let the traffic arrival rate be TR_i,(bps) and packet size is b_i bits. When a traffic flow wants to establish a connection with BS, it sends parameters TR_i, and $b_i$to the BS and waits for the responses from BS. An extra parameter, delay requirement $Dreq_i$, will be sent by rtPS flows. In order to meet delay requirement of rtPS packets, packets generated at time t must start to send after k_i-1 frames after t, where

$$k_i = \frac{Dreq_i}{F_L} \qquad (4)$$

If data rate is bigger than TR_i, these $b_i$bits can be shared by k_i-1 frames before deadline.
Therefore, our estimation of the data volume in a time frame is:

$$(TR_i * F_L) + \frac{Dreq_i}{k_i - 1} \qquad (5)$$

And, the expected bandwidth of the flow is estimated as

$$TR_i + \frac{Dreq_i}{(k_i - 1) * F_L} \qquad (6)$$

Let N_{rtPS} be the number of rtPS connections, BW_{req} be the bandwidth required by all rtPS connections, we can know that BW_{req} can be calculated as

$$BW_{req} = \sum_{i}^{N_{rtPS}} (TR_i + \frac{Dreq_i}{(k_i - 1) * F_L} \qquad (7)$$

D. Call Admission Control

In order to avoid starvation of some traffic classes, we set a threshold of bandwidth used for each class. They are: TUGS,
T_{rtPS}, T_{nrtPS} and T_{BE},
$T_{UGS} + T_{rtPS} + T_{nrtPS} + T_{BE} \leq BW_{Tot}$,

where $BW_{Tot}$is the total bandwidth. When the bandwidth occupied by a class is over its threshold, this class will have lower priority to the bandwidth resource.
For rtPS flow, (3) is used to estimate its bandwidth; for the other three flows, TR_i, the token rate, will be used to estimate bandwidth. Our CAC algorithm is as follows:

Algorithm

i. Calculate the residual bandwidth BW_{res} and requested bandwidth BWreq using (2) and (7), respectively.
ii. If BWreq< BWres, then
Accept the new flow
Else
iii. If BW (nrtPS) > ThnrtPS and BW (BE) > ThBE
Allocate less time slots
Go to step-2.
iv. Else if BW (rtPS) > Th_{rtPS} and BW (UGS) >Th_{UGS} then
Degrade Tr_i of UGS and rtPS.
Else
v. Reject new flow.
End if.
End if.
End if.

In the above algorithm, step-5 refers to the —Stealing bandwidth from upper class".Stealing bandwidth from upper class may be an issue. Stealing bandwidth from BE and nrtPS flows is relatively simple. We can easily decrease the bandwidth used by them because of they are not real-time flows. To steal bandwidth from the other two real-time classes, we will choose some connections of these two classes and degrade their TR_i, e.g. make TR_i to be C • TR_i, where 0 < C < 1.

IV. Simulation Results

A. Simulation Model And Parameters

To simulate the proposed scheme, network simulator (NS2) [13] is used. The proposed scheme has been implemented over IEEE 802.16 MAC protocol. In the simulation, clients (SS) and the base station (BS) are deployed in a 1000 meter x 1000 meter region for 50 seconds simulation time. All nodes have the same transmission range of 250 meters. In

the simulation, the video traffic (VBR) and CBR traffic are used.

The simulation settings and parameters are summarized in table 1.

Area Size	1000 X 1000
Mac	802.16
Nodes	50
Radio Range	250m
Simulation Time	50 sec
Traffic Source	VBR
Physical Layer	OFDM
Packet Size	1500 bytes
Frame Duration	0.005
Rate	1Mb
OFDM Bandwidth	10 MHz

B. *Performance Metrics*

We compare our efficient CAC (ECAC) method with the Modified Complete Sharing algorithm with CAC (MCS-CAC) [7]. We mainly evaluate the performance according to the following metrics

Blocking Probability- It is the ratio of number of requests rejected to the total number of requests.

Average End-to-End Delay-The end-to-end-delay is averaged over all surviving data packets from the sources to the destinations.

Throughput-It is the bandwidth received measured in Mb/s.

The performance results are presented in the next section.

V. RESULTS

A. *Based on Traffic class*

In our initial experiment we vary the classes: UGS, rtPS, nrtPS andBE, as 1, 2, 3 and 4

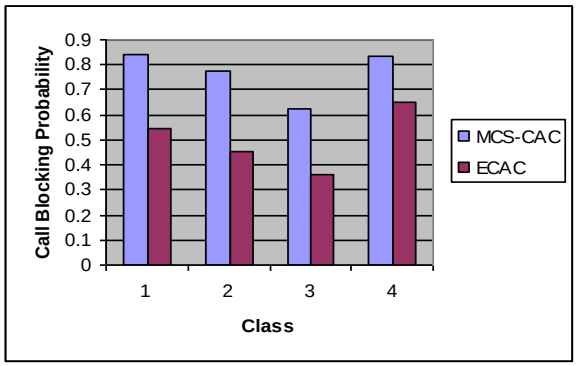


Fig: 1 Class Vs Blocking Probability

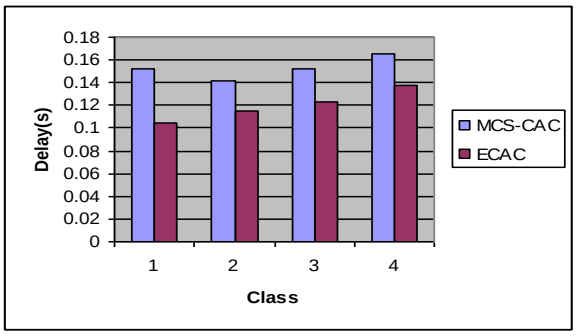


Fig: 2 Class Vs Delay

Fig: 1 shows that the blocking probability is more for MCS-CAC when compared with our proposed ECAC scheme. From Fig: 2 it is clear that the delay for our proposed ECAC scheme is less when compared with the MCS-CAC scheme.

B. *Based on number of Users*

In our second experiment we vary the number of users as 2, 4, 6 and 8.

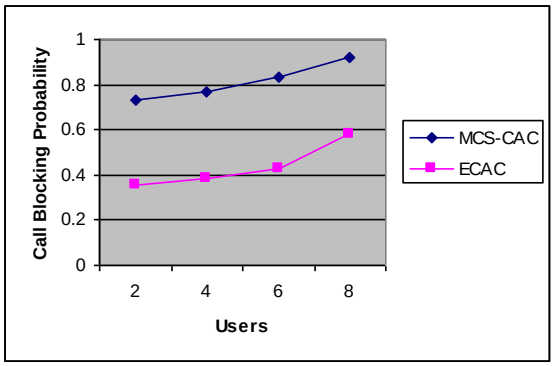


Fig: 3 Users Vs Blocking Probability

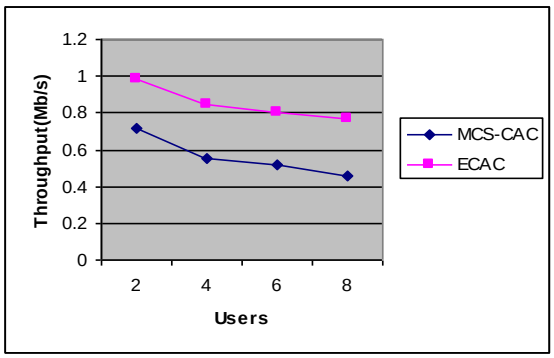


Fig: 4 Users Vs Throughput

Fig: 3 show that the blocking probability is more for MCS-CAC when compared with our proposed ECAC scheme. From Fig: 4 it is clear that the throughput for our proposed ECAC scheme is high when compared with the MCS-CAC scheme.

VI. CONCLUSION

There has been no architecture that clearly describes a CAC for IEEE 802.16 networks. Though some authors have suggested implicit conventional bandwidth based CAC, such simple CAC cannot guarantee QoS to application services.

In this paper, we have designed an efficient admission control mechanism for IEEE 802.16 networks to solve the above issues. Our CAC is based on the estimation of bandwidth utilization of each traffic class, with the constraint that the delay requirement of real-time flows should be satisfied. First the current available bandwidth is estimated for all the nodes based on the local and neighborhood bandwidth information. Then for the new incoming flows, the requested bandwidth is estimated for each class of service. Admission is made for the flows whose requested bandwidth is less than the available bandwidth. In order to admit a real time flow with additional bandwidth requirement, the QoS of best effort traffic is degraded by rate limiting its bandwidth. By simulation results we have shown that our proposed approach reduces the blocking probability, there by increasing the throughput for all classes of traffic.

VII. References

1) Chung-Wei Lin, Yu-Cheng Chen and Ai-Chun Pang, –A New Resource Allocation Scheme for IEEE 802.16-based Networks". 3rd IEEE VTS Asia Pacific Wireless Communications Symposium (AWPCS 2006), Aug. 2006.
2) M. Castrucci, I. Marchetti, C. Nardini, N. Ciulli and G. Landi, —A Framework for Resource Control in WiMAX Networks", In Proc. of the 2007 International Conference on Next Generation Mobile Applications, Services and Technologies, pp. 316-321, 2007.
3) Hanwu Wang and Weijia Jia, —Scalable and Adaptive Resource Scheduling in IEEE 802.16 WiMAX Networks", IEEE, GLOBECOM, 2008.
4) S.C. Wang, K.Q. Yan and C.H. Wang, –A Channel Allocation based WiMax Topology", International MultiConference of Engineers and Computer Scientists, March 18 - 20, 2009.
5) Arijit Ukil and Jaydip Sen, —QoSAware Cross-Layer Optimized Resource Allocation in WiMAX Systems", Wireless VITAE, 1st International Conference on 17-20 May 2009.
6) Xu-Zhen, Huang-ChuanHe and Hu-XianZhi, —Interference-aware Multi-path Routing and Bandwidth Allocation for Mobile Wireless Networks", ICCS, IEEE, 2008.
7) Ke Yu et al, –A Statistical Connection Admission Control Mechanism for Multiservice IEEE 802.16 Network", 69th Vehicular Technology Conference, IEEE, 26-29, April, 2009.
8) Ramesh Babu H.S, Gowrishankar and Satyanarayana .P, —A Analytical framework for Call Admission Control in Heterogeneous Wireless Networks", IJCSNS International Journal of 162 Computer Science and Network Security, VOL.9 No.10, October 2009.
9) Sarat Chandra and Anirudha Sahoo, –An Efficient Call Admission Control for IEEE 802.16 Networks", 15th IEEE Workshop on Local and Metropolitan Area Networks, LANMAN, June, 2007.
10) Eunhyun Kwon et al, –A Performance Model for Admission Control in IEEE 802.16", Proceedings of WWIC 2005, LNCS 3510, Springer-Verlag, vol. 3510, pp. 159-168, May, 2005.
11) Prasun Chowdhury, Iti Saha Misra and Salil K Sanyal, –An Integrated Call Admission Control and Uplink Packet Scheduling Mechanism for QoS Evaluation of IEEE 802.16 BWA Networks", Canadian Journal on Multimedia and Wireless Networks,vol-1, No.3, April 2010.
12) Anas Majeed, A. A. Zaidan, B. B. Zaidan and Laiha Mat Kiah, —Towards for Admission Control in WIMAX Relay Station Mesh Network for Mobile Stations out of Coverage Using Ad-Hoc", World Academy of Science, Engineering and Technology 54 2009.
13) Network Simulator, http://www.isi.edu/nsnam/ns

Generation Of Arbitrary Topologies For The Evaluation Stages In Critical Node Test Mechanism

Nitiket N Mhala

GJCST Classification
B.4.3,C.2.1

***Abstract*-The applications of MANET are increasing in modern generation. But MANET are more vulnerable to many attacks because of their adhoc nature. The security issue is the main concern in the use of MANET application.Therefor, the selection of efficient methodologies and techniques to protect MANET is an important aspect. Detecting malicious nodes in an open adhoc network in which participating nodes have no previous security associations presents a number of challenges not faced by the traditional wired networks. Traffic monitoring in wired network is usually preferred at switches, routers and gateways, but adhoc network does not have these types of network elements where the Intrusion Detection System (IDS) can collect and analyze audit data for the entire network. Any kind of network diagnosis or intrusion detection depends on the degree of mobility of nodes. This paper presents a Critical Node Test Mechanism which is a lightweight solution that can be used to determine the proper conditions to activate more demanding IDS. Here, we generate arbitrary logical network topologies in order to perform real time operations on adhoc network at a relatively low cost in a laboratory environment without having to physically move the nodes in the adhoc network.**

Keywords- adhoc, test bed, critical node, node degree, MANET, IDS.

I. INTRODUCTION

A mobile adhoc network is a relatively new communication paradigm. In modern generation, theapplications of MANET are increasing in use. MANET does not require expensive base stations of wired infrastructure. Therefore, it is an attractive networking option for connecting mobile devices quickly and spontaneously. MANET is self organized in such way that a collection of mobile nodes without a fixed infrastructure and central management is formed automatically. Wireless presents a number of unique problems for Intrusion Detection System (IDS). Network traffic can be monitored on a wire segment, but adhoc nodes can only monitor network traffic within their observable radio range. A MANET is most likely not under a single administrative domain, making it difficult to perform any kind of centralized management or control.

In an adhoc network, malicious node may enter and leave the intermediate radio transmission range at random interval, may collude with other malicious nodes to disrupt network activity and avoid detection, or behave maliciously only intermittently, further complication their detection. A node that sends out false routing information could be a compromised node, or merely a node that has a temporarily stale routing table due to volatile physical conditions. Packets may be dropped due to network congestion or because a malicious node is not faithfully executing a routing algorithm [1] MANET with loose or no prior security associations are more difficult to diagnose than a MANET comprised of nodes from the same organization with strong security services. Establishing trust in an open adhoc network in which higher-level security services are unavailable can be hampered by the short lived presence of both collaborating and malicious nodes. In addition to having no previously established trust associations, nodes in an adhoc network have little incentive for reciprocity to faithfully execute a routing protocol or provide a minimum level of service. Closed adhoc networks that support critical applications may not be able to tolerate the presence of malicious nodes; fortunately closed networks can more established prior trust associations for collaborative IDS. The effectiveness of collaborative IDS also depends on the amount and trustworthiness of data that can be collected by each node.

Malicious nodes in sparsely populated networks can be more harmful than malicious nodes in a densely populated network since these nodes can effectively not only disrupt communication but also disconnect the network.

II. RELATED WORK

Various IDS techniques have been proposed in the research literature.Zhang and Lee describe a distributed and collaborative anomly detection-based IDS for adhoc network [2,3]. Theodorakpoulos and Baras present a method for establishing trust metrices and Evaluting trust [4].Michiardi and Molva assign a value to the “reputation” of a node and use this information to identify misbehaving nodes and co-operate only with trusted reputations. [5].Certain nodes in MANETS can produce attacks which cause congestion, distribution of incorrect routing information,services preventing proper operation or disable them[6].As routing protocols exchange routing data between nodes, as a result, they would maintain routing status in each node.Based on routing status ,data packets are transmitted by mediated nodes along an established route to the destination [7]. M.K Rafsanjani,A Movaghar presents a scheme in which nodes do not need to exchange multiple messages to prove their identities[8].

III. METHODOLOGY

The dynamic nature of adhoc networks suggests that preventation techniques that monitor the security status of the network and identify anomalous and /or malicious

About-Associate Professor M.E(Electronic) Phd(Wireless Adhoc Network)(persuing) nitiket_m@rediffmail.com

behavior. These techniques are usually less expensive to implement and can be easily developed in existing adhoc networks without requiring modification to nodes configuration or routing protocols being used. Here, our concept is built around the notion of critical node in an adhoc network. We consider a critical node whose failure or malicious behavior disconnects or significantly degrades the performance of the network.

In order to determine a critical node, a graph theoretic approach to detect a vertex-cut and an edge-cut is studied. [9].A vertex-cut is a set of vertices whose removal produces a sub graph with more components than the original graph. A cut-vertex or articulation point is a vertex cut on sitting of single vertex. An edge-cut is a set of edges whose removal produces a sub graph with more components than original graph. A cut-edge or bridge, is an edge –cut consisting of a single edge. Although the cut-vertex or cut edge of graph G can be determined by applying a straight forward algorithm. Finding a cut vertex in the graphical representation of an adhoc network is not a straightforward, since the nodes cannot be assumed to be stationary. A network discovery algorithm can give an approximation of the network topology, but the value of such an approximation in performing any kind of network diagnosis or intrusion detection depends on the degree of mobility of nodes.

A. Role Of Our Adhoc Network Test Bed

The basic idea of our emulation Test Bed[10] is having a number of MANET nodes physically close to each other inside the laboratory, but forces them to 'think' that they can only communicate with a selected few of them. That way, we can emulate a logical topology. In order to work, there is the need of hardware. Our Test bed is an emulator, not a simulator. So, we have the necessary hardware equipment. Each node is a device that has a wireless (802.11 b/g) interface, so that it can communicate with other adhoc nodes and run MANET protocols. In addition, the device should also have a wired interface (Ethernet), which is used for administrative purposes. In brief, the Test Bed uses the wired interface to transfer files needed for its operation to and from the node and manipulate its networking element in such way that will create logical topology we want. That Leaves the wireless interface free of any interface and most importantly, emulates an actual MANET, which is the whole point all along. In fact, Test Bed uses ix86 architecture and Linux can run even in 80386 machines (at least requirement is Pentium II), so we can gather all those old PCs intended thrown away, adding a PCMCIA wireless card on each of them and set up a MANET test bed in a laboratory at a very low cost.

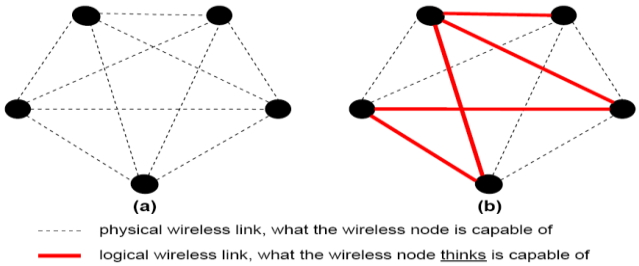


Figure1. (a) Physical links, (b) logical links between MANET nodes

B. Design Concept For Creation Of Logical Topology In Our Test Bed

Determining the global network topology in a mobile adhoc network is somewhat difficult, but determining an approximation of this topology or subset of this topology within a certain time frame may be useful. Our test bed allows user to create arbitrary network topologies and emulate the mobility. By changing the logical topology of the network, users can conduct test on adhoc network without having to physically move the nodes in the adhoc network. By giving the number of nodes in adhoc network Test Bed, each node's IP and MAC address, software module used in a test Bed creates arbitrarily connected graphs and updates each node's IP_TABLES accordingly through socket servers running on each network node in order to reflect the new logical topology. Thus arbitrary graph is represented in an adjacency matrix that is then translated into the corresponding IP_TABLES. Software module uses open source graph visualization tool Graphviz [11] to display the logical topology of the adhoc network as shown below.

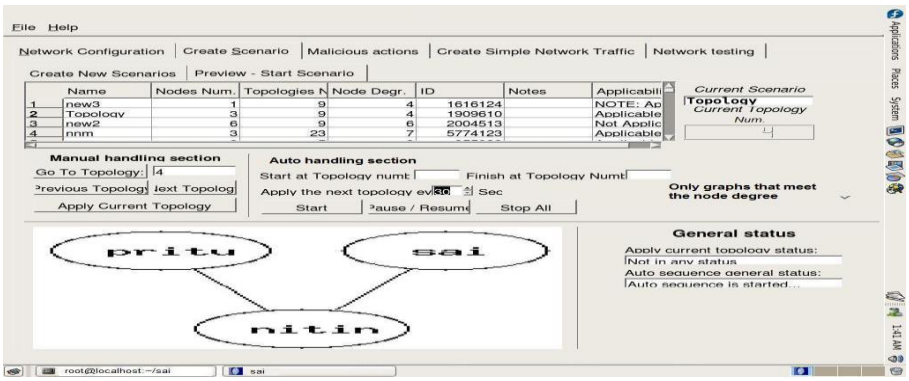


Fig. 2 Logical Topology Creation (Node degree = 4)

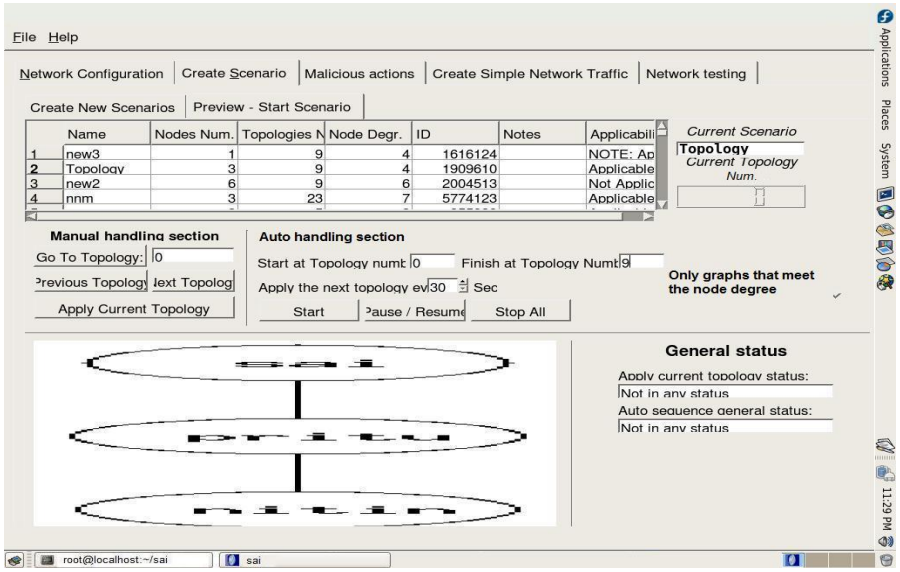


Fig. 3 Logical Topology Creation (Node degree = 4)

Above figures indicates arbitrary creation of logical topology of actual three nodes in every 30 seconds in our laboratory. We can set 150 physical nodes and theoretically, there is no limit to the number of nodes this test bed can handle. Therefore, we design the module which allows users to save and replay different mobility scenarios to control the maximum and minimum degree, produces an output in the form of adjacency matrix for further analysis and produces a framework for building additional adhoc network tools. An approximation of the network topology can provide the useful information about network density, network mobility, critical path and critical nodes.

IV. CRITICAL NODE TEST CONSIDERATION

A. Basic Steps

i. The node performing the test is referred to as testing node and the node under test is referred as node under test.

ii. Use of ip,route and ping utilities The ip utility is a TCP/IP interface configuration and routing utility that configures the network interfaces

iii. The route utility manipulates the Kernel's IP routing Table. It's primary purpose is to set static routes to specific hosts or networks via an interface after it has been configured with ifconfig program.

iv. When used together,ip route provides the necessary tools for manipulating any routing tables such as displaying routes, routing cache ,adding routes, deleting routes, altering routes, getting routing information and clearing routing table.

B. Evaluation Stages In A Critical Node Test Mechanism

It is very necessary to detect whether the testing node shares a critical link with its Neighbors.

i. First Stage

a) To temporarily modify the testing node's routing table to allow only one communication link to be operational at a time, while blocking communication through all others.

b) The enabled communication link will be between the testing node and a node other than the node under test.

c) Each communication link has to test sequentially in this way to determine if an alternative path to the link under test exists.

d) If an alternative path exists, then the link is not critical because its removal will not disconnect the network.

ii. Second Stage

1) This stage is for the host to attempt to discover an alternative path by using ping to the node under testwithout using the suspected cut-edge between the testing node and node under test.

2) To discover an alternative path to the node under test, the testing node executes the following command

#ping –c –s 4 < node_under_test> -A-R

Where –c is the number of pings that the host executes

-s is the number of data bytes to be sent

-A is the audit flag

-R flag returns the route, if exists, to the < node_under_test> node

iii. Third stage

1) When the results of the ping are returned, the network routing table is restored during this finalstep to its initial configuration.
2) . It is very important to note that, after the end of critical node test, all previously established routes are restored .The duration of critical node depends on the network density and topology.
3) Critical node conditions however are likely to occur when a node has a relatively small degree (see fig 3 and fig 4) and therefore fewer tests are required.

V. INFERENCES

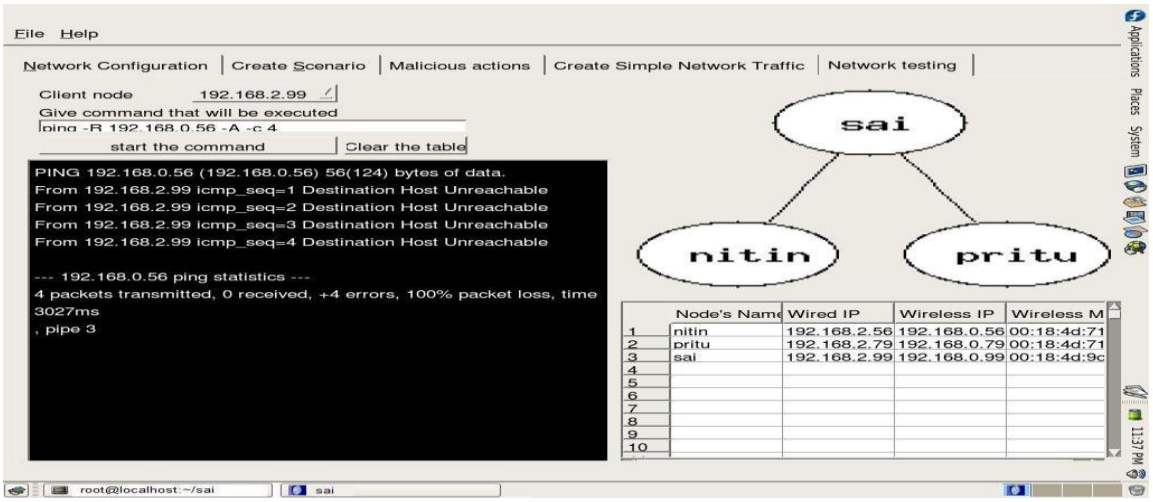


Fig. 4 (node test)

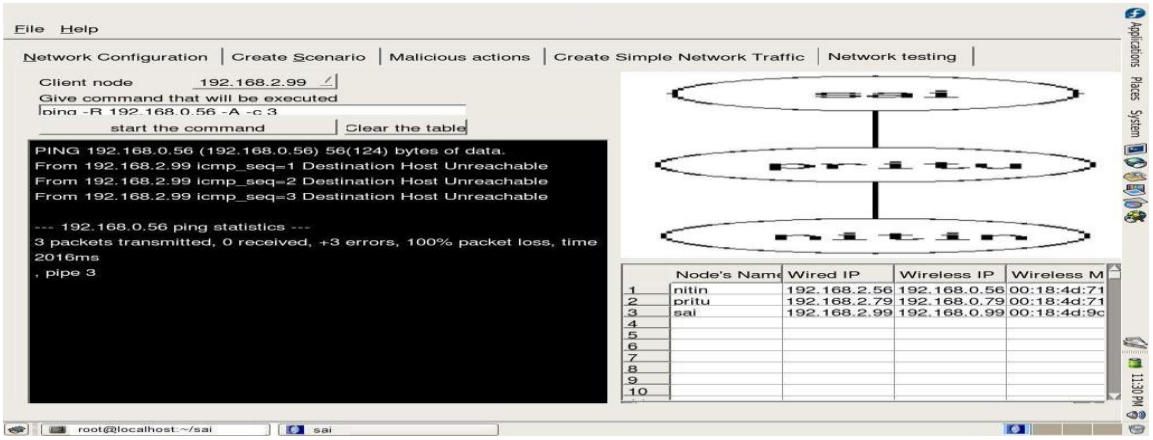


Fig. 5 (node test)

Above two figures show different topology created in our test bed for the same node degree of 4.

Fig 4- indicates the ping results from the Host node Sai (Wired IP 192.168.2.99 & Wireless IP 192.168.0.99) To node nitin (Wired IP 192.168.2.56 & wireless IP 192.168.0.56) showing the node nitin unreachable.

(The statistics is that 4 packets transmitted, 0 received, +4 errors, 100% packet loss, time 3027 ms,pipe 3)

Fig 5- indicates the ping results from the Host node Sai (Wired IP 192.168.2.99 & Wireless IP 192.168.0.99) to node nitin (Wired IP 192.168.2.56 & wireless IP 192.168.0.56) showing the node nitin unreachable for the changed topology.

(The statistics is that 3 packets transmitted, 0 received, +3 errors, 100% packet loss, time 2016 ms,pipe 3)Thus, we made inference that Host node Sai has a critical (or semi critical) link with node nitin.

VI. . Conclusion and Future Work

In order to improve the lifetime of the network, an effective method in selecting a monitoring node is needed so that a required level of detection Intrusion in MANET would be provided. When a critical link is detected, it can be the focus of more resource intensive or other diagnostic measures. The host node may choose expend additional resources to initiate an IDS module that is more resource intensive such as Traffic monitoring watch dog module or Collaborative IDS.But if there is no critical link then this metric can be used to help decide if the application or risk environment warrant the expenditure of additional requires monitoring diagnosis and and altering other nodes about the problems. Or if there is no critical link then host can use the lighter modules to continue to monitor network traffic. Therefore, we may conclude that Critical Node Test Mechanism is a lightweight solution that can be used to determine the proper conditions to activate more demanding IDS.Involment of Trigger mechanism for the invocation of critical node test in a mobile adhoc network will be the basis of our future work. This paper effort to focus that, generating arbitrary topologies create scenarios can help researchers to test experimental IDS system under the difficult situations. We may conclude since the global topology of the adhoc network is known, which will help researchers to benchmark the actual performance of their adhoc routing algorithms and applications against the theoretical optimal performance.

VII. Acknowledgement

The authors would like to thank everyone, including the anonymous reviewers

VIII. References

1) A.Patwardhan,J.Parkar,A.Johi, A. Karyygiannis and M Iorga. Secure routing and Intrusion Detection in Ad-hoc Networks. Third International conference on Pervasive computing and communications 2005
2) Y. Zhang and W Lee. Intrusion Detection in wireless ad hoc network. In Proceedings of the 6th annual International conference on Mobile Computing and Networking,pp 275-283,2000
3) Y. Zhang, W. Lee and Y.Hang. Intrusion Detection techniques for mobile wireless network. ACM/Kluwer Mobile Networks and applications (MONET), 2002
4) Theodorakopoules, George and Baras, Jhon. Trust evaluation in adhoc networks. Proceedings of the 2004 ACM workshop on Wireless security,pp. 1-10,2004
5) Michiardi, P and Molva, R,"Core: A Collaborative Reputation mechanism to enforce node cooperation in Mobile Adhoc Networks",Communication and Multimedia Security 2002 Conference.
6) Karygiannis, E.Antonakakis and A. Apostolopoulos, Detecting critical nodes for MANET intrusion detection system. In Proc 2nd International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous computing, 2006.
7) N.Komnios, D.Vergados and C. Douligeries. —Detecting unauthorized and compromised nodes in mobile adhoc network." Elseviewer Adhoc network, vol5, n0 3, pp.289-298, 2007
8) M. K Rafsanjani, A Movaghar,"Identifying monitoring nodes with selection of Authorized nodes in mobile Adhoc network",World Applied Sciences Journal,vol4,n03, pp.444-449,2008
9) Graphs:Theory and Algorithms, K. Thuasiraman, M.N.S Swamy.
10) Nitiket N Mhala, N K Choudhari, —An Envision of Low cost Mobile Adhoc network Test bed in a laboratory Environment emulating actual MANET ", IJCNC,Vol.2, No.3,May 2010.
11) http://www.graphviz.org

Global Journals Guidelines Handbook 2010

www.GlobalJournals.org

FELLOW OF INTERNATIONAL CONGRESS OF COMPUTER SCIENCE AND TECHNOLOGY (FICCT)

- FICCT' title will be awarded to the person after approval of Editor-in-Chief and Editorial Board. The title 'FICCT" can be added to name in the following manner e.g. **Dr. Andrew Knoll, Ph.D., FICCT, Er. Pettor Jone, M.E., FICCT**
- FICCT can submit two papers every year for publication without any charges. The paper will be sent to two peer reviewers. The paper will be published after the acceptance of peer reviewers and Editorial Board.
- Free unlimited Web-space will be allotted to 'FICCT 'along with subDomain to contribute and partake in our activities.
- A professional email address will be allotted free with unlimited email space.
- FICCT will be authorized to receive e-Journals - GJCST for the Lifetime.
- FICCT will be exempted from the registration fees of Seminar/Symposium/Conference/Workshop conducted internationally of GJCST (FREE of Charge).
- FICCT will be an Honorable Guest of any gathering hold.

ASSOCIATE OF INTERNATIONAL CONGRESS OF COMPUTER SCIENCE AND TECHNOLOGY (AICCT)

- AICCT title will be awarded to the person/institution after approval of Editor-in-Chef and Editorial Board. The title 'AICCTcan be added to name in the following manner:
  eg. **Dr. Thomas Herry, Ph.D., AICCT**
- AICCT can submit one paper every year for publication without any charges. The paper will be sent to two peer reviewers. The paper will be published after the acceptance of peer reviewers and Editorial Board.
- Free 2GB Web-space will be allotted to 'FICCT' along with subDomain to contribute and participate in our activities.
- A professional email address will be allotted with free 1GB email space.
- AICCT will be authorized to receive e-Journal GJCST for lifetime.
- A professional email address will be allotted with free 1GB email space.
- AICHSS will be authorized to receive e-Journal GJHSS for lifetime.

ANNUAL MEMBER

- Annual Member will be authorized to receive e-Journal GJCST for one year (subscription for one year).
- The member will be allotted free 1 GB Web-space along with subDomain to contribute and participate in our activities.
- A professional email address will be allotted free 500 MB email space.

PAPER PUBLICATION

- The members can publish paper once. The paper will be sent to two-peer reviewer. The paper will be published after the acceptance of peer reviewers and Editorial Board.

Process of submission of Research Paper

The Area or field of specialization may or may not be of any category as mentioned in 'Scope of Journal' menu of the GlobalJournals.org website. There are 37 Research Journal categorized with Six parental Journals GJCST, GJMR, GJRE, GJMBR, GJSFR, GJHSS. For Authors should prefer the mentioned categories. There are three widely used systems UDC, DDC and LCC. The details are available as 'Knowledge Abstract' at Home page. The major advantage of this coding is that, the research work will be exposed to and shared with all over the world as we are being abstracted and indexed worldwide.

The paper should be in proper format. The format can be downloaded from first page of 'Author Guideline' Menu. The Author is expected to follow the general rules as mentioned in this menu. The paper should be written in MS-Word Format (*.DOC,*.DOCX).

The Author can submit the paper either online or offline. The authors should prefer online submission.

Online Submission: There are three ways to submit your paper:

(A) (I) Register yourself using top right corner of Home page then Login from same place twice. If you are already registered, then login using your username and password.

(II) Choose corresponding Journal from "Research Journals" Menu.

(III) Click 'Submit Manuscript'. Fill required information and Upload the paper.

(B) If you are using Internet Explorer (Although Mozilla Firefox is preferred), then Direct Submission through Homepage is also available.

(C) If these two are not convenient, and then email the paper directly to dean@globaljournals.org as an attachment.

Offline Submission: Author can send the typed form of paper by Post. However, online submission should be preferred.

Preferred Author Guidelines

MANUSCRIPT STYLE INSTRUCTION (Must be strictly followed)

Page Size: 8.27" X 11'"

- Left Margin: 0.65
- Right Margin: 0.65
- Top Margin: 0.75
- Bottom Margin: 0.75
- Font type of all text should be Times New Roman.
- Paper Title should be of Font Size 24 with one Column section.
- Author Name in Font Size of 11 with one column as of Title.
- Abstract Font size of 9 Bold, "Abstract" word in Italic Bold.
- Main Text: Font size 10 with justified two columns section
- Two Column with Equal Column with of 3.38 and Gaping of .2
- First Character must be two lines Drop capped.
- Paragraph before Spacing of 1 pt and After of 0 pt.
- Line Spacing of 1 pt
- Large Images must be in One Column
- Numbering of First Main Headings (Heading 1) must be in Roman Letters, Capital Letter, and Font Size of 10.
- Numbering of Second Main Headings (Heading 2) must be in Alphabets, Italic, and Font Size of 10.

You can use your own standard format also.

Author Guidelines:

1. General,

2. Ethical Guidelines,

3. Submission of Manuscripts,

4. Manuscript's Category,

5. Structure and Format of Manuscript,

6. After Acceptance.

1. GENERAL

Before submitting your research paper, one is advised to go through the details as mentioned in following heads. It will be beneficial, while peer reviewer justify your paper for publication.

Scope

The Global Journals welcome the submission of original paper, review paper, survey article relevant to the all the streams of Philosophy and knowledge. The Global Journals is parental platform for Global Journal of Computer Science and Technology, Researches in Engineering, Medical Research, Science Frontier Research, Human Social Science, Management, and Business organization. The choice of specific field can be done otherwise as following in Abstracting and Indexing Page on this Website. As the all Global Journals are being

abstracted and indexed (in process) by most of the reputed organizations. Topics of only narrow interest will not be accepted unless they have wider potential or consequences.

2. ETHICAL GUIDELINES

Authors should follow the ethical guidelines as mentioned below for publication of research paper and research activities.

Papers are accepted on strict understanding that the material in whole or in part has not been, nor is being, considered for publication elsewhere. If the paper once accepted by Global Journals and Editorial Board, will become the copyright of the Global Journals.

Authorship: The authors and coauthors should have active contribution to conception design, analysis and interpretation of findings. They should critically review the contents and drafting of the paper. All should approve the final version of the paper before submission

The Global Journals follows the definition of authorship set up by the Global Academy of Research and Development. According to the Global Academy of R&D authorship, criteria must be based on:

1) Substantial contributions to conception and acquisition of data, analysis and interpretation of the findings.

2) Drafting the paper and revising it critically regarding important academic content.

3) Final approval of the version of the paper to be published.

All authors should have been credited according to their appropriate contribution in research activity and preparing paper. Contributors who do not match the criteria as authors may be mentioned under Acknowledgement.

Acknowledgements: Contributors to the research other than authors credited should be mentioned under acknowledgement. The specifications of the source of funding for the research if appropriate can be included. Suppliers of resources may be mentioned along with address.

Appeal of Decision: The Editorial Board's decision on publication of the paper is final and cannot be appealed elsewhere.

Permissions: It is the author's responsibility to have prior permission if all or parts of earlier published illustrations are used in this paper.

Please mention proper reference and appropriate acknowledgements wherever expected.

If all or parts of previously published illustrations are used, permission must be taken from the copyright holder concerned. It is the author's responsibility to take these in writing.

Approval for reproduction/modification of any information (including figures and tables) published elsewhere must be obtained by the authors/copyright holders before submission of the manuscript. Contributors (Authors) are responsible for any copyright fee involved.

3. SUBMISSION OF MANUSCRIPTS

Manuscripts should be uploaded via this online submission page. The online submission is most efficient method for submission of papers, as it enables rapid distribution of manuscripts and consequently speeds up the review procedure. It also enables authors to know the status of their own manuscripts by emailing us. Complete instructions for submitting a paper is available below.

Manuscript submission is a systematic procedure and little preparation is required beyond having all parts of your manuscript in a given format and a computer with an Internet connection and a Web browser. Full help and instructions are provided on-screen. As an author, you will be prompted for login and manuscript details as Field of Paper and then to upload your manuscript file(s) according to the instructions.

To avoid postal delays, all transaction is preferred by e-mail. A finished manuscript submission is confirmed by e-mail immediately and your paper enters the editorial process with no postal delays. When a conclusion is made about the publication of your paper by our Editorial Board, revisions can be submitted online with the same procedure, with an occasion to view and respond to all comments.

Complete support for both authors and co-author is provided.

4. MANUSCRIPT'S CATEGORY

Based on potential and nature, the manuscript can be categorized under the following heads:Original research paper: Such papers are reports of high-level significant original research work.

Review papers: These are concise, significant but helpful and decisive topics for young researchers.

Research articles: These are handled with small investigation and applications

Research letters: The letters are small and concise comments on previously published matters.

5. STRUCTURE AND FORMAT OF MANUSCRIPT

The recommended size of original research paper is less than seven thousand words, review papers fewer than seven thousands words also. Preparation of research paper or how to write research paper, are major hurdle, while writing manuscript. The research articles and research letters should be fewer than three thousand words, the structure original research paper; sometime review paper should be as follows:

Papers: These are reports of significant research (typically less than 7000 words equivalent, including tables, figures, references), and comprise:

(a)Title should be relevant and commensurate with the theme of the paper.

(b) A brief Summary, "Abstract" (less than 150 words) containing the major results and conclusions.

(c) Up to ten keywords, that precisely identifies the paper's subject, purpose, and focus.

(d) An Introduction, giving necessary background excluding subheadings; objectives must be clearly declared.

(e) Resources and techniques with sufficient complete experimental details (wherever possible by reference) to permit repetition; sources of information must be given and numerical methods must be specified by reference, unless non-standard.

(f) Results should be presented concisely, by well-designed tables and/or figures; the same data may not be used in both; suitable statistical data should be given. All data must be obtained with attention to numerical detail in the planning stage. As reproduced design has been recognized to be important to experiments for a considerable time, the Editor has decided that any paper that appears not to have adequate numerical treatments of the data will be returned un-refereed;

(g) Discussion should cover the implications and consequences, not just recapitulating the results; conclusions should be summarizing.

(h) Brief Acknowledgements.

(i) References in the proper form.

Authors should very cautiously consider the preparation of papers to ensure that they communicate efficiently. Papers are much more likely to be accepted, if they are cautiously designed and laid out, contain few or no errors, are summarizing, and be conventional to the approach and instructions. They will in addition, be published with much less delays than those that require much technical and editorial correction.

The Editorial Board reserves the right to make literary corrections and to make suggestions to improve briefness.

It is vital, that authors take care in submitting a manuscript that is written in simple language and adheres to published guidelines.

Format

Language: The language of publication is UK English. Authors, for whom English is a second language, must have their manuscript efficiently edited by an English-speaking person before submission to make sure that, the English is of high excellence. It is preferable, that manuscripts should be professionally edited.

Standard Usage, Abbreviations, and Units: Spelling and hyphenation should be conventional to The Concise Oxford English Dictionary. Statistics and measurements should at all times be given in figures, e.g. 16 min, except for when the number begins a sentence. When the number does not refer to a unit of measurement it should be spelt in full unless, it is 160 or greater.

Abbreviations supposed to be used carefully. The abbreviated name or expression is supposed to be cited in full at first usage, followed by the conventional abbreviation in parentheses.

Metric SI units are supposed to generally be used excluding where they conflict with current practice or are confusing. For illustration, 1.4 l rather than 1.4 × 10-3 m3, or 4 mm somewhat than 4 × 10-3 m. Chemical formula and solutions must identify the form used, e.g. anhydrous or hydrated, and the concentration must be in clearly defined units. Common species names should be followed by underlines at the first mention. For following use the generic name should be constricted to a single letter, if it is clear.

Structure

All manuscripts submitted to Global Journals, ought to include:
Title: The title page must carry an instructive title that reflects the content, a running title (less than 45 characters together with spaces), names of the authors and co-authors, and the place(s) wherever the work was carried out. The full postal address in addition with the e-mail address of related author must be given. Up to eleven keywords or very brief phrases have to be given to help data retrieval, mining and indexing.
Abstract, used in Original Papers and Reviews:
Optimizing Abstract for Search Engines
Many researchers searching for information online will use search engines such as Google, Yahoo or similar. By optimizing your paper for search engines, you will amplify the chance of someone finding it. This in turn will make it more likely to be viewed and/or cited in a further work. Global Journals have compiled these guidelines to facilitate you to maximize the web-friendliness of the most public part of your paper.

Key Words
A major linchpin in research work for the writing research paper is the keyword search, which one will employ to find both library and Internet resources.
One must be persistent and creative in using keywords. An effective keyword search requires a strategy and planning a list of possible keywords and phrases to try.

Search engines for most searches, use Boolean searching, which is somewhat different from Internet searches. The Boolean search uses "operators," words (and, or, not, and near) that enable you to expand or narrow your affords. Tips for research paper while preparing research paper are very helpful guideline of research paper.

Choice of key words is first tool of tips to write research paper. Research paper writing is an art.A few tips for deciding as strategically as possible about keyword search:

- One should start brainstorming lists of possible keywords before even begin searching. Think about the most important concepts related to research work. Ask, "What words would a source have to include to be truly valuable in research paper?" Then consider synonyms for the important words.
- It may take the discovery of only one relevant paper to let steer in the right keyword direction because in most databases, the keywords under which a research paper is abstracted are listed with the paper.
- One should avoid outdated words.

Keywords are the key that opens a door to research work sources. Keyword searching is an art in which researcher's skills are bound to improve with experience and time.

Numerical Methods: Numerical methods used should be clear and, where appropriate, supported by references.

Acknowledgements: Please make these as concise as possible.

References

References follow the Harvard scheme of referencing. References in the text should cite the authors' names followed by the time of their publication, unless there are three or more authors when simply the first author's name is quoted followed by et al. unpublished work has to only be cited where necessary, and only in the text. Copies of references in press in other journals have to be supplied with submitted typescripts. It is necessary that all citations and references be carefully checked before submission, as mistakes or omissions will cause delays.

References to information on the World Wide Web can be given, but only if the information is available without charge to readers on an official site. Wikipedia and Similar websites are not allowed where anyone can change the information. Authors will be asked to make available electronic copies of the cited information for inclusion on the Global Journals homepage at the judgment of the Editorial Board.

The Editorial Board and Global Journals recommend that, citation of online-published papers and other material should be done via a DOI (digital object identifier). If an author cites anything, which does not have a DOI, they run the risk of the cited material not being noticeable.

The Editorial Board and Global Journals recommend the use of a tool such as Reference Manager for reference management and formatting.

Tables, Figures and Figure Legends

Tables: Tables should be few in number, cautiously designed, uncrowned, and include only essential data. Each must have an Arabic number, e.g. Table 4, a self-explanatory caption and be on a separate sheet. Vertical lines should not be used.

Figures: Figures are supposed to be submitted as separate files. Always take in a citation in the text for each figure using Arabic numbers, e.g. Fig. 4. Artwork must be submitted online in electronic form by e-mailing them.

Preparation of Electronic Figures for Publication

Even though low quality images are sufficient for review purposes, print publication requires high quality images to prevent the final product being blurred or fuzzy. Submit (or e-mail) EPS (line art) or TIFF (halftone/photographs) files only. MS PowerPoint and Word Graphics are unsuitable for printed pictures. Do not use pixel-oriented software. Scans (TIFF only) should have a resolution of at least 350 dpi (halftone) or 700 to 1100 dpi (line drawings) in relation to the imitation size. Please give the data for figures in black and white or submit a Color Work Agreement Form. EPS files must be saved with fonts embedded (and with a TIFF preview, if possible).

For scanned images, the scanning resolution (at final image size) ought to be as follows to ensure good reproduction: line art: >650 dpi; halftones (including gel photographs) : >350 dpi; figures containing both halftone and line images: >650 dpi.

Color Charges: It is the rule of the Global Journals for authors to pay the full cost for the reproduction of their color artwork. Hence, please note that, if there is color artwork in your manuscript when it is accepted for publication, we would require you to complete and return a color work agreement form before your paper can be published.

Figure Legends: Self-explanatory legends of all figures should be incorporated separately under the heading 'Legends to Figures'. In the full-text online edition of the journal, figure legends may possibly be truncated in abbreviated links to the full screen version. Therefore, the first 100 characters of any legend should notify the reader, about the key aspects of the figure.

6. AFTER ACCEPTANCE

Upon approval of a paper for publication, the manuscript will be forwarded to the dean, who is responsible for the publication of the Global Journals.

6.1 Proof Corrections

The corresponding author will receive an e-mail alert containing a link to a website or will be attached. A working e-mail address must therefore be provided for the related author.

Acrobat Reader will be required in order to read this file. This software can be downloaded

(Free of charge) from the following website:

www.adobe.com/products/acrobat/readstep2.html. This will facilitate the file to be opened, read on screen, and printed out in order for any corrections to be added. Further instructions will be sent with the proof.

Proofs must be returned to the dean at dean@globaljournals.org within three days of receipt.

As changes to proofs are costly, we inquire that you only correct typesetting errors. All illustrations are retained by the publisher. Please note that the authors are responsible for all statements made in their work, including changes made by the copy editor.

6.2 Early View of Global Journals (Publication Prior to Print)

The Global Journals are enclosed by our publishing's Early View service. Early View articles are complete full-text articles sent in advance of their publication. Early View articles are absolute and final. They have been completely reviewed, revised and edited for publication, and the authors' final corrections have been incorporated. Because they are in final form, no changes can be made after sending them. The nature of Early View articles means that they do not yet have volume, issue or page numbers, so Early View articles cannot be cited in the conventional way.

6.3 Author Services

Online production tracking is available for your article through Author Services. Author Services enables authors to track their article - once it has been accepted - through the production process to publication online and in print. Authors can check the status of their articles online and choose to receive automated e-mails at key stages of production. The authors will receive an e-mail with a unique link that enables them to register and have their article automatically added to the system. Please ensure that a complete e-mail address is provided when submitting the manuscript.

6.4 Author Material Archive Policy

Please note that if not specifically requested, publisher will dispose off hardcopy & electronic information submitted, after the two months of publication. If you require the return of any information submitted, please inform the Editorial Board or dean as soon as possible.

6.5 Offprint and Extra Copies

A PDF offprint of the online-published article will be provided free of charge to the related author, and may be distributed according to the Publisher's terms and conditions. Additional paper offprint may be ordered by emailing us at:editor@globaljournals.org .

Informal Tips for writing a Computer Science Research Paper to increase readability and citation

Before start writing a good quality Computer Science Research Paper, let us first understand what is Computer Science Research Paper? So, Computer Science Research Paper is the paper which is written by professionals or scientists who are associated to Computer Science and Information Technology, or doing research study in these areas. If you are novel to this field then you can consult about this field from your supervisor or guide.

Techniques for writing a good quality Computer Science Research Paper:

1. Choosing the topic- In most cases, the topic is searched by the interest of author but it can be also suggested by the guides. You can have several topics and then you can judge that in which topic or subject you are finding yourself most comfortable. This can be done by asking several questions to yourself, like Will I be able to carry our search in this area? Will I find all necessary recourses to accomplish the search? Will I be able to find all information in this field area? If the answer of these types of questions will be "Yes" then you can choose that topic. In most of the cases, you may have to conduct the surveys and have to visit several places because this field is related to Computer Science and Information Technology. Also, you may have to do a lot of work to find all rise and falls regarding the various data of that subject. Sometimes, detailed information plays a vital role, instead of short information.

2. Evaluators are human: First thing to remember that evaluators are also human being. They are not only meant for rejecting a paper. They are here to evaluate your paper. So, present your Best.

3. Think Like Evaluators: If you are in a confusion or getting demotivated that your paper will be accepted by evaluators or not, then think and try to evaluate your paper like an Evaluator. Try to understand that what an evaluator wants in your research paper and automatically you will have your answer.

4. Make blueprints of paper: The outline is the plan or framework that will help you to arrange your thoughts. It will make your paper logical. But remember that all points of your outline must be related to the topic you have chosen.

5. Ask your Guides: If you are having any difficulty in your research, then do not hesitate to share your difficulty to your guide (if you have any). They will surely help you out and resolve your doubts. If you can't clarify what exactly you require for your work then ask the supervisor to help you with the alternative. He might also provide you the list of essential readings.

6. Use of computer is recommended: As you are doing research in the field of Computer Science, then this point is quite obvious.

7. Use right software: Always use good quality software packages. If you are not capable to judge good software then you can lose quality of your paper unknowingly. There are various software programs available to help you, which you can get through Internet.

8. Use the Internet for help: An excellent start for your paper can be by using the Google. It is an excellent search engine, where you can have your doubts resolved. You may also read some answers for the frequent question how to write my research paper or find model research paper. From the internet library you can download books. If you have all required books make important reading selecting and analyzing the specified information. Then put together research paper sketch out.

9. Use and get big pictures: Always use encyclopedias, Wikipedia to get pictures so that you can go into the depth.

10. Bookmarks are useful: When you read any book or magazine, you generally use bookmarks, right! It is a good habit, which helps to not to lose your continuity. You should always use bookmarks while searching on Internet also, which will make your search easier.

11. Revise what you wrote: When you write anything, always read it, summarize it and then finalize it.

12. Make all efforts: Make all efforts to mention what you are going to write in your paper. That means always have a good start. Try to mention everything in introduction, that what is the need of a particular research paper. Polish your work by good skill of writing and always give an evaluator, what he wants.

13. Have backups: When you are going to do any important thing like making research paper, you should always have backup copies of it either in your computer or in paper. This will help you to not to lose any of your important.

14. Produce good diagrams of your own: Always try to include good charts or diagrams in your paper to improve quality. Using several and unnecessary diagrams will degrade the quality of your paper by creating "hotchpotch." So always, try to make and include those diagrams, which are made by your own to improve readability and understandability of your paper.

15. Use of direct quotes: When you do research relevant to literature, history or current affairs then use of quotes become essential but if study is relevant to science then use of quotes is not preferable.

16. Use proper verb tense: Use proper verb tenses in your paper. Use past tense, to present those events that happened. Use present tense to indicate events that are going on. Use future tense to indicate future happening events. Use of improper and wrong tenses will confuse the evaluator. Avoid the sentences that are incomplete.

17. Never use online paper: If you are getting any paper on Internet, then never use it as your research paper because it might be possible that evaluator has already seen it or maybe it is outdated version.

18. **Pick a good study spot:** To do your research studies always try to pick a spot, which is quiet. Every spot is not for studies. Spot that suits you choose it and proceed further.

19. Know what you know: Always try to know, what you know by making objectives. Else, you will be confused and cannot achieve your target.

20. Use good quality grammar: Always use a good quality grammar and use words that will throw positive impact on evaluator. Use of good quality grammar does not mean to use tough words, that for each word the evaluator has to go through dictionary. Do not start sentence with a conjunction. Do not fragment sentences. Eliminate one-word sentences. Ignore passive voice. Do not ever use a big word when a diminutive one would suffice. Verbs have to be in agreement with their subjects. Prepositions are not expressions to finish sentences with. It is incorrect to ever divide an infinitive. Avoid clichés like the disease. Also, always shun irritating alliteration. Use language that is simple and straight forward. put together a neat summary.

21. Arrangement of information: Each section of the main body should start with an opening sentence and there should be a changeover at the end of the section. Give only valid and powerful arguments to your topic. You may also maintain your arguments with records.

22. Never start in last minute: Always start at right time and give enough time to research work. Leaving everything to the last minute will degrade your paper and spoil your work.

23. Multitasking in research is not good: Doing several things at the same time proves bad habit in case of research activity. Research is an area, where everything has a particular time slot. Divide your research work in parts and do particular part in particular time slot.

24. Never copy others' work: Never copy others' work and give it your name because if evaluator has seen it anywhere you will be in trouble.

25. Take proper rest and food: No matter how many hours you spend for your research activity, if you are not taking care of your health then all your efforts will be in vain. For a quality research, study is must, and this can be done by taking proper rest and food.

26. Go for seminars: Attend seminars if the topic is relevant to your research area. Utilize all your resources.

27. Refresh your mind after intervals: Try to give rest to your mind by listening to soft music or by sleeping in intervals. This will also improve your memory.

28. Make colleagues: Always try to make colleagues. No matter how sharper or intelligent you are, if you make colleagues you can have several ideas, which will be helpful for your research.

29. **Think technically:** Always think technically. If anything happens, then search its reasons, its benefits, and demerits.

30. Think and then print: When you will go to print your paper, notice that tables are not be split, headings are not detached from their descriptions, and page sequence is maintained.

31. Adding unnecessary information: Do not add unnecessary information, like, I have used MS Excel to draw graph. Do not add irrelevant and inappropriate material. These all will create superfluous. Foreign terminology and phrases are not apropos. One should NEVER take a broad view. Analogy in script is like feathers on a snake. Not at all use a large word when a very small one would be sufficient. Use words properly, regardless of how others use them. Remove quotations. Puns are for kids, not grunt readers. Amplification is a billion times of inferior quality than sarcasm.

32. Never oversimplify everything: To add material in your research paper, never go for oversimplification. This will definitely irritate the evaluator. Be more or less specific. Also too, by no means, ever use rhythmic redundancies. Contractions aren't essential and shouldn't be there used. Comparisons are as terrible as clichés. Give up ampersands and abbreviations, and so on. Remove commas, that are, not

necessary. Parenthetical words however should be together with this in commas. Understatement is all the time the complete best way to put onward earth-shaking thoughts. Give a detailed literary review.

33. Report concluded results: Use concluded results. From raw data, filter the results and then conclude your studies based on measurements and observations taken. Significant figures and appropriate number of decimal places should be used. Parenthetical remarks are prohibitive. Proofread carefully at final stage. In the end give outline to your arguments. Spot out perspectives of further study of this subject. Justify your conclusion by at the bottom of them with sufficient justifications and examples.

34. After conclusion: Once you have concluded your research, the next most important step is to present your findings. Presentation is extremely important as it is the definite medium though which your research is going to be in print to the rest of the crowd. Care should be taken to categorize your thoughts well and present them in a logical and neat manner. A good quality research paper format is essential because it serves to highlight your research paper and bring to light all necessary aspects in your research.

Informal Guidelines of Research Paper Writing

Key points to remember:

- Submit all work in its final form.
- Write your paper in the form, which is presented in the guidelines using the template.
- Please note the criterion for grading the final paper by peer-reviewers.

Final Points:

A purpose of organizing a research paper is to let people to interpret your effort selectively. The journal requires the following sections, submitted in the order listed, each section to start on a new page.

The introduction will be compiled from reference matter and will reflect the design processes or outline of basis that direct you to make study. As you will carry out the process of study, the method and process section will be constructed as like that. The result segment will show related statistics in nearly sequential order and will direct the reviewers next to the similar intellectual paths throughout the data that you took to carry out your study. The discussion section will provide understanding of the data and projections as to the implication of the results. The use of good quality references all through the paper will give the effort trustworthiness by representing an alertness of prior workings.

Writing a research paper is not an easy job no matter how trouble-free the actual research or concept. Practice, excellent preparation, and controlled record keeping are the only means to make straightforward the progression.

General style:

Specific editorial column necessities for compliance of a manuscript will always take over from directions in these general guidelines.

To make a paper clear

· Adhere to recommended page limits

Mistakes to evade

- Insertion a title at the foot of a page with the subsequent text on the next page
- Separating a table/chart or figure - impound each figure/table to a single page
- Submitting a manuscript with pages out of sequence

In every sections of your document

· Use standard writing style including articles ("a", "the," etc.)

· Keep on paying attention on the research topic of the paper

· Use paragraphs to split each significant point (excluding for the abstract)

· Align the primary line of each section

· Present your points in sound order

· Use present tense to report well accepted

· Use past tense to describe specific results

· Shun familiar wording, don't address the reviewer directly, and don't use slang, slang language, or superlatives

· Shun use of extra pictures - include only those figures essential to presenting results

Title Page:

Choose a revealing title. It should be short. It should not have non-standard acronyms or abbreviations. It should not exceed two printed lines. It should include the name(s) and address (es) of all authors.

Abstract:

The summary should be two hundred words or less. It should briefly and clearly explain the key findings reported in the manuscript--must have precise statistics. It should not have abnormal acronyms or abbreviations. It should be logical in itself. Shun citing references at this point.

An abstract is a brief distinct paragraph summary of finished work or work in development. In a minute or less a reviewer can be taught the foundation behind the study, common approach to the problem, relevant results, and significant conclusions or new questions.

Write your summary when your paper is completed because how can you write the summary of anything which is not yet written? Wealth of terminology is very essential in abstract. Yet, use comprehensive sentences and do not let go readability for briefness. You can maintain it succinct by phrasing sentences so that they provide more than lone rationale. The author can at this moment go straight to shortening the outcome. Sum up the study, with the subsequent elements in any summary. Try to maintain the initial two items to no more than one ruling each.

- Reason of the study - theory, overall issue, purpose
- Fundamental goal
- To the point depiction of the research
- Consequences, including definite statistics - if the consequences are quantitative in nature, account quantitative data; results of any numerical analysis should be reported
- Significant conclusions or questions that track from the research(es)

Approach:

- Single section, and succinct
- As a outline of job done, it is always written in past tense
- A conceptual should situate on its own, and not submit to any other part of the paper such as a form or table

- Center on shortening results - bound background information to a verdict or two, if completely necessary
- What you account in an conceptual must be regular with what you reported in the manuscript
- Exact spelling, clearness of sentences and phrases, and appropriate reporting of quantities (proper units, important statistics) are just as significant in an abstract as they are anywhere else

Introduction:

The **Introduction** should "introduce" the manuscript. The reviewer should be presented with sufficient background information to be capable to comprehend and calculate the purpose of your study without having to submit to other works. The basis for the study should be offered. Give most important references but shun difficult to make a comprehensive appraisal of the topic. In the introduction, describe the problem visibly. If the problem is not acknowledged in a logical, reasonable way, the reviewer will have no attention in your result. Speak in common terms about techniques used to explain the problem, if needed, but do not present any particulars about the protocols here. Following approach can create a valuable beginning:

- Explain the value (significance) of the study
- Shield the model - why did you employ this particular system or method? What is its compensation? You strength remark on its appropriateness from a abstract point of vision as well as point out sensible reasons for using it.
- Present a justification. Status your particular theory (es) or aim(s), and describe the logic that led you to choose them.
- Very for a short time explain the tentative propose and how it skilled the declared objectives.

Approach:

- Use past tense except for when referring to recognized facts. After all, the manuscript will be submitted after the entire job is done.
- Sort out your thoughts; manufacture one key point with every section. If you make the four points listed above, you will need a least of four paragraphs.
- Present surroundings information only as desirable in order hold up a situation. The reviewer does not desire to read the whole thing you know about a topic.
- Shape the theory/purpose specifically - do not take a broad view.
- As always, give awareness to spelling, simplicity and correctness of sentences and phrases.

Procedures (Methods and Materials):

This part is supposed to be the easiest to carve if you have good skills. A sound written Procedures segment allows a capable scientist to replacement your results. Present precise information about your supplies. The suppliers and clarity of reagents can be helpful bits of information. Present methods in sequential order but linked methodologies can be grouped as a segment. Be concise when relating the protocols. Attempt for the least amount of information that would permit another capable scientist to spare your outcome but be cautious that vital information is integrated. The use of subheadings is suggested and ought to be synchronized with the results section. When a technique is used that has been well described in another object, mention the specific item describing a way but draw the basic principle while stating the situation. The purpose is to text all particular resources and broad procedures, so that another person may use some or all of the methods in one more study or referee the scientific value of your work. It is not to be a step by step report of the whole thing you did, nor is a methods section a set of orders.

Materials:

- Explain materials individually only if the study is so complex that it saves liberty this way.
- Embrace particular materials, and any tools or provisions that are not frequently found in laboratories.
- Do not take in frequently found.
- If use of a definite type of tools.
- Materials may be reported in a part section or else they may be recognized along with your measures.

Methods:

- Report the method (not particulars of each process that engaged the same methodology)

- Describe the method entirely
- To be succinct, present methods under headings dedicated to specific dealings or groups of measures
- Simplify - details how procedures were completed not how they were exclusively performed on a particular day.
- If well known procedures were used, account the procedure by name, possibly with reference, and that's all.

Approach:

- It is embarrassed or not possible to use vigorous voice when documenting methods with no using first person, which would focus the reviewer's interest on the researcher rather than the job. As a result when script up the methods most authors use third person passive voice.
- Use standard style in this and in every other part of the paper - avoid familiar lists, and use full sentences.

What to keep away from

- Resources and methods are not a set of information.
- Skip all descriptive information and surroundings - save it for the argument.
- Leave out information that is immaterial to a third party.

Results:

The principle of a results segment is to present and demonstrate your conclusion. Create this part a entirely objective details of the outcome, and save all understanding for the discussion.

The page length of this segment is set by the sum and types of data to be reported. Carry on to be to the point, by means of statistics and tables, if suitable, to present consequences most efficiently.

You must obviously differentiate material that would usually be incorporated in a study editorial from any unprocessed data or additional appendix matter that would not be available. In fact, such matter should not be submitted at all except requested by the instructor.
Content

- Sum up your conclusion in text and demonstrate them, if suitable, with figures and tables.
- In manuscript, explain each of your consequences, point the reader to remarks that are most appropriate.
- Present a background, such as by describing the question that was addressed by creation an exacting study.
- Explain results of control experiments and comprise remarks that are not accessible in a prescribed figure or table, if appropriate.
- Examine your data, then prepare the analyzed (transformed) data in the form of a figure (graph), table, or in manuscript form.

What to stay away from

- Do not discuss or infer your outcome, report surroundings information, or try to explain anything.
- Not at all, take in raw data or intermediate calculations in a research manuscript.
- Do not present the similar data more than once.
- Manuscript should complement any figures or tables, not duplicate the identical information.
- Never confuse figures with tables - there is a difference.

Approach

- As forever, use past tense when you submit to your results, and put the whole thing in a reasonable order.
- Put figures and tables, appropriately numbered, in order at the end of the report
- If you desire, you may place your figures and tables properly within the text of your results part.

Figures and tables

- If you put figures and tables at the end of the details, make certain that they are visibly distinguished from any attach appendix materials, such as raw facts
- Despite of position, each figure must be numbered one after the other and complete with subtitle
- In spite of position, each table must be titled, numbered one after the other and complete with heading
- All figure and table must be adequately complete that it could situate on its own, divide from text

Discussion:

The Discussion is expected the trickiest segment to write and describe. A lot of papers submitted for journal are discarded based on problems with the Discussion. There is no head of state for how long a argument should be. Position your understanding of the outcome visibly to lead the reviewer through your conclusions, and then finish the paper with a summing up of the implication of the study. The purpose here is to offer an understanding of your results and hold up for all of your conclusions, using facts from your research and generally accepted information, if suitable. The implication of result should be visibly described.
Infer your data in the conversation in suitable depth. This means that when you clarify an observable fact you must explain mechanisms that may account for the observation. If your results vary from your prospect, make clear why that may have happened. If your results agree, then explain the theory that the proof supported. It is never suitable to just state that the data approved with prospect, and let it drop at that.

- Make a decision if each premise is supported, discarded, or if you cannot make a conclusion with assurance. Do not just dismiss a study or part of a study as "uncertain."
- Research papers are not acknowledged if the work is imperfect. Draw what conclusions you can based upon the results that you have, and take care of the study as a finished work
- You may propose future guidelines, such as how the experiment might be personalized to accomplish a new idea.
- Give details all of your remarks as much as possible, focus on mechanisms.
- Make a decision if the tentative design sufficiently addressed the theory, and whether or not it was correctly restricted.
- Try to present substitute explanations if sensible alternatives be present.
- One research will not counter an overall question, so maintain the large picture in mind, where do you go next? The best studies unlock new avenues of study. What questions remain?
- Recommendations for detailed papers will offer supplementary suggestions.

Approach:

- When you refer to information, differentiate data generated by your own studies from available information
- Submit to work done by specific persons (including you) in past tense.
- Submit to generally acknowledged facts and main beliefs in present tense.

Administration Rules Listed Before Submitting Your Research Paper to Global Journals

Please carefully note down following rules and regulation before submitting your Research Paper to Global Journals:

Segment Draft and Final Research Paper: You have to strictly follow the template of research paper. If it is not done your paper may get rejected.

- The **major constraint** is that you must independently make all content, tables, graphs, and facts that are offered in the paper. You must write each part of the paper wholly on your own. The Peer-reviewers need to identify your own perceptive of the concepts in your own terms. NEVER extract straight from any foundation, and never rephrase someone else's analysis.
- Do not give permission to anyone else to "PROOFREAD" your manuscript.

- Methods to avoid Plagiarism is applied by us on every paper, if found guilty, you will be blacklisted by all of our collaborated research groups, your institution will be informed for this and strict legal actions will be taken immediately.)
- To guard yourself and others from possible illegal use please do not permit anyone right to use to your paper and files.

Criterion for Grading a Research Paper (Compilation) by Global Journals

Please note that following table is only a Grading of "Paper Compilation" and not on "Performed/Stated Research" whose grading solely depends on Individual Assigned Peer Reviewer and Editorial Board Member. These can be available only on request and after decision of Paper. This report will be the property of Global Journals.

Topics	Grades		
	A-B	C-D	E-F
Abstract	Clear and concise with appropriate content, Correct format. 200 words or below	Unclear summary and no specific data, Incorrect form Above 200 words	No specific data with ambiguous information Above 250 words
Introduction	Containing all background details with clear goal and appropriate details, flow specification, no grammar and spelling mistake, well organized sentence and paragraph, reference cited	Unclear and confusing data, appropriate format, grammar and spelling errors with unorganized matter	Out of place depth and content, hazy format
Methods and Procedures	Clear and to the point with well arranged paragraph, precision and accuracy of facts and figures, well organized subheads	Difficult to comprehend with embarrassed text, too much explanation but completed	Incorrect and unorganized structure with hazy meaning
Result	Well organized, Clear and specific, Correct units with precision, correct data, well structuring of paragraph, no grammar and spelling mistake	Complete and embarrassed text, difficult to comprehend	Irregular format with wrong facts and figures
Discussion	Well organized, meaningful specification, sound conclusion, logical and concise explanation, highly structured paragraph reference cited	Wordy, unclear conclusion, spurious	Conclusion is not cited, unorganized, difficult to comprehend
References	Complete and correct format, well organized	Beside the point, Incomplete	Wrong format and structuring

Index

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

Global Journal of Computer Science and Technology

Visit us on the Web at www.GlobalJournals.org | www.ComputerResearch.org
or email us at helpdesk@globaljournals.org

ISSN 9754350