Online ISSN : 0975-4172
Print ISSN : 0975-4350

Global Journal of Computer Science and Technology : E

Network, Web & Security

DISCOVERING THOUGHTS AND INVENTING FUTURE

HIGHLIGHTS

- Gait Recognition Approaches
- Stable Routing Protocol
- Wireless Sensor Networks
- QoS-Aware Web Service

Computer Server Farm

Volume 12 | Issue 10 | Version 1.0 ENG

Global Journal of Computer Science and Technology: E
Network, Web & Security

Global Journal of Computer Science and Technology: E
Network, Web & Security

Volume 12 Issue 10 (Ver. 1.0)

Open Association of Research Society

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 Association of Research, Marsh Road, Rainham, Essex, London RM13 8EU United Kingdom.

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) & 250 USD (Color)

Editorial Board Members (HON.)

Dr. Bart Lambrecht
Director of Research in Accounting and FinanceProfessor 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 SchoolPh.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 NeuroscienceNorthwestern University
Feinberg School of Medicine

Dr. Pina C. Sanelli
Associate Professor of Public Health
Weill Cornell Medical College
Associate Attending Radiologist
NewYork-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, TaiwanUniversity 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

Contents of the Volume

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 12 Issue 10 Version 1.0 May 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Bayesiane Filter for Detecting a Spam

By Elma Zanaj & Bledi Shkurti

Faculty of Information Technology Polytechnic University of Tirana Tirana, Albania

Abstract - The detected of spam messages in terms that better having a spam email in the inbox than a ham message in the junk, has been investigated recently. The main contribution of the paper consists in comparing three antispam filters used more nowadays, and will find that which is filter is of the future. By using filters we will also create some patterns as the result of training with different number of emails. Simulations show that due to the trainging of the filters it will be easier to detect the spams.

Keywords : *filter; Bayesian; spam; ham.*

GJCST-E Classification: *H.3.3*

Strictly as per the compliance and regulations of:

Bayesiane Filter for Detecting a Spam

Elma Zanaj [α] & Bledi Shkurti [σ]

Abstract - The detected of spam messages in terms that better having a spam email in the inbox than a ham message in the junk, has been investigated recently. The main contribution of the paper consists in comparing three antispam filters used more nowadays, and will find that which is filter is of the future. By using filters we will also create some patterns as the result of training with different number of emails. Simulations show that due to the trainging of the filters it will be easier to detect the spams.

Keywords : filter; Bayesian; spam; ham.

I. Introduction

Spam emails or otherwise UCE (Unsolicited Commercial E-mail) have no exact definition. Most spam emails can be considered as undesirable but not all unwanted emails are spam [1]. A different name may be unwanted commercial emails, but unfortunately there are just spam advertising messages. Fig.1 shows the set of all email messages and the place that spam occupy.

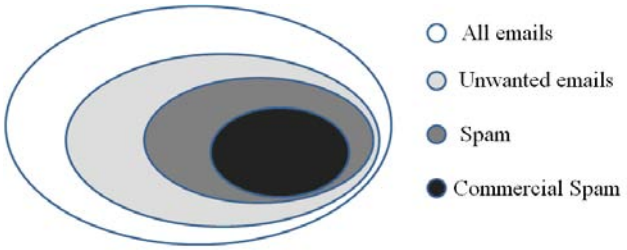


Figure 1: The set of spam e-mails compared with other e-mails

In the email context, the term spam refers to the electronic equivalent of junk email: a set of unwanted messages. Many definitions present spam as messages sent to many people without the consent of recipients. UBE (Unsolicited Bulk Email) are messages sent to many addresses without their request and approval. Examples of UBE are political or religious emails, hate messages for different groups or fraud on the Internet. UBE includes UCE, and then commercial messages sent to many persons can be considered UBE and UCE. While we refer to messages that are not spam as "not spam" or "legitimate messages", a fitting name could be "ham".

The history of spam can be divided into three different parts:

- The early spam letters addressed and sent manually
- The sender that use machines, which led to a dramatic increase in the number of spam
- The last part is when "machine learning" came for filtering spam and made filtering more effective.

The use of Bayesian networks, does filtering not only more effective, but it also learns the characteristics of the message received. Even if spam senders do a lot of new tricks, Bayesian filters have good chances to filter them. Fig.2 shows the results of the questionnaire issued by the spam to a user group [2].Statistics in December of 2010 show that 33% of Internet users do not like spam and 52% of them not only dislike but are frustrated of them, while only 15% of users do not have those problems. It is worth noting that 85% of users have problems with spam.

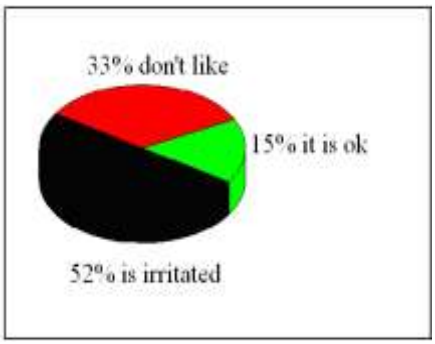


Figure 2 : The opinion of the users for spam emails Irritated

If a company has no filter and the employees receive 6 spam messages per day, it must require at average 5 seconds reading and deleting each spam message, which means that the worker will spend 3 hours a year to read and delete spam. These estimates are prudent and do not take into account the time required for discussing the spam and their differences, or the contacting of the specialists for other problems caused by spam.

This paper will present a study, on the basis of which a filter can be selected, so less spams can be in our inbox.

The remainder of the paper is organized as follows. In Section 2, are presented some statistics and fact about the spam. Section 3 outlines some methods of fighting the spams, while Section 4 describes the three filters that we are going to use.Our simulation results are presented in Section 5, and the Conclusions concludes the paper.

Author α : Faculty of Information Technology Polytechnic University of Tirana Tirana, Albania. E-mail : ezanaj@fti.edu.al
Author σ : Faculty of Information Technology Polytechnic Univeristy of Tirana Tirana, Albania. E-mail : bledi.shkurti@fti.edu.al

II. Statistics and Facts About Spam

Today are counted 14.5 billion spam per day distributed in whole world [3]. We can say that spam are 45% of all emails. In fact some companies have estimated that spam occupy a high percentage of all global email communications, such as 73%. United States of America are the first to send spam, with the largest number, followed by Korea comes as second distributor of unwanted messages. Most used type of spam is online advertising, which occupy 36% of all spam. The second largest are links to adult which constitute 31.7% of all spam. Unwanted emails relating to financial matters occupy third place with 26.5% of spam. In fact, observations indicate that spam has reduced public confidence towards online communications. More people have completely lost confidence in Internet communications because of spam.

Companies look at spam as a problem that reduces productivity and safety. About 52% of the interviewed companies rated the fight against spam as most needed and as the most important. Regarding a study done by "Radicati Research Group", a research company in California, spam cost to the business 20.5 billion $ annually in the reduction of productivity and technical expenses. Another study says that the average annual loss for an employee is approximately 1934$. Future forecast for the costs of spam are not very good, it is provided that 58 billion spam emails will be sent every day and that within the next 8 years, that overdrafts will cost to the businesses 198 billion $ every day. The number of spam emails depends on frequency of use of email. For example, if someone receives 10 emails every week, and has only a spam, then to him is simple and easy to delete unwanted email than to implement a filter for his emails. Spam usually causes problems for users who receive hundreds of emails a week, for who is really annoying to delete hundreds of spam emails every week. One of the characteristics and trends can be the language [4]. Most of the spams are written in English. Another characteristic is their hour of delivery. The time when a spam is sent, is during working hours in the United States of America. In the area of Washington DC, New York obtained an average of 50% spam over time 8 am to 2 pm, that in other times of the day. All these statistics can serve as a basis for solutions antispam filters. Spam are: advertising, finance, Phinishing.

III. Simple Methods to Fight Spam

Some very simple methods are discovered during the evolution of spam filters. These are ideal to combine with more complex filters. Greater efficiency can be achieved by using small pieces together of these filtration methods:

1) *The key words*. The first chooice is to look for key words in the message subject.
2) *Black list*. It is necessary to make the difference between the two levels of the black list: the black list of network-level and black list at the address.
3) *White List*. These are the opposite of black lists. Content filtering identifies spam, and white lists require the identification of users. A white list is a safe community contacts (not dangerous to send spam).

If the method of the black list and white list are used together, would necessitate a different filtering to find addresses that are not in any of the lists referred above.

4) *Throttling.* Throttling only slows down the speed at which a network or a machine can send traffic. In fact this is the most effective ways to fight spam.
5) *Filtering in cooperation.* This will allow individuals to communicate in reliable groups for infected messages with other group members.
6) *Network filtering*. Protocol Simple Mail Transfer Protocol (SMTP) is the way that email servers communicate. This protocol was designed to function independently and to ensure the privacy of Internet users. Senders of spam have benefited from this protocol of servers to send spam emails anonymously. In fact, authenticated SMTP thought to be an answer to spam, but was seen to be necessary only to identify legitimate email senders. Authenticated SMTP requires to the users to give their password before sending email. Many spam-sending today build their email servers and keep in non specious networks to send their emails and passing the required authentication during delivery [1]. SMTP provides several other opportunities for later use.
7) *Fake Worker.* The main idea of this solution is to create a fake email address will be used to set "traps" . This can be used especially with names of companies (eg.: xyz@company.com) [5].
8) *Project Honey Pot.* Project Honey Pot is the first system capable to identify the senders of spam and robot programs, which are used to gather email addresses from web sites [6]. To participate in the project Honey Pot, web page builders must install the program on the server where the page is held. The rest is managed automatically.
9) *SPF (Sender Policy Framework)* [7]. The issue is the falsification of address of the sender. Falsification of the address of the sender is a problem for simple users or companies. It even reduces the trust in email communications because it reduces user's confidentiality and their trust.

To filter a spam, it starts with getting the email that is addressed to a particular receiver. The message is sent to antispam filter that classifies mail as spam or non-spam by using several methods. If the filter is classified ham (legitimate email) it is sent to the directory

ham message (inbox) in which the user receives his emails. Filters should be able to continuously update. Filters updating strategies are as diverse as filtration methods. The updates are two types: manual and self-learning (training). A manual update involves a person changing the filter parameters. In updating self-learning (training), the filter will find in the contents of the mail, the pieces that show for a spam or non-spam emails, from emails that are previously classified. The time that the filter can be updated, is every month or may be more often (after every new email). Online updating, the messages are processed and classified one after another. Before processing the next message, the filter can be adopted based on information received, and this is called training. When a filter is trained by more than one message at the same time, this process is called multiple training.

Classification of spam is based on Bayes theorem that establishes the link between conditional propabilities of two events [9]. Bayes theorem provides a way to calculate the probability of the hypothesis, when the event Y takes the training data, which appear with X:

$$P(Y/X) = P(X|Y) * P(X)/P(Y) \quad (1)$$

This theorem is the basis of statistics Bayesiane, which compute the probability of a new event based on other propabilities calculated before. When we test a new email message the starting point is a null hypothesis: "the message is spam", the alternative hypothesis is: "the message is not spam" [9].To classify a message as spam, is created the frequency distribution of their components and is compared with previous records of training (the corpus of spam) with a statistical test. Statistical tests will provide a probability value p, and if it is lower than a significance level, the null hypothesis is discarded and is verified that the message is not spam. Otherwise the null hypothesis is accepted. The probability of the Bayesiane statistics of a model based on data is calculated differently from classical statistics that estimate the probability of data by providing a hypothesis [8]. Bayesian classifier calculates the probability that a message is spam.

IV. The Choice of Antispam Filter

In our experiment we will compare antispam filters used more nowadays, and will find that which is filter is of the future. By using filters we will also create some patterns as the result of training with different number of emails. For all antispam solutions that use Bayesian network, we must first train the filters. To compare the filters is important not only to find a way for training, but that all filters must be trained in the same manner and with the same email messages. So the emails used can be classified before.

During the training process, the values of the particles differ in particle vocabulary of the filter, to obtain a high accuracy. This makes spam messages known from filters.

We should note that the training process does not end after the conclusion of training, it continues during the filter testing. Moreover, the filter becomes more personalized and closer to our needs during its use. For testing and comparison purposes we will use some programs that are convenient. Having met the requirements of users, we will compare the programs that are free. Although there are many different filters, because of limits for testing, we will compare three of them that are used more nowadays. The filters are:

1) *SpamAssassin,* an open source program and the most famous and widely used [9]. It is among the most effective filters, especially when used with databases of spams. SpamAssassin is a spam filter based on a set of rules to identify spams. Each rule checks the emails to assess whether it is spam or not. When all rules are applied, the amount is compared with the threshold set by the user. A number greater or equal to the limit means that the message is spam, and a smaller number than the threshold indicates that email is ham. First to make the classification of spam or ham, we have to train SpamAssassin filter. So the filter known the characteristices of the messages and creates a decision database, which will be used in the testing phase. So we have to train regularly with new messages to keep updated with messaging characteristices. We must train with the spam and ham messages. Training only with one category will enable the filter to recognize messages. To make a good training, it is recommended to use 1000 ham and 1000 spam messages, if it is possible. From the tests performed till now, the training with more than 5000 messages does not make a difference to accuracy.
2) *Mozilla Thunderbird.* The second program that we will use is Mozilla Thundebord. Mozilla's products have filter very well implemented and designed [10]. The filter has an automatic opportunity to be trained, and learns quickly from training, giving positive results in many everyday situations. Thunderbird included a Bayesian filter, a white list and may make classifications effectively as a filter SpamAssassin on a server.
3) *SpamProbe*. The third program is SpamProbe, another open source filter, which is a statistical spam filter [11]. It have rules created by users, and is based on Bayesian analysis of the frequency of the words in spam or ham emails taken by a user.

All Bayesian filters seek to train which can be done in several ways. Three main training methods are shown below: a) training with all, is the training when: all

the particles will be registrated to the database and their values will be updated after each recived email. This solution provides the ability to adapt to frequent changes in the characteristics of email, but it requires considerably resources (processing power) for each email that gets to manage all the particles and change their values.

b) training when there are errors: this refers to the idea that the frequent change of values can lead to more errors (incorrect values). In this case the values of the particle in the database are modified only if there is a reaction by the user. So the user controls whether the classification was correct or not. If the classification is incorrect, the user makes changes manually by placing email into the appropriate directory (inbox or spam). This requires less memory compared with the first mode of training. Negative aspects of this method are the difficulties in adopting with the new features of emails. For example, a new kind of spam may require more time until it is classified correctly.

c) training till to maturity: this solution is obtained by merging the two methods above. Initially pursued the idea of "training to all" and till are obtained a sufficient knowledge, passed on "training where no errors", so the changes happen only when errors occur. This combination of methods provides the advantages of both solutions; the only problem is the determining when the filter has received enough knowledge to move to another method.

V. Simulation Results

In our simulations is used the way "training to all". Note here the training is done after each email, but in everyday use, this is done once a day, not to consume the processing power of machines. For a simple user, daily training do not brings any greater advantage, but at the company level it can be very important.

To compare the filters, the most useful training is 30 to 70 which means that the filter is trained with 70% of all received email (70% of all email messages contain different messages spam or ham). The filter uses "knowledge" obtained from the training phase to determine whether an email is spam or legitimate.

After every processed mail the filter generates a binary result. In our case 1 means that the message is categorized as spam and 0 means it is classified as legitimate. This result is a binary vector which will be compared with results of other filters and also with the original classification.

The results were above our forecast, and the filtrate reacted very well during testing, and this was as the result of a large number of emails that were used for training. The efficiency of filters was above our forecasts for the entire group of emails, so it was reasonable to create models with different training. This brought the idea of training with 40% of all messages. In this case the testing is done with 30% of the messages, which are from the training group and the same for all filters.

This experiment aims to compare the filter with different training. For example, the message No. 1 was tested with trained Spam Assassin with 70% of messages; message No. 1 was also tested Spam Assassin filter that was trained with 40% of all messages. One should note that by switching to the filter with 40% training, the database of 70% model is deleted, and then the filter has other knowledge.

So in this experiment not only filters are compared with each other, but the same filter with different training. However the results were similar with acceptable accuracy.

In the end we trained the filter with 10% of messages. Although we had little training messages, the difference between models is small.

Filter Thunderbird will be test without doing the training. This program has knowledge of the daily use. The main reason of this test is to evaluate the ability of the program without doing the training and to have information on the accuracy of filters that are trained by daily use. As we shall see later, a trained filter with messages to a user for 6 months (although most of the messages are written in Albanian) will have the accuracy of a trained filter manually. Remember that personal messages of 6 months are sent at the thunderbird filter and are made their manual classification. So this serves as training for the filter, but are not used messages that have trained other filters.

Filters are shown in Table 1 and the models are compared with each other. Mark "X" indicates that the testing is done for the respective model.

Table 1: Training Sequences for Each Filter

	70% training	40% training	10% training	0% training
SpamAssassin	X	X	X	
SpamProbe	X	X		
Thunderbird	X			X

Training and testing time should not remain outside our attention because it is very important when filters will be used for large companies with more email traffic. Also is important the training time versus the time of testing. In everyday uses we are not able to measure the training time, so we can see only the testing times. The time it takes for each program is shown in Table 2. Our tests are done on a computer with processor frequency (CPU) 1.2GHz and 1GB of RAM memory.

Table 2 : Different Training for the Testing

	70% training	30% training
SpamAssassin	5 min	12 min
SpamProbe	3 min	7 min
Thunderbird	0 min	15 min

Table 2 show that the filter SpamProbe is fastest on both stages.The second is SpamAssassin, which for the two different training requires approximately double of the time than in the first case. The slowest seems Thunderbird, which requires double the time that SpamProbe.

To analyze the statistical is used the margin of error. The number of errors is divided by the number of all messages tested. The error rate can be called failure rate. On the degree error is taken into account only the number of errors occurring. As expected more spam messages are allowed than legitimate emails filtered. This refers to the principle that better to have spam in the inbox, rather than to go legitimate messages to the directory spam, which in many cases we do not control at all, and so may lose forever these messages.

Thunderbird filter is used for 6 months no training is done with training emails, it results are poor. This was somewhat expected because the program was used with Albanian language messages, while messages for the testing are in English. However, after training the results are comparable with other filters. Spam that can pass without being filtered are called "false negative", while legitimate messages that are filtered are called "false positive". Remember that there are 603 messages used for testing, of these 413 are legitimate messages and 190 are spam messages. So we know the original classification of messages.

All three filters have a tendency to increase the accuracy with increased training. So the graphics being to decrease from left to right. So it is expected that for the Bayesian filters as much training to do the greater is the accuracy. Spam Assassin filter has a balanced result, so that not necessarily with more training brings greater precision. It is important to emphasize that Spam Probe gives us the best result and is the only filter with precision greater than 90%.

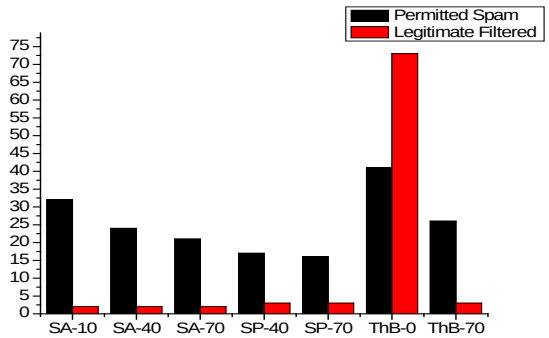


Figure 3 : The number of error from 603 messages

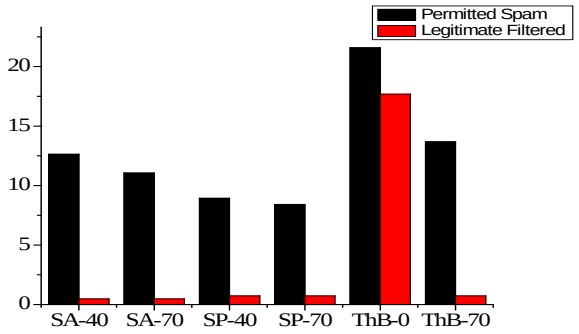


Figure 4: The error rate

Thunderbird has an intermediate result between the filters, but it is the simplest to use, because it serves even as a program to manage emails. Thunderbird which was not training, gave us a very poor result, but it will not take much into account, because to compare the filters should be put on equal terms.

VI. Conclusions

The conclusions are that all three filters have advantages and disadvantages. Cannot conclude what is the best filter. A brief summary is presented in Table 3. As can be seen, it is not clear which filter to choose, or which one is the best. There are several points of view to be taken into account.

Table 3 : Conclusions for the Filters

Filters	advantages	Disadvantages
SpamAssassin	Good ability to training	Poor results with little training emails
SpamProbe	Good results with little training emails	More training does not lead to increased accuracy
Thunderbird	Easy to use	Requires more time

However, it may be a prediction that filtering with only one program does not yield results that will receive the filter with more programs. In fact for future work can be considered the union of two filters with one another to achieve greater precision.

References Références Referencias

1. Jonathan A. Zdziarski, “Ending Spam - Bayesian Content Filtering and the Art of Statistical Language Classification” No Starch Press, Jul 5, 2005.
2. SpamCop statistics, http://www.spamcop.net/spamstats.shtml
3. Spam statistics and facts http://www.spamlaws.com/spam-stats.html
4. Sophos: still far from death as spam http://www.sg.hu/cikkek/41288/sophos_messze_meg_a_spam_halala

5. Aaron E. Kornblum “SMTP Path Analysis – Exposing Zombie Spammers”, in CEAS 2005.
6. Project “honey pot”, http://www.projecthoney pot.org/
7. SPF http://www.openspf.org/
8. Jon Kågström “Impoving naïve Bayesian spam filtering”, Master Thesis, 2005.
9. SpamAssassin, http://spamassassin.apache.org/
10. Mozilla Thunderbird, http://www.mozilla.com/ thunderbird/
11. SpamProbe, http://spamprobe.sourceforge.net/

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 12 Issue 10 Version 1.0 May 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

A Survey of Gait Recognition Approaches Using PCA & ICA

By M.Pushparani & D.Sasikala
Mother Teresa Women's University, Kodaikanal, India

Abstract - Human identification by gait has created a great deal of interest in computer vision community due to its advantage of inconspicuous recognition at a relatively far distance. Biometric systems are becoming increasingly important, since they provide more reliable and efficient means of identity verification. Biometric gait Analysis (i.e. recognizing people from the way they walk) is one of the recent attractive topics in biometric research. It has been receiving wide attention in the area of Biometric. In Gait biometric research there are various gait recognition approaches are available. In this paper, the gait recognition approaches such as "Wavelet Descriptor with ICA", and "Hough transform with PCA" are compared and discussed.

Keywords : *Biometrics, Survey, Gait Recognition approaches.*

GJCST Classification: *D.4.6*

Strictly as per the compliance and regulations of:

A Survey of Gait Recognition Approaches Using PCA & ICA

M.Pushparani [α] & D.Sasikala [σ]

Abstract - Human identification by gait has created a great deal of interest in computer vision community due to its advantage of inconspicuous recognition at a relatively far distance. Biometric systems are becoming increasingly important, since they provide more reliable and efficient means of identity verification. Biometric gait Analysis (i.e. recognizing people from the way they walk) is one of the recent attractive topics in biometric research. It has been receiving wide attention in the area of Biometric. In Gait biometric research there are various gait recognition approaches are available. In this paper, the gait recognition approaches such as "Wavelet Descriptor with ICA", and "Hough transform with PCA" are compared and discussed.

Keywords : Biometrics, Survey, Gait Recognition approaches.

I. Introduction

The first and foremost important steps towards preventing unauthorized access are user authentication. User authentication is the process of verifying identity. Biometric authentication is based on something one's physiological and behavioral characteristics. In traditional approaches, passwords and tokens were used and it can be forgotten, lost or stolen. There is also usability limitations associated with them. Recently, biometric is attracting more and more attentions. Generally, biometric is a field of technology that uses automated methods for identifying or verifying a person based on a physiological or behavioral trait.[1] These traits are always measured in different systems are the face, fingerprints, palm print, handwriting, iris, gait, and voice etc. Among them, gait recognition, as a relatively new biometric technique, aims to recognize individuals by the way they walk. The advantages of gait recognition are that it can be applied inconspicuously and it offers an ability to recognize at a distance or at low resolution.

II. Related Work

The Gait recognition approaches for human identification plays an important role in many applications especially in security systems. The first gait recognition approach was developed by Niyogi and Adelson on a small gait database in 1994 [2]. Consequently, the HumanID program sponsored by Defense Advanced Research Projects Agency (DARPA) [3] assists greatly in advancing automatic gait recognition. Spurred by the HumanID program, many international famous universities and research institutes, such as the University of Southampton, the Massachusetts Institute of Technology (MIT), Carnegie Mellon University (CMU), Institute of Automation Chinese Academy of Sciences, etc, have made a lot of researches on gait recognition. There are various approaches available for gait recognition which can be divided into two broad categories such as Model based and Model free approaches. Zhang et al. [4] proposed a novel two-step, model-based approach to recognize gait by employing a five-link biped locomotion human model. . Meyer et al. [5] extracted and tracked the contours of different parts of the human body. Lee et al. [6] fitted seven ellipses in the human body area, and used their locations, orientations, and aspect ratios as features to represent the gait. In general, the features used in model-based approaches are insensitive to background cluttering and noise. Model based approaches has high computational complexity and more difficult in low resolution images. However, Model-based approaches are somewhat difficult in real environment because feature extraction process and matching is very difficult. The Model-free approaches are well suitable for real time systems because it is easy to extract the feature and computational complexity is low.

III. Techniques Used

a) Wavelet Descriptors with ICA for Feature Extraction

In this approach, the automatic Gait recognition has been accomplished based on wavelet descriptors and independent component analysis (ICA) for the purpose of human identification at a distance. The background extraction method is applied to subtract the moving human figures accurately and to obtain binary silhouettes. The binary silhouettes are described with wavelet descriptors and convert it into ID signals to get Independent Components (ICs) of these signals using ICA. The fixing point algorithm is used for calculating the Independent Component adoption and selection. Finally using Nearest Neighbor and SVM classifiers are used for recognition.

Author α : Dr. M. Pushpa Rani, Professor & Head, Dept. of Computer Science, Mother Teresa Women's University, Kodaikanal, India.
E-mail : pushpa_john@yahoo.com
Author σ : Mrs.D.Sasikala, Research Scholar, M.Phil(CS), Mother Teresa Women's University, Kodaikanal, India.
E-mail : ashwathiram.sasi@yahoo.com

Fig.1: Example of gait image preprocessing [7]

a. Original Image b. Background subtraction

c. Image after d. Last edge

b) Shadow Elimination

Wavelet descriptors are used to describe human silhouettes $d_i = \sqrt{(x_i - x_c)^2 + (y_i - y_c)^2}$ where (x_c, y_c) is the centroid of human boundary.

a. original boundary b. boundary with wavelet descriptor

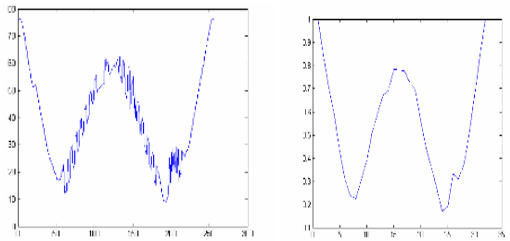


Fig. 2 : Feature representation using wavelet descriptor

Then, the feature extraction and training gait using ICA is done. Using Wavelet descriptors the required variables obtained. Finally the classification process is done using Nearest Neighbor and SVM classifiers. To evaluate the discriminatory of two gait sequences Euclidean distance is applied. There are several kernel functions used in SVM, here radial basis function (RBF) is adopted.

IV. Hough Transform and PCA

a) Hough Transform for Feature Extraction

For efficient gait recognition, the information of straight lines in gait silhouettes is very important. In spatio-temporal gait representation based on the Hough transform contains more straight lines information, and is more insensitive to image noise. Hough Transform is a feature extraction technique which was proposed by Paul Hough who patented the method in 1962. This technique can be used to isolate features of a particular shape within an image [8]. Using some mathematical functions, it is possible to find imperfect instances of objects to describe the boundary curves. Since its computational complexity, Hough Transform is normally restricted to first and second order equation. Commonly, the classical Hough Transform is used for the detection of regular curves such as lines, circles, and ellipses, etc.

PCA

Principal component analysis (PCA) is a mathematical procedure that uses an orthogonal transformation to convert a set of observations of possibly correlated variables into a set of values of linearly uncorrelated variables called principal components.[9] Principal Component Analysis (PCA) is widely utilized to reduce the dimensionality of the data. The goal of PCA is to reduce the dimensionality of the data while retaining as much as possible of the variation present in the original dataset. PCA allows us to compute a linear transformation that maps data from a high dimensional space to a lower dimensional space. Based on these two methods the gait recognition approach was generated. In this approach, initially the preprocessing works were done as follows. First, the image sequences were aligned using some mathematical approaches. It is used to resize the various sizes of images into same size. The Fig.4 shows several gait silhouette images after alignment.

Fig.3 : The Silhouette images after alignment

Secondly the Gait cycle detection was done. Before constructing the Hough template it is very important to compute the periodicity of walking in a gait sequence. After constructing a Hough Transform the Gait Template was constructed. The Gait template was constructed using Laplacian of Gaussian methods. Using this method the edges in intensity gait images were detected. Finally the PCA technique was applied for Feature extraction.

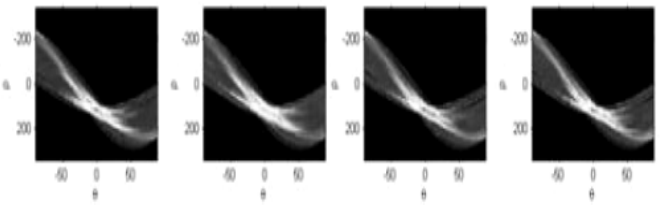


Fig.4 : Gait Templates using Hough Transform

V. Discussion on Analysis

The Gait recognition using Wavelet Descriptor with ICA used two public gait databases, namely Chinese National Laboratory of Pattern Recognition (NLPR) and Chinese Xi'an University of Technology (XAUT) gait database were used to test and evaluate this approach. Here NLPR database having 20 subjects and four sequences for each views angle and have three angles, namely laterally (0°), obliquely (45°) and frontally (90°), XAUT database includes 10 subjects and four sequences for each views angle and have three angles, namely laterally (0°), obliquely (45°) and frontally (90°). The Gait recognition using Hough Transform with PCA used CASIA-A gait database for the analysis purpose [10]. All subjects walk on a straight line under normal conditions. Similar to the Wavelet Descriptors with ICA the three different view angles were [11] used to capture every subject. The database consists of 20 different persons. Each person has 4 sequences per view. The database thus includes a total of 240 (20×4×3) sequences. The length of each collected sequence varies with the pace of the walker, but the average is about 90 frames [11].

Table 1: Ranking & Accuracy of Features extracted

View Angles & Ranks	Performance Analysis (Accuracy %)	
	Wavelet Descriptor with ICA (SVM - NN)	Hough Transform with PCA (CMS)
Laterally (0°)		
Rank 5	97.5%	98.5%
Rank 10	100%	97.5%
Obliquely (45°)		
Rank 5	92.5%	100%
Rank 10	100%	98.5%
Frontally (90°)		
Rank 5	90%	100%
Rank 10	100%	100%

The above table shows the accuracy percentage of the two techniques with respect to the three view angles such as laterally (0°), obliquely (45°) and frontally (90°). In this table for all the three angles the Rank 10 has 100% accuracy for Wavelet Descriptor with ICA technique. Hough Transform with PCA has 97.5% accuracy for Rank 10 and 98.5% accuracy for obliquely (45 °). In the case of frontally (90°) angle both the techniques has 100% accuracy. The increase in the percentage of accuracy for wavelet descriptor with ICA is shown in the below graph.

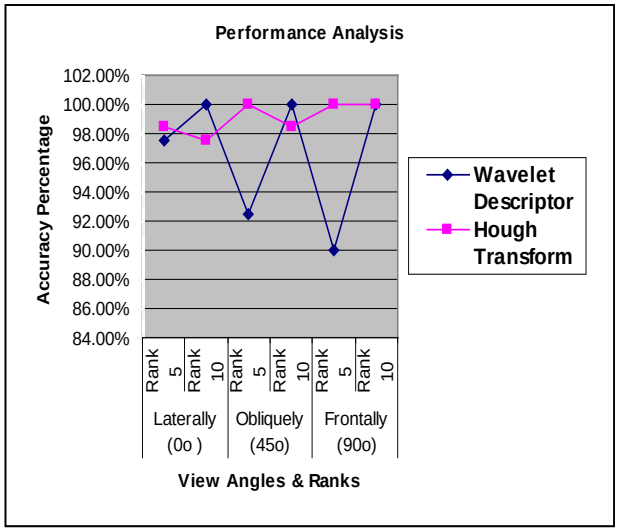


Fig 5 : Accuracy (%) of PCA & ICA techniques

VI. Conclusion

The wavelet descriptor with ICA uses SVM and Nearest Neighbour classifier for classification and recognition. The second approach uses Cumulative Match Scores (CMS) for gait recognition. Both the techniques were compared with different kinds of databases and the results were shown.

References Références Referencias

1. Qinghan, "Technology review - Biometrics-Technology,Application, Challenge and Computational Intelligence Solutions," IEEE Computational Intelligence Magazine, vol. 2, pp. 5-25, 2007.
2. Niyogi, S., Adelson, E.: Analyzing and Recognizing Walking Figures in XYT. In:IEEE Computer Society Conference on Computer Vision and Pattern Recognition, Seattle, Wash, USA, pp. 469–474 (1994)
3. Sarkar, S., Phillips, P.J., Liu, Z.Y., et al.: The HumanID Gait Challenge Problem: Data sets, Performance, and Analysis. IEEE Trans. Pattern Anal. Mach. Intell. 27(2),162–177 (2005)
4. Zhang, R., Vogler, C., Metaxas, D.: Human Gait Recognition at Sagittal Plane. Image Vision Computing 25(3), 321–330 (2007)
5. Meyer, D., Denzler, J., Niemann, H.: Model Based Extraction of Articulated Objects in Image Sequences for Gait Analysis. In: Proceedings of International Conference on Image Processing, October 1997, vol. (3), pp. 78–81 (1997)
6. Lee, L., Grimson, W.E.L.: Gait Analysis for Recognition and Classification. In:Proc. IEEE Int. Conf. Automatic Face and Gesture Recognition, Washington, DC, pp.148–155 (2002).

7. Jiwen Lu et.al., Gait Recognition Using Wavelet Descriptors and Independent Component Analysis Springer-Verlag Berlin Heidelberg 2006
8. Yu, J., Duan, J., Su, K.: A Hough Transform Based Method for Gait FeatureExtraction Journal of Image and Graphics 10(10), 1304–1309 (2005)
9. Boulgouris, N.V., Plataniotis, K.N., Hatzinakos, D.: An Angular Transform of Gait Sequences for Gait Assisted Recognition. In: Proc. IEEE Int. Conf. Image Processing, Singapore, pp. 857–860 (2004)
10. CASIA-A Gait Database [OL/DB], http://www.cbsr.ia.ac.cn/
11. Wang, L., Tan, T.N., Hu, W.M., Ning, H.Z.: Automatic Gait Recognition Based on Statistical Shape Analysis. IEEE Transactions on Image Processing 12(9), 1120–1129 (2003)
12. Ling-Feng Liu, Wei Jia1, and Yi-Hai Zhu : Gait Recognition Using Hough Transform and Principal Component Analysis Springer-Verlag Berlin Heidelberg 2009.
13. Jiwen Lu, Erhu Zhang, and Cuining Jing : Gait Recognition Using Wavelet Descriptors and Independent Component Analysis Springer-Verlag Berlin Heidelberg 2006.

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 12 Issue 10 Version 1.0 May 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Proposed Smart DSR(S-DSR) Protocol for Ad Hoc Network

By Anupam Baliyan & Sanjeev Gupta
IMR, Ghaziabad, (U.P) India

Abstract - Mobile Ad hoc networks (MANET) are considered as promising communication networks in situations where rapid deployment and self-configuration is essential. In ad hoc networks, nodes are allowed to communicate with each other without any existing infrastructure. Typically every node should also play the role of a router. This kind of networking can be applied to scenarios like conference room, disaster management, battle field communication and places where deployment of infrastructure is either difficult or costly. Many routing protocols exist to enable communication in ad hoc networks like, DSR [2], AODV [1], DSDV [3], etc. All these protocols assume that the source and destination nodes can reach each other using a single or multi-hop path. But, there exist situations when connectivity between source and destination cannot be guaranteed always. DSR [2] delivers data in a MANET with the assumption that the network is connected DSR, fails when the network is partially connected, source and destination are in different partitions. Connectivity in the network is very low for less number of nodes in the network. As the density of nodes increases, connectivity improves.

In this Paper we mainly focus on these kinds of networks.We discuss the challenges in Moblie ad hoc network ands more topology related details and the applicability of one of the existing routing schemes (DSR) on these networks in the forthcoming sections. In this paper we proposed SDSR(Smart DSR protocol) which deliver data in a partially connected ad hoc network.

GJCST Classification: C.2.1

Strictly as per the compliance and regulations of:

Proposed Smart DSR(S-DSR) Protocol for Ad Hoc Network

Anupam Baliyan [α] & Sanjeev Gupta [σ]

Abstract - Mobile Ad hoc networks (MANET) are considered as promising communication networks in situations where rapid deployment and self-configuration is essential. In ad hoc networks, nodes are allowed to communicate with each other without any existing infrastructure. Typically every node should also play the role of a router. This kind of networking can be applied to scenarios like conference room, disaster management, battlefield communication and places where deployment of infrastructure is either difficult or costly. Many routing protocols exist to enable communication in ad hoc networks like, DSR [2], AODV [1], DSDV [3], etc. All these protocols assume that the source and destination nodes can reach each other using a single or multi-hop path. But, there exist situations when connectivity between source and destination cannot be guaranteed always. DSR [2] delivers data in a MANET with the assumption that the network is connected DSR, fails when the network is partially connected, source and destination are in different partitions. Connectivity in the network is very low for less number of nodes in the network. As the density of nodes increases, connectivity improves.

In this Paper we mainly focus on these kinds of networks.We discuss the challenges in Moblie ad hoc network ands more topology related details and the applicability of one of the existing routing schemes (DSR) on these networks in the forthcoming sections. In this paper we proposed SDSR(Smart DSR protocol) which deliver data in a partially connected ad hoc network.

I. Introduction

Ad hoc network can be defined as an assembly of communication nodes willing to communicate with one another over a wireless medium. There is no fixed infrastructure in an ad hoc network, unlike in the cellular networks. Such devices can communicate with another node that is immediately within their radio range (peer-to-peer communication) or one that is outside their radio range (remote2remote communication) using intermediate node(s) to relay or forward the packet from the source (sender) toward the destination (receiver) [6]. Power consumption is a serious issue in an ad hoc networks, since it rely on forwarding data packets sent by other nodes.

Ad hoc networks are self-creating, self-organizing and self-administering. That is to say that a formed network can be deformed while on transit without the need for any system administration. Ad hoc network is mostly used in conditions where there is non-availability of infrastructure, unreliable or entrusted networks especially under emergency conditions.

Example of such communication capacity of an ad hoc networking can be applied in military war fighters in the battlefield, conferencing, sensor networks, home networking, embedded computing and personal area networking.

Due to lack of wired infrastructures and power control, there is always a problem of constant changes in the connectivity and link characteristics in ad hoc networks. In an ad hoc networking, multi-layer problem is always the case. Here, the physical layer should adapt to the constant changes in the link characteristics. It is important that ad hoc network applications should be design in such a way that it will handle connectivity problems. Packet delay and lost problems as well, have to be put into consideration when designing the network.

II. Challenges in Manet

Two main challenges in MANETs (when traditional routing protocols fail) are Intermittent Connectivity and Network Partition.

Intermittent connectivity:

- When nodes are in motion, links can be obstructed by intervening objects.
- When nodes conserve power, links are shutdown periodically Network partition:
- When no path exists between source and destination, it is perfectly possible that two nodes may never be part of the same connected portion of the network.

III. Issues in Conventional Manet Routing Protocol

Intermittently Connected Mobile ad hoc network with long disconnection time creates network partition. In this context, conventional routing schemes fail, because they try to establish complete end-to-end path between sources to destination before any data is sent. Existing Routing protocols [1],[2] simply discard the packets if the packet is not delivered within a small amount of time. These routing protocols fail in Intermittently Connected Mobile Ad hoc networks because of the following characteristics of Network:

- Intermittent network contacts

Author α : Associate Proffesor - IMR, Ghaziabad, (U.P) India.
Author σ : Director General-KRM Mangalam, New Delhi, India.

- End-to-end path between the source and the destination may have never existed
- Disconnection and reconnection is common highly variable link performance

IV. Partially Connected ad Hoc Network

Intermittently connected Mobile Ad hoc networks are mobile wireless networks where most of the time there does not exist a complete path from a source to a destination, or such a path is highly unstable and may change or break soon after it has been discovered. This is due to Node mobility, limited radio range, physical obstacles, severe weather, wide deployment area or other physical factors. Most ad hoc network routing algorithms are designed for networks that are always connected. While it is certainly desirable to maintain a connected network, various conditions may cause a mobile ad hoc network to become partitioned, meaning that there is no single-hop or multiple-hop route between some (or all) source/destination node pairs. Might prevent some nodes from communicating with others and result in a partitioned network. The existence of network partitioning requires a new routing approach other than the traditional "store-and forward" routing paradigm used in most current ad hoc routing algorithms, in which messages are dropped if no route is found to reach a destination within a small amount of time.

V. Routing Considerations in Partially Connected ad Hoc Network

There are many characteristics DTN protocols, including routing, must take into consideration. A first consideration is if information about future contacts is readily available. For example, in interplanetary communications, many times a planet or moon is the cause of contact disruption, and large distance is the cause of communication delay. However, due to the laws of physics, it is possible to predict the future in terms of the times contacts will be available, and how long they will last. These types of contacts are known as scheduled or predictable contact [7]. On the contrary, in disaster recovery networks the future location of communicating entities, such as emergency responders, may not be known. These types of contacts are known as intermittent or opportunistic contacts.

A second consideration is if mobility can be exploited and, if so, which nodes are mobile. There are three major cases, classifying the level of mobility in the network. First, it is possible that there are no mobile entities. In this case, contacts appear and disappear based solely on the quality of the communication channel between them. For instance, in interplanetary networks, large objects in space, such as planets, can block communicating nodes for a set period of time. Second, it is possible that some, but not all, nodes in the network are mobile. These nodes, sometimes referred to as Data Mule [8][9], are exploited for their mobility. Since they are the primary source of transitive communication between two non-neighboring nodes in the network, an important routing question is how to properly distribute data among these nodes. Third, it is possible that the vast majority, if not all, nodes in the network are mobile. In this case, a routing protocol will most likely have more options available during contact opportunities, and may not have to utilize each one[11][13][14]. An example of this type of network is a disaster recovery network where all nodes (generally people and vehicles) are mobile [15]. A second example is a vehicular network where mobile cars, trucks, and buses act as communicating entities [6].

A third consideration is the availability of network resources. Many nodes, such as mobile phones, are limited in terms of storage space, transmission rate, and battery life. Others, such as buses on the road, may not be as limited. Routing protocols can utilize this information to best determine how messages should be transmitted and stored to not over-burden limited resources. As of April 2008, only recently has the scientific community started taking resource management into consideration, and this is still an active area of research

VI. Related Work

A number of projects attempt to enable message delivery in a partially connected Ad Hoc Network **Data MULE project** uses mobile nodes to collect data from sensors which is then delivered to a base station. The Data MULEs are assumed to have sufficient buffer space to hold all data until they pass a base station. The approach is similar to the technique used in [25]. These projects study opportunistic forwarding of information from mobile nodes to a fixed destination. However, they do not consider opportunistic forwarding between the mobile nodes. **Li** [22] explore message delivery in disconnected MANETs where nodes can be instructed to move in order to transmit messages in the most efficient manner.

Epidemic Routing [32] provides message delivery in disconnected environments where no assumptions are made in regards to control over node movements or knowledge of the network's future topology. Each host maintains a buffer containing messages. Upon meeting, the two nodes exchange summary vectors to determine which messages held by the other have not been seen before. They then initiate a transfer of new messages. In this way, messages are propagated throughout the network. This method guarantees delivery if a route is available but is

expensive in terms of resources since the network is essentially flooded. Attempts to reduce the number of copies of the message are explored in [25] and [26]. Ni et al. [25] take a simple approach to reduce the overhead of flooding by only forwarding a copy with some probability $p < 1$, which is essentially randomized flooding.

The Spray-and-Wait solution presented by Spyropoulos [26] assigns a replication number to a message and distributes message copies to a number carrying nodes and then waits until a carrying node meets the destination. A number of solutions employ some form of 'probability to deliver 'metric in order to further reduce the overhead associated with Epidemic Routing by preferentially routing to nodes deemed most likely to deliver. These metrics are based on contact history, location information or utility metrics.

The message ferrying project [23] proposes proactively changing the motion of nodes to help deliver data. They investigate both 'node initiated' mobility, where the nodes move to meet a known message ferry trajectory, or 'ferry initiated' mobility, Where the nodes signal communication requests via a long range radio, and the message ferry moves to meet them. Both assume control over node movements and in the case of message ferries, knowledge of the paths to be taken by these message ferry nodes. Other work utilizes a time-dependent network graph in order to efficiently route messages.

Replace message ferrying approach [33] state that in message ferrying approach ferry node is a central point of failure for the system. New approaches have been proposed which focus on the reliability of the systems. One of the solutions to this problem is replacement of ferry as proposed in. They proposed two protocols - either change the ferry node when the current ferry node fails, or change the ferry node periodically. The first method is centralized approach where successor ferry is always decided by the present ferry. Later is a distributed way of choosing the ferry node. Here each node declares its willingness to become ferry and on the basis of vote, one node will be chosen as ferry node information only.

Musolesi. [27] Introduce a generic method that uses Kalman filters to combine and evaluate the multiple dimensions of a node's context in order to make routing decisions. The context is created from measurements that nodes perform periodically, which can be related to connectivity. The approach only uses a single copy of a message, which is passed from one node to a node with a higher 'delivery metric'.

Jain [21] assume knowledge of connectivity patterns where exact timing information of contacts is known, and then modifies Dijkstra's algorithm to compute the cost edges and routes accordingly. Merugu likewise make the assumption of detailed knowledge of node future movements.

Handorean [31] take a similar approach with knowledge of connectivity. However, they do relax this assumption where only partial information is known. This information is time-dependent and routes are computed over the time-varying paths available. However, if nodes do not move in a predictable manner, or are delayed, then the path is broken. Additionally, if a path to the destination is not available using the time-dependent graph, the message is flooded.

PROPHET Routing [30] is also probability-based, using past encounters to predict the robability of meeting a node again, nodes that are encountered frequently have an increased probability whereas older contacts are degraded over time. Additionally, the transitive nature of encounters is exploited where nodes exchange encounter probabilities and the probability of indirectly encountering the destination node is evaluated. Similarly [25] and [29] define probability based on node encounters in order to calculate the cost of the route. [27] And [28] use the so-called 'time elapsed since last encounter' or the 'last encounter age' to route messages to destinations. In order to route a message to a destination, the message is forwarded to the neighbor who encountered the destination more recently than the source and other neighbors.

Spyropoulos [20] use a combination of random walk and utility-based forwarding. Random walk is used until a node with a sufficiently high utility metric is found after which the utility metric is used to route to the destination node.

Leguay [24] present a virtual coordinate system where the node coordinates are composed of a set of probabilities, each representing the chance that a node will be found in a specific location. This information is then used to compute the best available route.

Lebrun [28] propose a location-based delay-tolerant routing scheme that uses the trajectories of mobile nodes to predict their future distance to the destination and passes messages to nodes that 33 are moving in the direction of the destination.

Border node Based Routing (BBR)[35] protocol for partially connected VANETs state that considers the characteristics of partially connected VANETs while at the same time takes into account the limitations of existing routing approaches for partially connected ad hoc networks The BBR protocol is specifically designed to accommodate for the effects of node mobility on data delivery. The BBR protocol has two basic functional units: a neighbor discovery algorithm, and a border node selection algorithm. The neighbor discovery process is responsible for collection of current one-hop neighbor information. This step requires periodic beaconing of "hello" messages. The border node selection process is responsible for selection of the right candidate/candidates for packet forwarding based on

the one hop neighbor information collected in the neighbor discovery process.

Random and Encounter Time Based Forwarding mechanism[4] state that based on the analysis of the existing utility-based forwarding mechanisms, for the inefficient forwarding of history encounter time based forwarding mechanism in the initial phase of the node movement, a Random and Encounter Time Based algorithm named RET is proposed in this paper. RET divides the nodes moving into two phases-random forwarding phase (initial phase) and utility-based forwarding phase. In random forwarding phase, random algorithm is used to forward packets. And in utility-based forwarding phase, the packets are forwarded by using utility value. The results of simulation experiment show that the RET algorithm can reduce the delivery delay under low node density.

VII. Working of Dsr

DSR contains 2 phases

- Route Discovery (find a path)
- Route Maintenance (maintain a path)

Route Discovery and Route Maintenance only response on a request.

a) Route Discovery

If node A has in his Route Cache a route to the destination E, this route is immediately used. If not, the Route Discovery protocol is started:

- Node A (initiator) Sends a Route Request packet by flooding the network as shown in Fig1, each route request packet contains
  - ➢ Route record
  - ➢ Initiator Address
  - ➢ Request ID

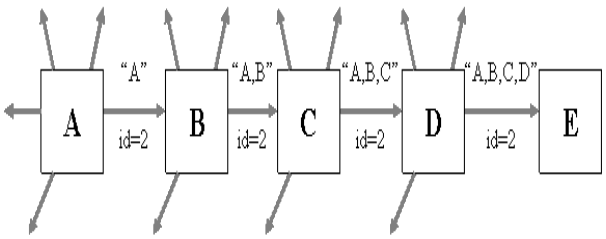


Fig. 1: Route Discovery example: Node A is the initiator, and node E is the target

- If the route discovery is successful the initiating host receives a route reply packet.
- When any host receives a route request packet, it processes the request accounting to the following steps.
  - ➢ If < initiator address, request id > is found in this host then discards the route request packet.
  - ➢ If this host's address is already listed in the route record Discard the route request packet.
  - ➢ If the target of the request matches this host's address return a copy of this route in a route reply packet to the initiator.
  - ➢ Otherwise, append this host's address to the route record, and re-broadcast the request.

After getting the route reply the sender send the data to the destination.

b) Route Maintenance

In DSR every node is responsible for confirming that the next hop in the Source Route receives the packet. Also each packet is only forwarded once by a node (hop-by-hop routing). If a packet can't be received by a node, it is retransmitted up to some maximum number of times until a confirmation is received from the next hop. Only if retransmission results in a failure, a Route Error message is sent to the initiator that can remove that Source Route from its Route Cache. So the initiator can check his Route Cache for another route to the target. If there is no route in the cache, a Route Request packet is broadcasted.

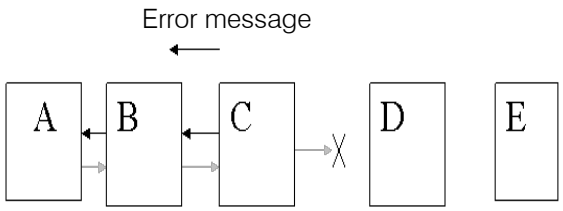


Fig. 2:

- ➢ If node C does not receive an acknowledgement from node D after some number of requests, it returns a Route Error to the initiator A.
- ➢ As soon as node receives the Route Error message, it deletes the broken-link-route from its cache. If A has another route to E, it sends the packet immediately using this new route.
- ➢ Otherwise the initiator A is staring the Route Discovery process again.

VIII. Dsr Over Partially Connected ad Hoc Networks

DSR [2] delivers data in a MANET with the assumption that the network is connected DSR, fails when the network is partially connected, source and destination are in diffirent partitions. Connectivity in the network is very low for less number of nodes in the network. As the density of nodes increases, connectivity improves. When the source node and destination node are connected then DSR work well but when the source node and destination node are not connected mean there is no path between source node and the destination node then DSR does not deliver data due to no path between source and destination.

IX. Smart Dsr Protocol

Smart DSR Protocol is an extension of DSR Protocol which can delivers data from a source to a destination even there is no path between source and destination. This protocol will work as normal DSR if the network is fully connected and when the network is not fully connected then also this protocol will make it ensure that data will be delivered from a source to a destination.

a) Design Issues

The following design issues have been identified that need to be addressed while Designing the proposed protocol.

- Which node will become a smart node?
- How will a source choose among the more than one smart replies?
- When will a node decide that it is in a new locality?

b) Smart Node Parameter

Which node will become the smart node there may be following parameter for that

- A node can be a smart node on behalf of the number of neighbors seen by node per unit time. If a node seen maximum number of neighbors it will indicate that mobility of node is high and there is a chance that the node will come near to the destination frequently.
- A node can be the smart node if the routing table of node is big which indicate that node is well connected to the network.

c) Selection of Smart Replies

As more than one node can send the smart reply to the source so selection of one reply out of many is also an issue to be consider. The source node can use the same parameter as we mentioned above to sort out this issue. A node which sends a smart reply will send the smart parameter to the source and source node can select best smart node on behalf of these parameters

d) Proposed Smart DSR Protocol

The proposed smart protocol will go for RREQ/RREP, RREQ/SRREP and SRREQ/SRREP cycle. We use the following symbolic notation for the proposed smart DSR protocol.

RREQ	Route Request
RREP	Route Reply
SRREQ	Smart Route Request
SRREP	Smart Route Reply

The proposed Smart DSR protocol will work according to the following steps.

Step 1 - A Source node need a route to destination it broadcast a RREQ packet across the Network.

Step 2 - Any node receiving this packet update their information for the source node and Will do following.

2.1- If <Source address, Req id> is found in this node then discard the Route Request packet.

2.2 - If the node address listed in the Route Record. Discard the Route Request Packet.

2.3 - If the target of the Request node match this host address return a copy of this route in a Route replies Packet to the source node and goes to Step 3

2.4 - Otherwise append this host address to the route record, and rebroadcast this Request.

2.5 - If this is the last RREQ retry, the node checks its eligibility to become a Smart node and send a SRREP to the source if it satisfies all the criteria and goes to Step4

Step-3 If the source node gets the reply from the destination then after establish the path the source node send data to the destination,

Step-4 If Source node receives SRREP then it store the smart route reply and wait for more reply. After the expiry the timer the source will select some of the Smart reply and send data to only those smart nodes.

Step-5 After getting data from the original source the Smart node will do following

5.1- After receiving the data from the source, smart node will store the data and permanently checks for new locality.

5.2 - When a smart node detect that it is in a new locality it send a SRREQ to destination on behalf of the source.

5.3 - If a smart node will receive a Route Reply from the destination then it deliver its data to the destination .After delivering the data to the actual destination the smart node will send an acknowledgement to the actual source so that the source node will aware of this fact that its data is sent to the destination.

5.4 - If Smart node will not get a route Reply from the destination it indicate that the destination is not connected with the smart node so smart node will select some another smart node to keep the data on behalf of the previous smart node and when then new smart node will move near to the destination it deliver data to the destination on behalf of the previous smart node.

5.5 - After delivery of data the new smart node will send acknowledgement to the previous smart node and when previous smart node move near to the original source node then it send an acknowledgement to the source node so that the original source node will be aware that data is deliver to the destination

e) States of Node

During the Smart DSR protocol node can be in various state those are explain below

Node has Data to Send:

This event is explained by the following algorithim1. A node initiates a RREQ message if it is the original source of this message, or it initiates a SRREQ message if it is storing data on behalf of other node.

Algorithim1:-
If node has data **Then** Node send a RREQ
If node receives a RREP **then** Protocol will use DSR
Else
If node receives SRREP **then** wait for RREP

If there is no RREP then node will select Smart node and node sends data to the Smart node.

Node Receives a SRREQ:

This event is explained by the following algorithm 2. When a node receives a SRREQ it checks whether, it is the destination for this request.

Algorithim2:-
If a node A receive SRREQ **Then**
If A = Destination **Then** Protocol will use DSR
Else
if A is a Smart Node **Then**
A store SRREQ in database.
A send SRREP to source and broadcast SRREQ.
A wait for data if data is available then A store data.

If it is the destination then the node sends a back RREP otherwise this node is not the original destination for this request then this node makes calculation for proxy selection parameters, if the parameter values are above some defined threshold then, the node sends a SRREP. At the end it simply forwards the SRREQ.

When a Node Receives a SRREP This situation is also Explain in Algorithim2. When a proxy/original source gets a original reply from a node. It simply sends data to destination.

If node gets a proxy reply then it will store this reply in a data structure and wait for route retries time out and then used some functions to evaluate the proxy route replies to choose some nodes to become proxy.

A Node Senses a New locality:

When a node realizes that it is in a new locality then it checks for locally stored data. If it finds some data then it initiates a Smart route request for that data.

X. Conclusion

The Smart DSR protocol designed in the work behave like a normal DSR protocol if the source and the destination are connected and however there is no path between source and destination then the Smart DSR protocol will be used to send the data between source and destination therefore using of the above protocol shall enhance the DSR Routing in partially connected network as well.

The proposed protocol seems to be effective when the network is partially connected additionally the proposed protocol will work when the network is connected mean there is a path between source and destination. We can enhance the efficiency of the protocol by changing the parameter for selection of a proxy node.

There is a trade off between “Load on Network” and “Message Delivery efficiency”. If we impose less restriction on proxy selection, then the probability of message delivery increases But at the same time load on network and nodes increases. If we impose strict restrictions on proxy selection criteria, then message delivery probability decreases. In future we will modified the above mentioned protocol w.r.t the route maintaince as here the SDSR will use the same route maintaince as DSR. We also implement the above protocol on simulation and compare the result in future.

References Références Referencias

1. C. Perkins and E. Royer. Ad-hoc on-demand Distance Vector Routing. pages 90–100,1999.
2. David B. Johnson and David A. Maltz. Dynamic Source Routing in ad hoc Wireless Networks. In Mobile Computing, Kluwer Academic Publishers, 1996.
3. Perkins C.E. and Praveen Bhagwat. Destination-sequenced Distance vector (dsdv) protocol. In SIGCOMM ’94, Conference on Communications Architecture, Protocol and Application, pages 234–244, August 1994.
4. Jain Shu,Kun Yu,Yebin Chen,Youlei Fan “A Random and Encounter Time based Forwarding mechanism for Opportunistic Network”, ISIP, 2010, ISBN-9781424486274, pp 50-53
5. Bheemarjuna Reddy, T., Karthigeyan, I., Manoj, B.S. and SivaRam Murthy, C. (2006) 'Quality of service provisioning in ad hoc wireless networks: a survey of issues and solutions', *Ad Hoc Networks*, Vol. 4, No. 1, pp. 83-124.
6. John Burgess, Brian Gallagher, David Jensen, and Brian Neil Levine. MaxProp: Routing for vehicle-based disruption-tolerant networks. In Proc. IEEE INFOCOM, April 2006
7. Sushant Jain, Kevin Fall, and Rabin Patra. Routing in a delay-tolerant network. In Proc. ACM SIGCOMM, 2004
8. Jea D., Somasundara A. A, and Srivastava M. B. Multiple Controlled Mobile Elements (Data Mules) for Data Collection in Sensor Networks. In Proc. IEEE/ACM International Conference on Distributed Computing in Sensor Systems (DCOSS), June 2005.
9. Rahul C. Shah, Sumit Roy, Sushant Jain, and Waylon Brunette. Data MULEs: Modeling a Three-tier Architecture for Sparse Sensor Networks. In

Proc. IEEE SNPA Workshop, May 2003 [10] Li Wei and Guizan Mohsen "Quality of services in Mobile Ad hoc Networks", Eurasup journal on wireless communication and networking,Jan,2006.

10. C. Murthy and B. Manoj, "Ad Hoc Wireless Networks." Pentice Hall Publishers 2004.
11. Aruna Balasubramanian, Brian Neil Levine, and Arun Venkataramani. DTN routing as a resource allocation problem. In Proc. ACM SIGCOMM, August 2007.
12. P.Trakadas, T. Zahariadis, S.Voliotis, C. Manasis, "Efficient Routing in PAN and Sensor Networks," ACM SIGMOBILE Mobile Computing and Communication review vol.8 no.1 2008
13. Thrasyvoulos Spyropoulos, Konstantinos Psounis, and Cauligi S. Raghavendra. Spray and wait: An efficient routing scheme for intermittently connected mobile networks. In WDTN '05: Proceeding of the 2005 ACM SIGCOMM workshop on Delay-tolerant networking, 2005
14. Thrasyvoulos Spyropoulos, Konstantinos Psounis, and Cauligi S. Raghavendra. Spray and focus: Efficient mobility-assisted routing for heterogeneous and correlated mobility. In Fifth Annual IEEE International Conference on Pervasive Computing and Communications Workshops, 2007.
15. Samuel C. Nelson, Albert F. Harris, and Robin Kravets. Event-driven, role-based mobility in disaster recovery networks. In Chants 07: Proceedings of the second workshop on Challenged Networks, 2007
16. Zhao W., Ammar M., and Zegura E. A message ferrying approach for data delivery in sparse ad hoc networks. In Proceedings of 5th international symposium on mobile ad hoc networking and computing, 2004.
17. Jain Sushant, Kevin Fall, and Patra Rabin. Routing in a delay tolerant network. In SIGCOMM '04: Proceedings of the 2004 conference on Applications, technologies, architectures, and protocols for computer communications, 2004.
18. Sunil Kumar, Vineet S. Raghavan and Jing Deng," Medium Access Control protocols for ad hoc wireless networks 2006.
19. Spyropoulos, T., Psounis, K., and Raghavendra, C. S. Single-copy routing in intermittently connected mobile networks. In *proc. SECON '04* (2004), IEEE, pp. 235–244.
20. Jain, S., Fall, K., and Patra, R. Routing in a delay tolerant network. *SIGCOMM Comput. Commun. Rev. 34*, 4 (October 2004), 145–158.
21. LI, Q., and Rus, D. Sending messages to mobile users in disconnected ad-hoc wireless networks. In *proc. MobiCom '00* (2000), ACM Press, pp. 44–55.
22. Zhao, W., Ammar, M., and Zegura, E. Amessage ferrying approach for data delivery in sparse mobile ad hoc networks. In *proc. MobiHoc '04* (2004), ACM Press, pp. 187–198.
23. Leguay, J., Friedman, T., and Conan, V. Evaluating mobility pattern space routing for DTNs. In *proc. IEEE Infocom 2006* (April 2006), vol. 5, IEEE, pp. 2540–2549.
24. NI, S.-Y., Tseng, Y.-C., Chen, Y.-S., and Sheu, J.-P. The broadcast storm problem in a mobile ad hoc network. In *proc. MobiCom '99* (1999), ACM Press, pp. 151–162. 26
25. Spyropoulos, T., Psounis, K., and Raghavendra, C. S. Spray and wait: an efficient routing scheme for intermittently connected mobile networks. In *proc. WDTN '05* (2005), ACM Press, pp. 252–259.
26. Dubois-Ferriere, H., Grossglauser, M., and Vetterli, M. Age matters: efficient route discovery in mobile ad hoc networks using encounter ages. In *proc. MobiHoc '03* (2003), ACM Press, pp. 257–266.
27. Grossglauser, M., and Vetterli, M. Locating nodes with ease: last encounter routing in ad hoc networks through mobility diffusion. In *proc. INFOCOM '03* (2003), vol. 3, IEEE, pp. 1954–1964 vol.3
28. Tan, K., Zhang, Q., and Zhu, W. Shortest path routing in partially connected ad hoc networks. In *proc. GLOBECOM '03* (2003), vol. 2, IEEE, pp. 1038–1042 Vol.
29. Lindgren, A., Doria, A., and Schelén, O. Probabilistic routing in intermittently connected networks. *Lecture Notes in Computer Science 3126* (2004), 239–254.
30. Handorean, R., Gill, C., and Roman, G.-C. Accommodating transient connectivity in ad hoc and mobile settings. *Lecture Notes in Computer Science 3001* (March 2004), 305–322
31. Vahdat, A., and Becker, D. Epidemic routing for partially connected ad hoc networks. *Technical Report CS-200006, Duke University* (2000).
32. J.Yang, Y. Chen, M. Ammar, and C. K. Lee. Ferry replacement protocols in sparse manet message ferrying systems. In college of Computing, Georgia Tech, 2004.
33. A. Demers, D. Greene, C. Hauser, W. Irish, J. Larson, S. Shenker, H. Sturgis, D. Swinehart, and D. Terry, "Epidemic algorithms for replicated database maintenance," Proceedings of the Sixth Symposium on Principles of Distributed Computing, 1987, pp. 1–1
34. Mingliu Zhang ,Wolf R.S Globecom workshop,2007 IEEE,Inspec:978-1-4244-2024-7 pp 1-7

This page is intentionally left blank

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 12 Issue 10 Version 1.0 May 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Power Saving Mechanism with Less Number of Nodes in the Routing Path in Adhoc Wireless Networks Using MARI Algorithm

By Dr.M.V.Subramanyam & P.V.Gopikrishna Rao
RGM College of Engineering, Nandyal, kurnool (dt), India

Abstract - Adhoc wireless networks have emerged as one of the key growth areas for wireless3 networking and computing technology. Adhoc networks are a new wireless networking paradigm for mobile hosts. Unlike traditional mobile wireless networks, adhoc networks do not rely on any fixed infrastructure. Instead, hosts rely on each other to keep the network connected. The nodes in ad-hoc networks are battery operated and have limited energy resources, which is indeed a key limitations. Each node consumes a large amount of energy while transmission or reception of packets, among the nodes. While the nodes depend on each other for efficient transferring of packets, it is a key issue in adhoc networks to have efficient methods for forwarding of packets between any given pair of nodes, with minimum power consumption and less number of intermediate nodes . In this study we propose an optimal routing protocol called MARI (Mobile Agent with Routing Intelligence). The MARI Topology proposed for power management is novel and is used for the consumption of minimum power in an adhoc wireless network, at each node. The Protocol groups the network into distinct networks with the selection of MARI nodes and Gateways for efficient packet transmission between any member node pair. The operational cycle at each node is classified into four distinct operations, i.e., transmitting, receiving, idle and sleep cycle, in order to achieve efficient power management in an Adhoc wireless network.

GJCST Classification: C.2.1

Strictly as per the compliance and regulations of:

Power Saving Mechanism with Less Number of Nodes in the Routing Path in Adhoc Wireless Networks Using MARI Algorithm

Dr. M.V.Subramanyam[α] & P.V.Gopikrishna Rao[α]

Abstract - Adhoc wireless networks have emerged as one of the key growth areas for wireless3 networking and computing technology. Adhoc networks are a new wireless networking paradigm for mobile hosts. Unlike traditional mobile wireless networks, adhoc networks do not rely on any fixed infrastructure. Instead, hosts rely on each other to keep the network connected. The nodes in ad-hoc networks are battery operated and have limited energy resources, which is indeed a key limitations. Each node consumes a large amount of energy while transmission or reception of packets, among the nodes. While the nodes depend on each other for efficient transferring of packets, it is a key issue in adhoc networks to have efficient methods for forwarding of packets between any given pair of nodes, with minimum power consumption and less number of intermediate nodes . In this study we propose an optimal routing protocol called MARI (Mobile Agent with Routing Intelligence). The MARI Topology proposed for power management is novel and is used for the consumption of minimum power in an adhoc wireless network, at each node. The Protocol groups the network into distinct networks with the selection of MARI nodes and Gateways for efficient packet transmission between any member node pair. The operational cycle at each node is classified into four distinct operations, i.e., transmitting, receiving, idle and sleep cycle, in order to achieve efficient power management in an Adhoc wireless network.

I. Introduction

Wireless networking grows rapidly because of the human desires for mobility and for freedom from limitation, i.e., from physical connections to communication networks [10]. Recent advances in wireless technology have equipped portable computers, such as notebook computers and Personal Digital Assistants (PDA's) with wireless interfaces that allow networked communication even while a user is mobile [4]. A particular kind of wireless network called mobile adhoc network is presently under development, which is the subject of this. A mobile adhoc network is a self-organizing and rapidly deployable network in which neither a wired backbone nor a centralized control exists. The network nodes communicate with one another over scarce wireless channels in a multi-hop fashion.

In this, we propose an algorithm for topology management for the Adhoc wireless networks is: A power management algorithm to reduce the consumption of the power of each node in the adhoc wireless networks, by the introduction of MARI (**Mobile Agents with Routing Intelligence**) topology (a topology having MARI nodes) and management.

The absence of a central infrastructure implies that an adhoc wireless network does not have an associated fixed topology. Hence, a most important task of an adhoc wireless network consisting of geographically dispersed nodes is to determine (in real time) an appropriate topology over which high-level routing protocols can be implemented [12].

Some of the properties of adhoc networks that make them difficult to manage are:

1. Complexity of nodes.
2. Message overhead
3. Energy consumption.
4. Mobility
5. Degraded channel quality
6. Security

II. Mari Topology Formation and Management

Minimizing energy consumption is an important as well as a difficult challenge in mobile networking. The requirement of cooperation between power saving [7] and routing protocols is particularly important in the case of multi-hop adhoc wireless networks, where nodes must forward packets from one to another [3,8,9].

This thesis proposes a novel topology management scheme for adhoc wireless networks for power management called, MARI Topology. The nodes in this scheme are classified into three categories based on their power level. They are:

a) MARI Nodes

MARI nodes are selected in such a way that they have the maximum power level among their one-hop neighbors and all non-MARI nodes in the one-hope neighborhood are within the transmission range of MARI nodes. These MARI nodes [16] have the routing intelligence i.e. they make decisions related to routing, such as path finding. Every MARI node has a group of member nodes connected to it, usually in its one-hop neighborhood. The responsibility of every MARI node is

Author α : Prof of ECE, RGM College of Engineering, Nandyal, kurnool (dt), India. E-mail : mvsraj@yahoo.com

to make necessary communication with any member node connected to itself or with other MARI nodes (through Gateways) within the network, for both transmission and reception of the packets. MARI nodes are selected or formed by a procedure that is explained later in this chapter.

b) Gateway Nodes

The Gateway nodes [16] having sufficient power level are selected by the MARI nodes such that they can be used to forward packets between MARI nodes. Any two adjacent MARI nodes (within two-hop distance usually) in the network are connected through the concerned Gateway node only. Gateway nodes do not have routing intelligence. The MARI nodes select these Gateway nodes, according to the procedure outlined later. *The MARI and the Gateway nodes stay continuously awake to route the packets of other member nodes.*

c) Member Nodes

A member node is a non-MARI and non-Gateway node. These are the nodes, which want to communicate with each other [16,17]. Every member node is connected to one of the MARI nodes (some kind of belonging or bonding) through which it transmits or receives the packets. The member nodes wake up only at certain specified time epochs, and for very short periods, during any given beacon period T. When a member node wakes up and if it does not have to transmit or receive data, then it goes to sleep mode again, after a brief period. This is the main principle behind the power-efficient operation of the network. The wake-up time epochs of each member node are determined apriority (pre-determined). In our simulation of the operation of an adhoc wireless network, this is accomplished with the help of pseudo-random number generator. Also, these wake-up time epochs of a member node are known to its corresponding MARI node and its one-hop neighbor nodes, through the WAKEUP messages that are exchanged at the beginning of a beacon period. Thus, the member node can remain in power saving sleep mode for most of the time [6,11], especially when it is not actively sending or receiving packets. The packets are routed over the virtual backbone consisting of MARI nodes and Gateway nodes, which are awake continuously. This is the main power-saving advantage of the topology that is suggested and nurtured in this thesis.

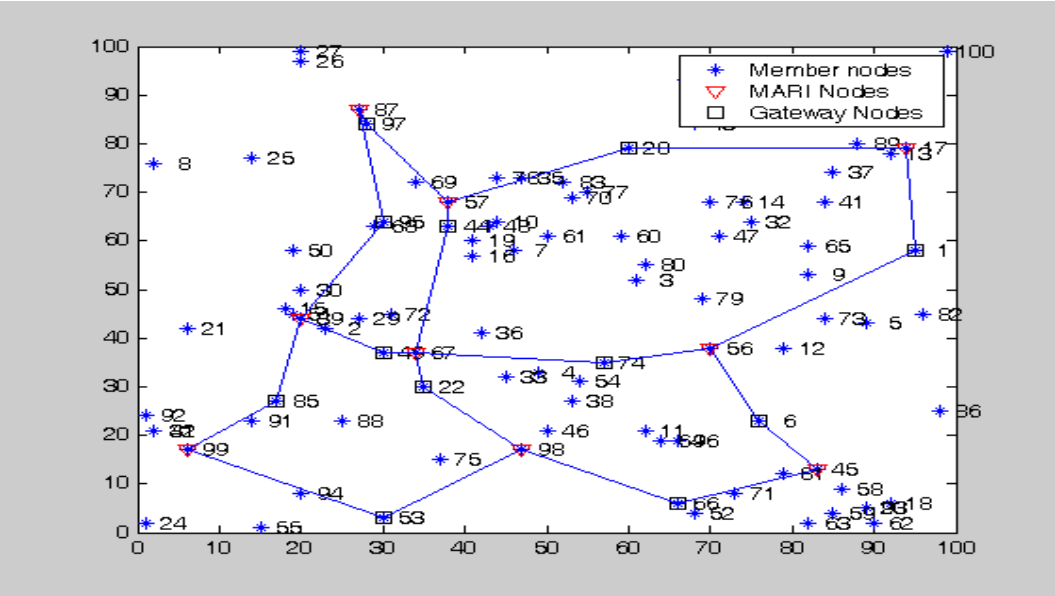


Fig.1: Random distribution of 100 nodes in the adhoc wireless network

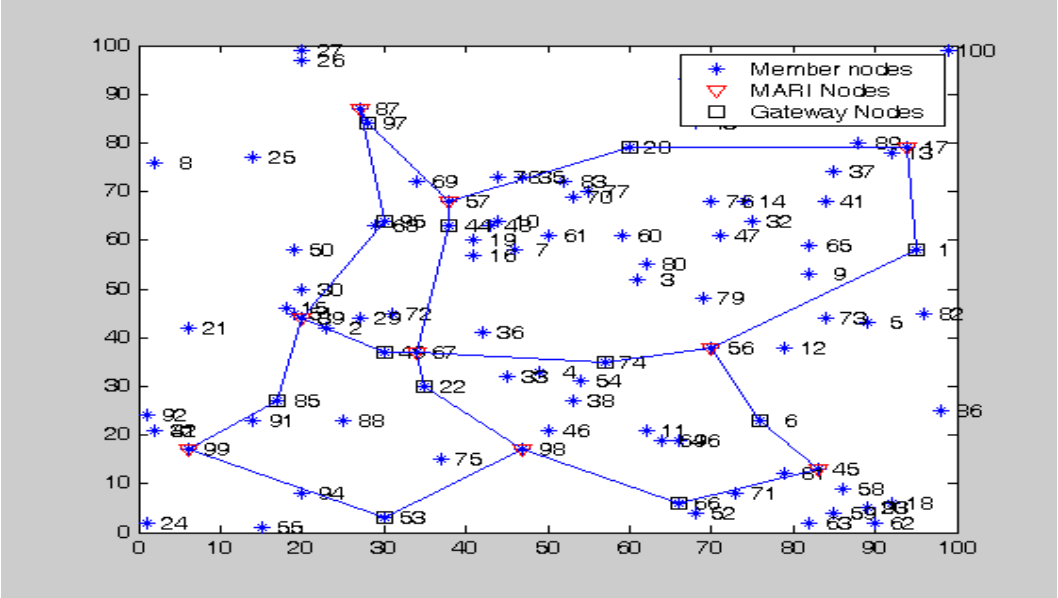


Fig. 2 : Adhoc network with MARI nodes, Gateway nodes and member nodes

The Fig.2 is the resultant after executing the following algorithms:

(1) MARI Placement algorithm and
(2) Gateway node selection algorithm

From the fig.2 it is clear that the number of nodes in the virtual backbone is 20% to 25% only. For an example, the list of MARI nodes, Gateway nodes and member nodes for the given MARI Topology network is shown in the table.1. From the table it is clear that the number of MARI nodes are: 09, number of Gateway nodes are: 12, and the number of member nodes are: 79.

File Edit View Web Window Help

```
Mari Nodes
     2    26    33    41    48    56    72    80    85

Gateway Nodes
     3    12    16    18    19    22    27    54    64    93    94   100

Member Nodes

     1     4     5     6     7     8     9    10    11    13    14    15    17    20    21    23

    24    25    28    29    30    31    32    34    35    36    37    38    39    40    42    43

    44    45    46    47    49    50    51    52    53    55    57    58    59    60    61    62

    63    65    66    67    68    69    70    71    73    74    75    76    77    78    79    81

    82    83    84    86    87    88    89    90    91    92    95    96    97    98    99
```

Table.1: List of MARI nodes, Gateway nodes and member nodes

In our simulation, we have considered that the nodes are operating in one of the four modes and their power consumptions are listed in table-2.

Mode	Transmit	Receive	Idle	Sleep
Power Consumption	1400mW	1000mW	830mW	130mW

Table. 2: Shows the amount of power consumption value by each node based on their mode of operation

III. Results

We have used MATLAB 7.0 for the simulation of results. In this section we have shown the analysis of adhoc wire less network with MARI topology. The results are compared with the existing flat topology. The parameters we considered for analysis and evolution, and their respective results are given below:

a. Power consumption of the network as number of nodes in the network increases. (fig-3)
b. Number of nodes in the backbone as the number of nodes in the network increases is shown in fig.4.
c. Overhead in each packet is shown in fig.5.

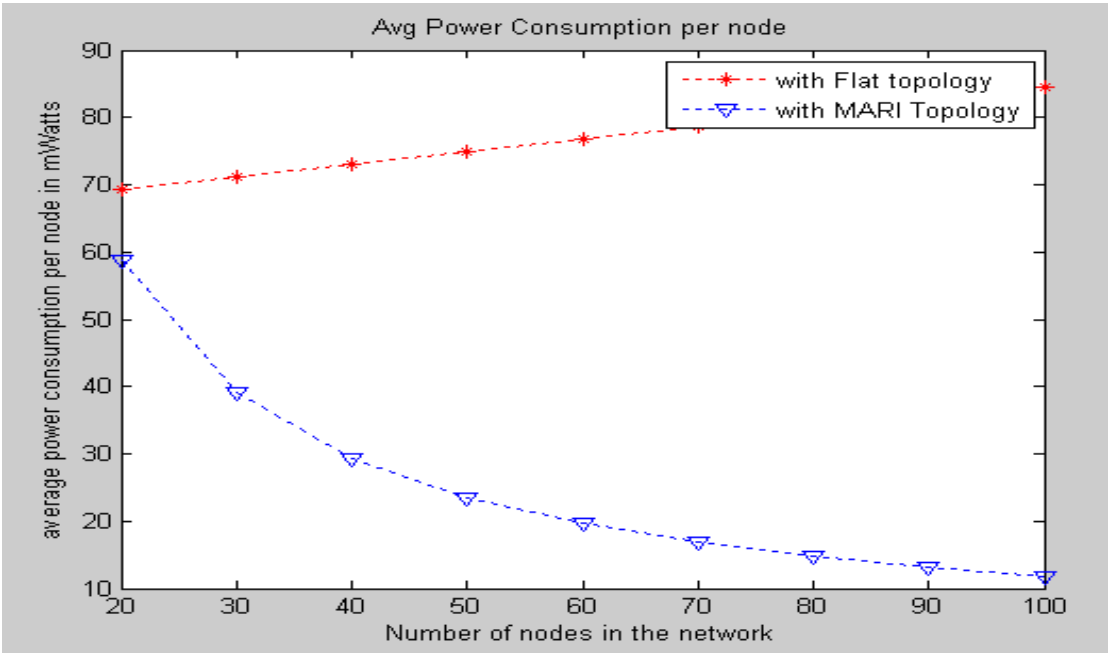


Fig. 3: Power consumption of the network as number of nodes in the network increases

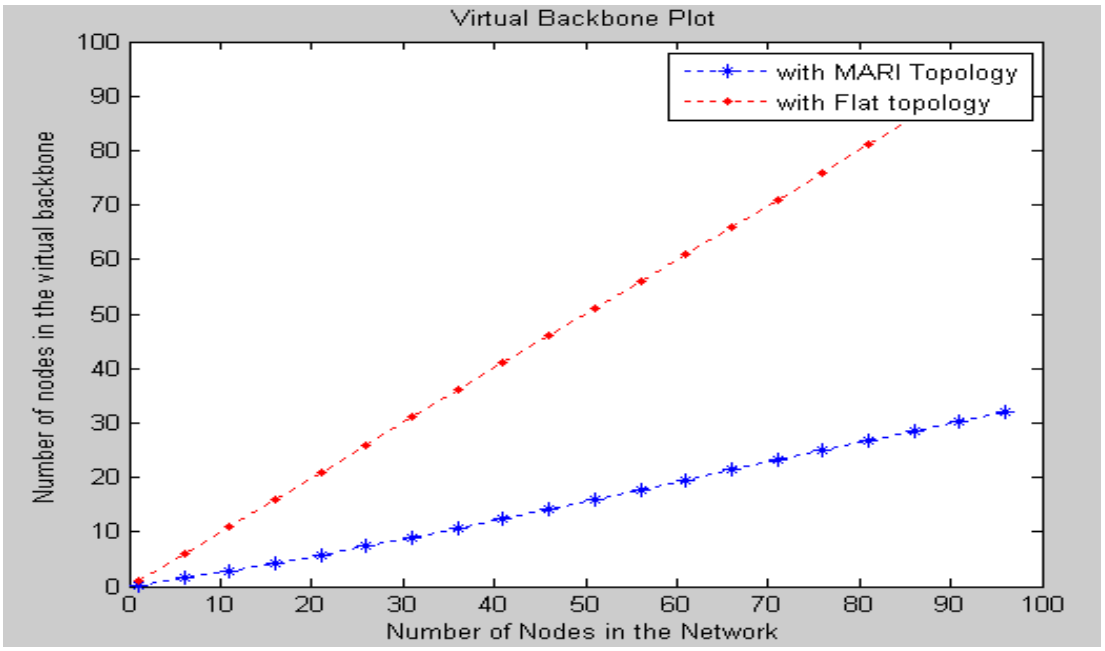


Fig.4: Number of nodes in the backbone as the number of nodes in the network increases

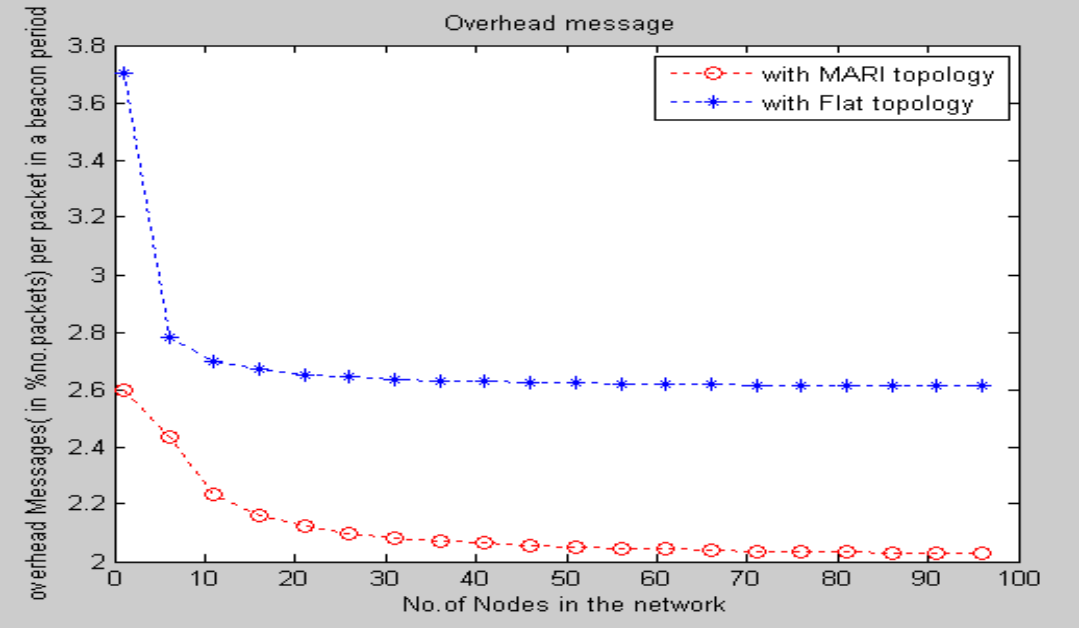


Fig.5: overhead in each packet per node

IV. Conclussions

The performance evaluation of the implemented wireless network is carried out in order (i) to demonstrate the successful operation of the MARI topology concept, (ii) to compare its performance to that of an equivalent (in size) flat-topology network, (iii) to prove the point that the MARI topology performs a way better than an equivalent flat-topology. In our illustration and demonstration, the performance measures that we have considered for simulation study are, (i) the number of backbone nodes as a proportion of the total number of nodes in the network, (ii) overhead messages, and (iii) average power consumption in the network. Analysis is also done in the following cases:

1. Keeping the data packet size and beacon period constant.
2. Variable data packet size with constant beacon period.
3. Fixed data packet size with variable beacon period.

V. Further Scope

(1) Management protocols for multicasting (one source to Many number of destinations simultaneously) can be designed upon MARI topology or with some further and appropriate modifications to the MARI topology. Load distribution and load balancing among the paths in the network can be considered.

(2) Performance study for multi-access level ($l > 1$) is another important topic. When the multi-access level increases, the power dissipation and the throughput increase. Therefore, there may exist an 'optimal' multi-access level in a given context and under certain conditions. Finding that optimal multi-access level can be a very good topic for R&D.

(3) Security levels on each packet, path and node can be implemented, with analysis of security by simulation or bench marking.

Bibliography

1. Baker, Marti, Giuli, and Lai Baker Data/Voice Communication over a Multihop, Mobile, High Frequency Network. In proceedings of the IEEE Military Communications Conference (MILCOM'97), Nov1997.
2. Buttyan and Habaux "Packet dropping in the MANET based on their malicious property of the nodes", In Proceedings of the 4th ACM International Symposium on Mobile Adhoc Networking and Computing, (MobiHoc2003), June 2003.
3. Halpem. J.Y and Li. L "Minimum-energy mo-bile wireless networks revisited," in IEEE Inter-national Conference on Communications, June2001.
4. Hass. Z.J, "Guest Editorial: Wireless Adhoc Networks", IEEE Journal on Selected Areas of Communications, Volume 17, No. 8, pp.1329, august 1999.
5. Hu Y.C., Johnson. D, Jetcheva J.G and Maltz D.A. "The Dynamic Source Routing Protocol for Mobile Adhoc Networks", Mobile Ad-hoc Network (MANET) Working Group, IETF, February 2002.
6. Jung E.-S and Vaidya N. H "A power control MAC protocol for ad-hoc networks," in ACM MOBICOM, 2002.
7. Kawadia. V, Kumar P. R., Sreenivas R. S. and Narayanaswamy. S "Power Control in Ad-Hoc Networks: Theory, Architecture, Algorithm and Implementation of the COMPOW Protocol," in Proceedings of European Wireless, pp. 156{62, Feb. 2002.

8. Lloyd E.L, Liu.R, Marathe.V, Ramanathan.R and Ravi S. S. Algorithmic Aspects of Topology Control Problems for Adhoc Networks," in Mobihoc, EPFL Lausanne, Switzerland, June 2002.
9. Meng T. H. and Rodoplu. V Minimum energy mobile wireless networks," in IEEE Journal on Selected Area on Communications, Vol. 17, No.8,pp 413-418 August 1999.
10. Perkins C.E Adhoc networking, Addison-Wesley ,Boston, 2001
11. Raghavendra C. S. Singh. S "Power efficient MAC protocol for multihop radio networks," in The Ninth IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, pp. 153–157,1998.
12. Ramanathan. R and Rosales - Hain.R "Topology control of multihop wireless networks using transmit power adjustment," in Proceedings of INFOCOM, pp. 404–413,2000.
13. Broch. J, et'al "A performance comparison of multi-hop wireless adhoc network routing protocols". In Proceedings of MOBICOM 1998, pp-1998.
14. Sonja . B and Yves Le Boudec. J Nodes Bearing Grudges: Towards Routing Security, Fairness, and Robustness in Mobile Adhoc Networks. In Proceedings of the Tenth Euro micro Workshop on Parallel, Distributed and Network-based Processing, pages 403 – 410, Canary Islands, Spain, IEEE Computer Society, pp-January2002.
15. Sonja . B and Yves Le Boudec.J Cooperative routing in mobile adhoc networks: Current efforts against malice and selfishness. In Proceedings of Mobile Internet Workshop. Informatik 2002. Dortmund, Germany, pp-October 2002.

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 12 Issue 10 Version 1.0 May 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Energy Efficient, Secure and Stable Routing Protocol for MANET

By Sunil Taneja & Ashwani Kush

Aruna Asaf Ali Government Post Graduate College, Haryana, India

Abstract - Mobile Adhoc Network (MANET) is characterized by mobile hosts, dynamic topology, multi-hop wireless connectivity and infrastructureless ad hoc environment. The adhoc environment is accessible to both legitimate network users and malicious attackers. Moreover, as the wireless links are highly error prone and can go down frequently due to mobility of nodes, therefore, energy efficient, secure and stable routing over MANET is still a very critical task due to highly dynamic environment. In this research paper, an effort has been done to combine these factors of security, power and stable routing by proposing a new protocol EESSRP (Energy Efficient, Secure and Stable Routing Protocol). An experimental analysis of proposed protocol has been carried out using network simulator NS-2.34. An effort has been made to perform analysis using random way point mobility model. The results have been derived using self created network scenarios for varying number of mobile nodes. The performance metrics used for evaluation are packet delivery ratio, average end to end delay, throughput, normalized routing load and packet loss. It has been concluded that the proposed protocol i.e. EESSRP provides energy efficient, secure and stable routing strategy for mobile adhoc networks.

Keywords : *EESSRP, Energy Efficient, MANET, Protocol, Routing, Secure, Stable.*

GJCST-E Classification: *C.2.1*

Strictly as per the compliance and regulations of:

Energy Efficient, Secure and Stable Routing Protocol for MANET

Sunil Taneja [α] & Ashwani Kush [σ]

Abstract - Mobile Adhoc Network (MANET) is characterized by mobile hosts, dynamic topology, multi-hop wireless connectivity and infrastructureless ad hoc environment. The adhoc environment is accessible to both legitimate network users and malicious attackers. Moreover, as the wireless links are highly error prone and can go down frequently due to mobility of nodes, therefore, energy efficient, secure and stable routing over MANET is still a very critical task due to highly dynamic environment. In this research paper, an effort has been done to combine these factors of security, power and stable routing by proposing a new protocol EESSRP (Energy Efficient, Secure and Stable Routing Protocol). An experimental analysis of proposed protocol has been carried out using network simulator NS-2.34. An effort has been made to perform analysis using random way point mobility model. The results have been derived using self created network scenarios for varying number of mobile nodes. The performance metrics used for evaluation are packet delivery ratio, average end to end delay, throughput, normalized routing load and packet loss. It has been concluded that the proposed protocol i.e. EESSRP provides energy efficient, secure and stable routing strategy for mobile adhoc networks.

Keywords : EESSRP, Energy Efficient, MANET, Protocol, Routing, Secure, Stable.

I. Introduction

MANET is self-organizing, rapidly deployable, and requires no fixed infrastructure. An Adhoc wireless network is a collection of mobile devices equipped with interfaces and networking capability. It is adaptive in nature and is self organizing. A formed network can be de-formed and again formed on the fly and this can be done without the help of system administration. Each node may be capable of acting as a router. Applications include but are not limited to virtual classrooms, military communications, emergency search and rescue operations, data acquisition in hostile environments, communications set up in exhibitions, conferences and meetings, in battle field among soldiers to coordinate defence or attack, at airport terminals for workers to share files etc. Although security has long been an active research topic in wired networks, the unique characteristics of Adhoc networks present a new set of nontrivial challenges to security design. These challenges include open network architecture, shared wireless medium, stringent resource constraints, and highly dynamic topology. Consequently, the existing security solutions for wired networks do not directly apply to the Adhoc environment. The main goal of the security solutions for an Adhoc network is to provide security services, such as authentication, confidentiality, integrity, anonymity and availability to mobile users [2]. One distinguishing characteristic of this network from the security design perspective is the lack of a clear line of defense. Unlike wired networks that have dedicated routers, each mobile node in an adhoc network may function as a router and forward packets for other peer nodes. The wireless channel is accessible to both legitimate network users and malicious attackers. In such an environment, there is no guarantee that a path between two nodes would be free of malicious nodes, which would not comply with the employed protocol and attempt to harm the network operation. Another major hurdle in communication via Adhoc networks is their power limitations. As most of them use battery power and also are moving so there is always limitation of battery power. A new scheme has been proposed here to incorporate security and power features in adhoc networks. The scheme takes care of basic security needs and uses concept of Hash Key generation to attain the goal of security. It uses route table entry for its power status. The work is an extension of earlier work done [3, 4] in the fields of power, security and stability. The scheme has been incorporated on the refined version of SSRP (Stable and Secure Routing Protocol) [3] and AODV (Adhoc On-Demand Distance Vector Routing Protocol) [5].

II. Energy Efficient and Stable Routing

An ad hoc network consists of hosts communicating among themselves with portable radios. This network can be deployed without any wired base station or infrastructure support where routes are mainly multi-hop because of the limited radio propagation range. The nodes in an ad hoc network are constrained by battery power for their operation. To route a packet from a source to a destination involves a sufficient number of intermediate nodes. Battery power of a node is a precious resource that must be used efficiently in order to avoid early termination of a node or a network. One distinguishing feature of Energy Efficient ad hoc

Author α : Department of Computer Science, Smt. Aruna Asaf Ali Government Post Graduate College, Kalka-133 302, Haryana, India.
E-mail : suniltaneja.iitd@gmail.com
Author σ : Department of Computer Science, University College, Kurukshetra University, Kurukshetra-132 119, Haryana, India.
E-mail : akush20@gmail.com

routing protocol is its use of Power for each route entry. Given the choice between two routes to a destination, a requesting node is required to select one with better power status and more active.

Efficient battery management [6, 7, 8], transmission power management [9, 10] and system power management [11, 12] are the major means of increasing the life of a node. These management schemes deal in the management of energy resources by controlling the early depletion of the battery, adjust the transmission power to decide the proper power level of a node and incorporate low power consumption strategies into the protocols. Typical metrics used to evaluate ad hoc routing protocols are shortest hop, shortest delay and locality stability. However, these metrics may have a negative effect in MANETs because they result in the over use of energy resources of a small set of nodes, decreasing nodes and network lifetime. The energy efficiency of a node is defined by the number of packets delivered by a node in a certain amount of energy.

A few reasons for energy management in MANETs are:

a) Ad hoc networks have been developed to provide communication for an environment where fixed infrastructure cannot be deployed. Nodes in ad hoc networks have very limited energy resources as they are battery powered.
b) In so many situations like hostile territory, it is very difficult or almost impossible to replace the battery or recharge it.
c) There is no central coordinator in case of ad hoc networks as a base station in cellular networks.

Therefore ad hoc networks work on the concept of multi-hop routing in which intermediate nodes play the role of the relay nodes. If the relay traffic is very high, it leads to rapid depletion of a node and if the traffic is negligible upon a node that leads to the partitioning of a network. If the battery size is very small, it decreases the lifetime of a node and if battery size of a node is large, it increases the weight of the mobile node. So to keep the standard small size of a battery, energy management techniques are required to utilize it efficiently. Optimal value selection for transmitting a packet is difficult but as this transmission power increases, it increases the consumption of the battery but the connectivity increases. This increases the number of paths to the destination. Therefore selection of the transmission power should be done in order to reduce the consumption of the battery power so as to maximize the simultaneous packet transmission and preserve connectivity.

Energy control algorithms [13, 14, 15] are very useful for the systems in which the available bandwidth is shared among all the users. Reduction in transmission power increases frequency reuse, which leads to better channel reuse. Although developing battery efficient systems that have low cost and complexity, remains a crucial issue. Efficient battery aware protocol is the need of today's ad hoc networks. Designing smart battery packs that can select appropriate battery discharge policies under different load conditions is a challenging problem. Other issues that exist at the physical layer includes efficient battery scheduling techniques[15] selection of an optimal transmission power for the nodes and finding the appropriate time duration for switching off the nodes . Investigations at data link layer are; addressing the issues of relay traffic, such as finding an optimal strategy that decides the amount of allowable relay traffic for a node. Developing battery aware MAC algorithms for the nodes that increase the lifetime of the nodes is an important issue. Finally, at the network layer designing of an efficient routing algorithm that increases the network lifetime by selecting an optimal relay node.

The network layer can aid in the conservation of energy by reducing the power consumed for two main operations, namely, communication and computation. The communication power consumption is mainly due to transmission and reception of bits. Whenever a node remains active, it consumes power. Even when the node is not actively participating in communication, but is in the listening mode waiting for the packets, the battery keeps discharging. The computation power consumption refers to the power spent in calculations that take place in the nodes for routing and other decisions. The following section discusses some of the power-efficient routing algorithms. In general, a routing protocol which does not require large tables to be downloaded or greater number of calculations is preferable, the amount of data compression before transmission decreases the power consumed for communication although the number of computation tasks increases. Since the energy required per bit for communication is hundred times compared to computation, data compressed is preferred. MANETs allow anywhere, any time network connectivity with complete lack of control, ownership and regulatory influence. Each node in a MANET participates in the routing function. To establish communication among different nodes, the "death" of few nodes is possible due to energy exhaustion.

In traditional routing algorithms, routes are constructed on the basis of shortest path but these protocols are not aware of the energy consumed for the path setup or maintenance. Shortest path algorithm may result in a quick depletion of the energy of nodes along the heavily used routes.

Designing energy aware routing protocols has attracted a lot of attention for prolonged network operational time. Design objective of energy aware protocols is to select energy efficient routes and simultaneously minimizing the overhead incurred in the selection of the routes. Some routing algorithms given

by [16, 17] can optimize the energy use with a global perspective. But these algorithms incur expensive overheads for gathering, exchanging and storing the state information. These algorithms can be improvised in order to make them scalable. For this purpose a localized topology controlling algorithm [16] or a distributed energy aware dominating set generating algorithm [18] can be applied on nodes and a traditional base algorithm like AODV or DSR may be run in the network. This kind of protocol design can reduce the communication overheads consumed for route discovery. Implementation of this kind of approach requires the knowledge of one or two hop neighbours at the nodes. This requirement can consume bandwidth and use energy for gathering such information at nodes constantly in dynamic networks. Some algorithms [16, 19, 20] work without assuming any topological knowledge at nodes and they can avoid the proactive overheads required for topological information. These kind of on demand approaches are required for energy efficient paths. Due to the reactive nature of on demand protocols, these are more energy efficient in MANETs and therefore in this chapter, only on demand protocols have been analyzed on the anvil of their energy, so that selection of a better base protocol may lead to find energy efficient paths. A lot of work has been carried in the direction of energy aware routing. They modify either AODV or DSR, which are taken as the base protocol. An Energy and Delay Constrained Routing in MANETs have been proposed by Laura et al. [21], in which energy saving and timely delivery of data packets is incorporated into the route discovery phase to select paths with lower cost. This algorithm utilizes two metrics, residual energy and queue length at each node. Buffer information is considered as a traffic load characteristic and its use is to limit the battery power consumption and end to end delay. Chen et al. [22] have proposed an Energy Efficient AODV for Low Mobility Ad hoc Networks, in which the node energy consumption of the overall network is reduced by dynamically controlling the transmission power by utilizing a novel route cost metric. Three extensions to the traditional AODV protocol, named Local Energy Aware Routing (LEAR-AODV), Power Aware Routing (PAR-AODV) and Lifetime Prediction Routing (LPR-AODV) have been proposed by [23], for balanced energy consumption in MANETs. These algorithms use energy consumption as a routing metric and try to reduce the nodes energy consumption by routing packets using energy optimal routes. Li et al. [16] have proposed an algorithm to maximize the network life time by balancing the energy draining rates among nodes using precise global state information. Narayanaswami et al. [24] have designed an approach named COMPOW, which works to find the minimal common value of node transmission range to maintain the network connectivity. COMPOW attempts to satisfy three major objectives. Increasing the battery lifetime of all the nodes, increasing the traffic carrying capacity of the network and reducing the contention among the nodes. The main reason behind the need for an optimal transmit power level for the nodes in MANETs is that battery power is saved by reducing the transmission range of the node. It has been proved by Kawadia et al. [36] that the COMPOW protocol works only in a network with a homogeneous distribution of nodes. CLUSTERPOW is an extension of COMPOW for non-homogeneous dispersion of the nodes. It is a power control clustering protocol in which each node runs a distributed algorithm to choose the minimum power p to reach the destination through multiple hops. Unlike COMPOW, where all the nodes of the network agree on a common power level, in CLUSTERPOW the value of p can be different for different nodes and is proved to be in non-increasing sequence toward the destination. An extended approach to COMPOW is used to reduce the energy consumed in packet forwarding for heterogeneous networks. These approaches introduce the excessive overheads and they have the scalability issue. Some pure on demand energy aware approaches have also been designed. Xue et al. [25] have introduced a location aided routing with energy awareness. In this approach each node with a packet to forward performs per hop power aware forwarding with the help of location information of the destination, neighbouring nodes and the node itself. With this approach good energy efficiency can be achieved but at the cost of more resource consumption for updating and collecting the information in the dynamic environment of MANETs.

III. Secure Routing

Security is an important issue for ad hoc networks, especially for those security-sensitive applications. It has become a primary concern in order to provide protected communication between mobile nodes in a hostile environment. The salient features of ad hoc networks pose both challenges and opportunities in achieving the aforementioned goals. *First,* use of wireless links renders an ad hoc network susceptible to link attacks ranging from passive eavesdropping to active impersonation, message replay, and message distortion. Eavesdropping might give an adversary access to secret information, violating confidentiality. Active attacks might allow the adversary to delete messages, to inject erroneous messages, to modify messages, and to impersonate a node, thus violating availability, integrity, authentication, and non-repudiation. *Secondly*, nodes, roaming in a hostile environment e.g. in a battlefield with relatively poor physical protection, have non-negligible probability of being compromised. Therefore, one should not only consider malicious attacks from outside a network, but also take into account the attacks launched from within

the network by compromised nodes. Therefore, to achieve high survivability, ad hoc networks should have a distributed architecture with no central entities. Introducing any central entity into our security solution could lead to significant vulnerability; that is, if this centralized entity is compromised, then the entire network is subverted. *Thirdly,* an ad hoc network is dynamic because of frequent changes in both its topology and its membership. Trust relationship among nodes also changes, for example, when certain nodes are detected as being compromised. Unlike other wireless mobile networks, such as mobile IP, nodes in an ad hoc network may dynamically become affiliated with administrative domains. Any security solution with a static configuration would not suffice. It is desirable for our security mechanisms to adapt on-the-fly to these changes. *Finally,* an ad hoc network may consist of hundreds or even thousands of nodes. Security mechanisms should be scalable to handle such a large network.

These challenges motivate for building multi fence security solutions that achieve both broad protection and desirable network performance. Basically, the complete security solution should span both layers, and encompass all three security components of prevention, detection, and reaction. The dilemma is that how should it be judged whether the mobile ad hoc network is secure or not. Some of the main security attributes [26, 27] that are used to inspect the security state of the mobile ad hoc networks are availability, integrity, confidentiality, authenticity, non repudiation, authorization and anonymity.

In mobile ad hoc networks, radio transmission is the most common means of communication. Eavesdropping on a node is far easier than in wired networks. Since intermediate nodes no longer belong to a trusted infrastructure, but may be eavesdroppers as well, consequent end-to-end encryption is mandatory. Next, as all nodes in an Ad hoc network cooperate in order to discover the network topology and forward packets, denial of service attacks on the routing function are very easy to mount. Nodes may create stale or wrong routes, creating black holes or routing loops. Furthermore, in ad hoc networks exists a strong motivation for non-participation in the routing system. Both the routing system and the forwarding of foreign packets consume a node's battery power, CPU time, and bandwidth, which are restricted in mobile devices. Consequently, selfish nodes may want to save their resources for own use. There are three main causes for a node not to work according to the common routing protocol. Malfunctioning nodes are simply suffering from a hardware failure or a programming error. Although this is not an attack, they may cause severe irritation in the routing system of an ad hoc network. Selfish nodes try to save their own resources, as described above. Malicious nodes are trying to sabotage other nodes or even the whole network, or compromise security in some way. Before developing a security framework that prevents selfish or malicious nodes from harming the network, it is worthwhile to first create a structured overview on what kinds of attacks are possible in ad hoc networks. Network security attacks [25, 26] are typically divided into two categories passive vs. active attacks which have already been discussed in previous chapter. MANETs are extremely vulnerable to attacks due to their dynamically changing topology, absence of conventional security infrastructures and open medium of communication, which, unlike their wired counterparts, cannot be secured with ease. MANET security involves authentication, key establishment and distribution, and encryption. Despite the fact that security of ad hoc routing protocols is causing a major roadblock in commercial applications of this technology, only a limited work has been done in this area. Such efforts have mostly concentrated on the aspect of data forwarding, disregarding the aspect of topology discovery. On the other hand, solutions that target route discovery have been based on approaches for fixed-infrastructure networks, defying the particular ad hoc network challenges. To address these concerns, several secure routing protocols have been studied and some of the popular secured protocols are ARAN [28], SEAD [29], SRP [30], SECURE AODV [31], SLSP [32], ARIADNE [33] and SAR [34].

IV. Proposed Algorithm

The proposed algorithm takes care of three core issues of energy efficient, secure and stable routing over mobile ad hoc networks is given below:

a) Secure Routing

In the proposed algorithm, secure routing has been implemented in three steps:

(i) Diffie-Hellman Algorithm of key exchange for generation of secret key
(ii) Apply hashing to generate subsequent keys over selected route
(iii) Encryption and Decryption using XOR operation

b) Energy Efficient and Stable Routing

In the proposed algorithm, energy efficient and stable routing has been implemented in five steps:

(i) The source node S broadcasts RREQ message containing threshold value Th.
(ii) At a neighbor node N, If En > ETh a reply message is sent otherwise no reply is sent
(iii) At the source node S, all reply messages are scanned. The neighbour with shortest active route is selected for forwarding the data and other nodes are stored as alternate nodes in the event of a link failure.

(iv) RREQ message is sent to the selected node and the selected node receives RREQ message. It forwards the same on the available active route.

(v) The destination node D sends back RREP on the reverse path. When S receives RREP, it means route is established and data is forwarded over the established route.

V. Performance Metrics

RFC 2501 describes a number of quantitative metrics that can be used for evaluating the performance of a routing protocol for mobile wireless ad-hoc networks. Some of these quantitative metrics [3, 35] are defined as follow:

a) Packet Delivery Fraction (PDF)

The packet delivery fraction is defined as the ratio of number of data packets received at the destinations over the number of data packets sent by the sources as given in equation (1). This performance metric is used to determine the efficiency and accuracy of MANET's routing protocols.

$$\text{Packet Delivery Fraction} = \frac{\text{Total Data Packets Received}}{\text{Total Data Packets Sent}} \times 100 \quad (1)$$

b) Average End-to-End Delay (AE2ED)

This is the average time involved in delivery of data packets from the source node to the destination node. To compute the average end-to-end delay, add every delay for each successful data packet delivery and divide that sum by the number of successfully received data packets as given in equation (2). This metric is important in delay sensitive applications such as video and voice transmission.

$$\text{Average End to End Delay} = \frac{\sum (\text{Time Received} - \text{Time Sent})}{\text{Total Data Packets Received}} \quad (2)$$

c) Network Throughput

A network throughput is the average rate at which message is successfully delivered between a destination node (receiver) and source node (sender). It is also referred to as the ratio of the amount of data received from its sender to the time the last packet reaches its destination. Throughput can be measured as bits per second (bps), packets per second or packet per time slot. For a network, it is required that the throughput is at high-level. Some factors that affect MANET's throughput are unreliable communication, changes in topology, limited energy and bandwidth.

d) Normalized Routing Load (NRL)

The normalized routing load is defined as the fraction of all routing control packets sent by all nodes over the number of received data packets at the destination nodes. In other words, it is the ratio between the total numbers of routing packets sent over the network to the total number of data packets received as given in equation (3). This metric discloses how efficient the routing protocol is. Proactive protocols are expected to have a higher normalized routing load than reactive ones. The bigger this fraction is the less efficient the protocol.

$$\text{Normalized Routing Load} = \frac{\text{Total Routing Packets Sent}}{\text{Total Data Packets Received}} \quad (3)$$

e) Packet Loss (PL)

Packet loss occurs when one or more packets being transmitted across the network fail to arrive at the destination. It is defined as the number of packets dropped by the routers during transmission. It can be shown by equations (4) to (6).

$$\text{Packet Loss} = \text{Total Data Packets Dropped} \quad (4)$$

$$\text{Packet Loss} = \text{Total Data Packets Sent} - \text{Total Data Packets Received} \quad (5)$$

$$\text{Packet Loss (\%age)} = \frac{\text{Total Packets Dropped}}{\text{Total Data Packets Sent}} \times 100 \quad (6)$$

In this research paper, performance of the proposed protocol EESSRP has been evaluated w.r.t. SSRP and AODV.

VI. Simulation Model

An effort has been carried out to develop a new protocol, EESSRP (Energy Efficient, Secure and Stable Routing Protocol). This protocol provides energy-efficient, secured and stable routing strategy for mobile ad hoc networks. The results have been derived by writing a *tcl* script and generating corresponding *trace* and *nam* files. Varying number of UDP connections/traffic agents have been used to analyze the traffic. The mobility model used is random waypoint model in a square area. The area configurations used are 750 meter x 750 meter for 20 nodes, 1000 meter x 1000 meter for 50 nodes and 1500 meter x 1500 meter for 80 nodes. The packet size is 512 bytes. The simulation run time is 500 seconds during analysis of 20 nodes, 700 seconds for 50 nodes and 950 seconds for 80 nodes. All simulation parameters have been summarized below in table 1.

Table 1: Simulation Parameters during analysis of EESSRP

Simulation Software	NS-2.34		
Channel	Wireless		
Mobility Model	Random Waypoint		
Frequency	915e+6		
Transmitted Signal Power	0.2818 W		
Power Consumption for Transmission	1.6 W		
Power Consumption for Reception	1.2 W		
Threshold	10 db		
System Loss Factor	1.0		
Data Rate	1 mbps		
Protocols	AODV, SSRP and EESSRP		
Packet size	512 byte		
Transmission Range	200 meter		
Traffic Agent	UDP		
Queue Length	150		
Number of Nodes	20	50	80
Simulation Time (seconds)	500	700	950
Area	750 × 750	1000 × 1000	1500 × 1500
Fixed Speed (meter/second)	5	5	5
Pause time (seconds)	100 to 500	100 to 500	100 to 950

a) Snapshots of Simulation Environment

An extensive simulation model having scenario of 20, 50 and 80 mobile nodes is used to study inter-layer interactions and their performance implications. Same scenario has been used for performance evaluation of EESSRP, SSRP and AODV protocols at one time. Some of the snapshots of trace and NAM files created using AODV, SSRP and EESSRP protocols for 50 nodes are shown in figure 1 to 6.

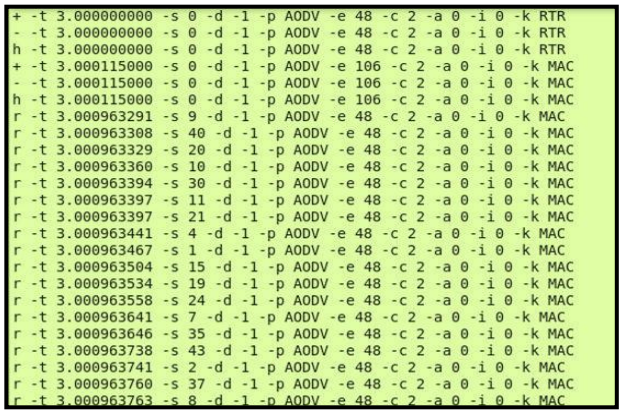


Figure 1: NAM File using AODV (50 Nodes)

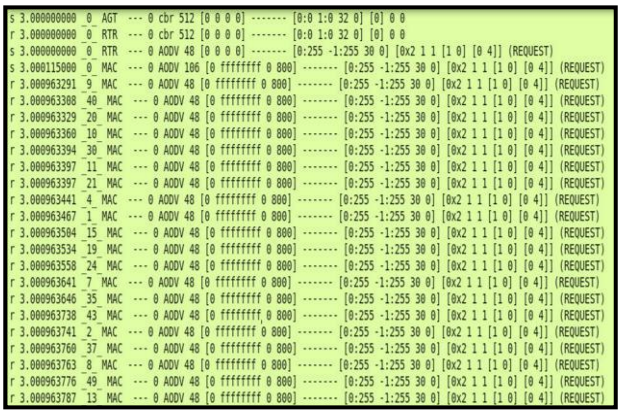


Figure 2: Trace File using AODV (50 nodes)

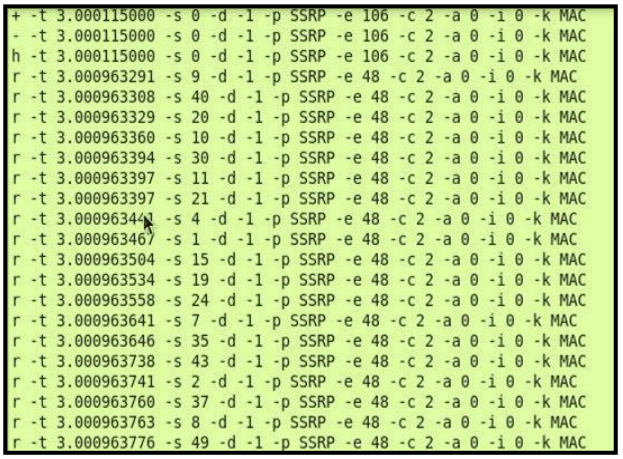


Figure 3 : NAM File using SSRP (50 Nodes)

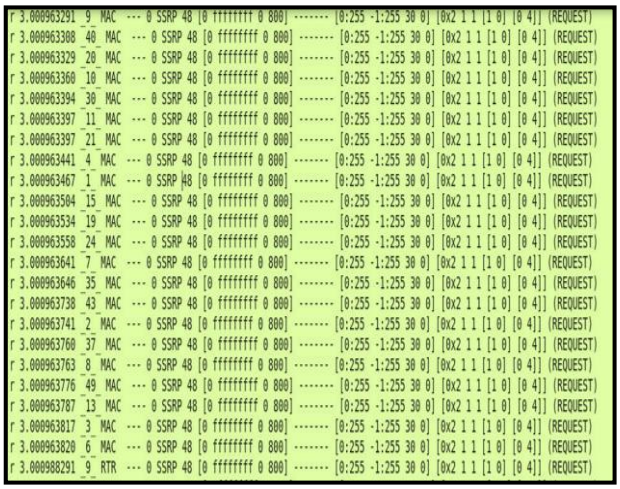


Figure 4: Trace File using SSRP (50 Nodes)

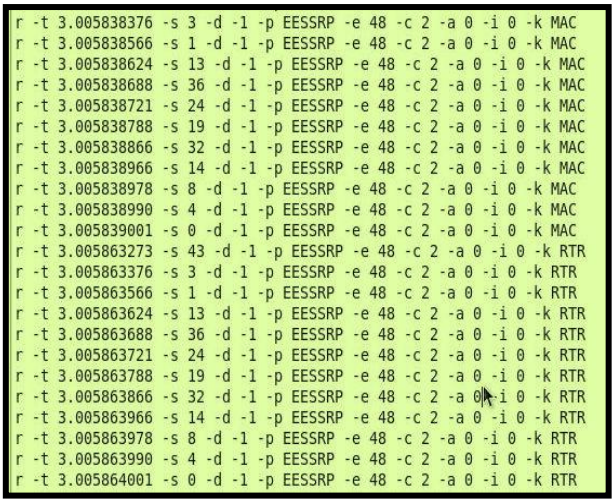


Figure 5 : NAM File using EESSRP (50 Nodes)

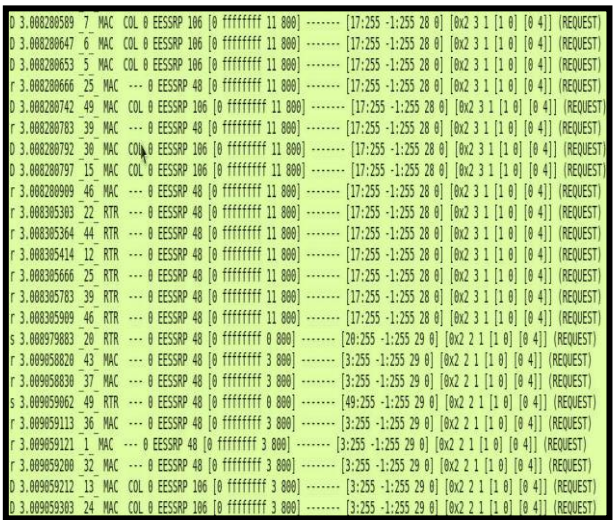


Figure 6 : Trace File using EESSRP (50 Nodes)

A graphical tool known as Network Animator is used to observe the visual representation of NAM files created during simulation of 50 nodes. The snapshots of visual representations taken at two different times t_1= 138.942153 Sec. and t_2= 138.974673 Sec. are given in figure 7 and 8.

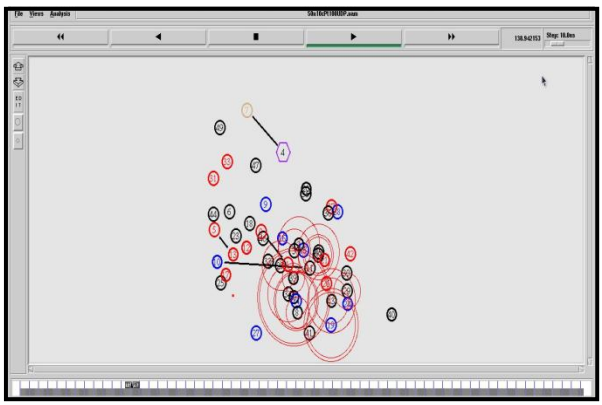


Figure 7 : Position at time t_1= 138.942153 Seconds (50 Nodes)

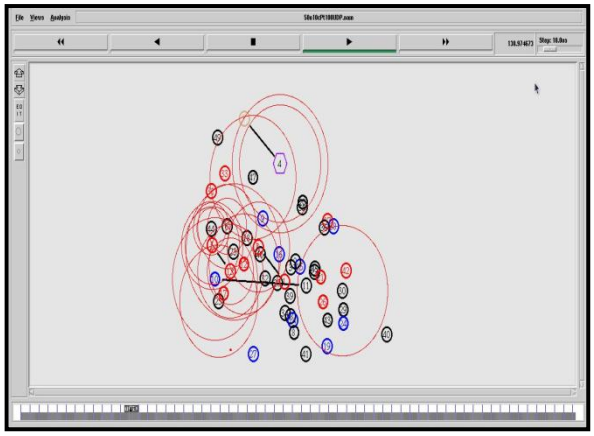


Figure 8 : Position at time t_2= 138.974673 Seconds (50 Nodes)

b) Simulation Results for 20 Nodes

All the performance metrics have been evaluated for EESSRP, SSRP and AODV protocols using 6 UDP connections. All nodes are moving at a fixed speed of 5 meters/second. Two malicious nodes have been introduced in the network scenarios which are moving at a speed of 1 meter/second. The pause time has been used as a varying parameter from 100 seconds to 500 seconds and the queue length is 150.

Figure 9 shows packet delivery fraction with respect to pause time. The observation is that EESSRP and SSRP gives almost same PDF but it is high than that of AODV. Therefore, EESSRP protocol outperforms AODV in terms of energy-efficient, secured and stable routing over MANET. In figure 10, average end to end delay has been presented with respect to pause time. When the pause time is 100 seconds, AODV has high average end to end delay than SSRP and EESSRP but after that AODV, SSRP and EESSRP gives almost same results. On an average, EESSRP outperforms AODV. The network throughput with respect to pause time has been shown in figure 11. The protocol having high network throughput is more efficient and in this figure, EESSRP gives high throughput than SSRP and SSRP gives high throughput than AODV. Therefore, EESSRP outperforms AODV and SSRP in terms of throughput. Figure 12 shows normalized routing load by varying pause time. The bigger this fraction is the less efficient the routing protocol. When the pause time is between 100 seconds to 300 seconds, AODV shows bigger NRL than SSRP and EESSRP but after that EESSRP, SSRP and AODV gives almost same results. On an average, EESSRP outperforms AODV and SSRP in terms of normalized routing load. In figure 13, the packet loss has been shown for both protocols. Higher the packet loss, less efficient is routing protocol and in this figure, AODV gives high packet loss than SSRP and EESSRP. Therefore, EESSRP outperforms than AODV and SSRP in terms of packet loss.

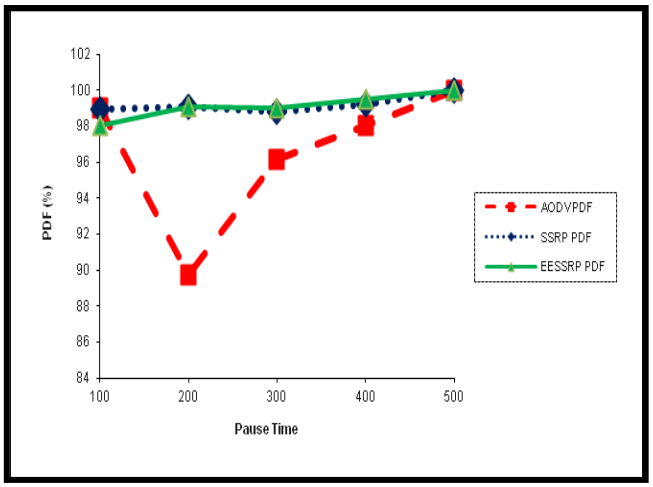


Figure 9 : Packet Delivery Fraction (20 Nodes)

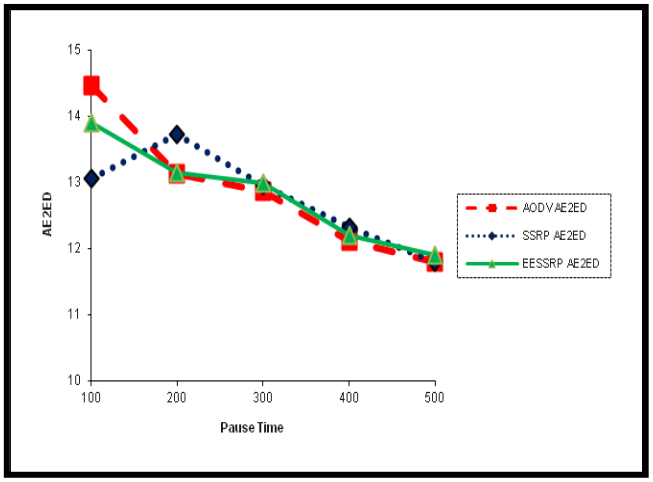


Figure 10 : Average End to End Delay (20 Nodes)

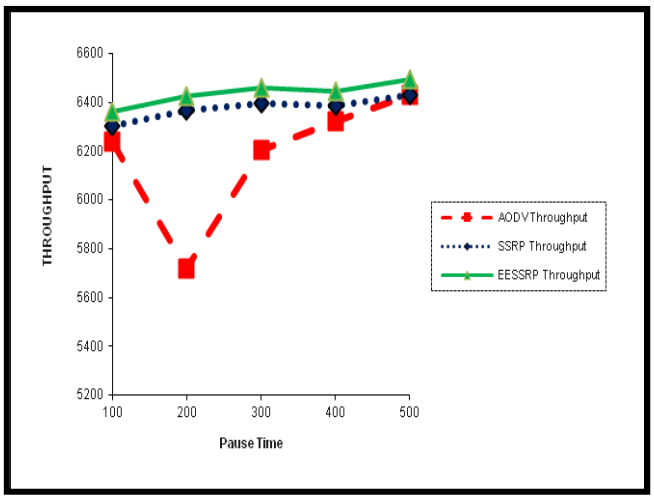


Figure 11: Network Throughput (20 Nodes)

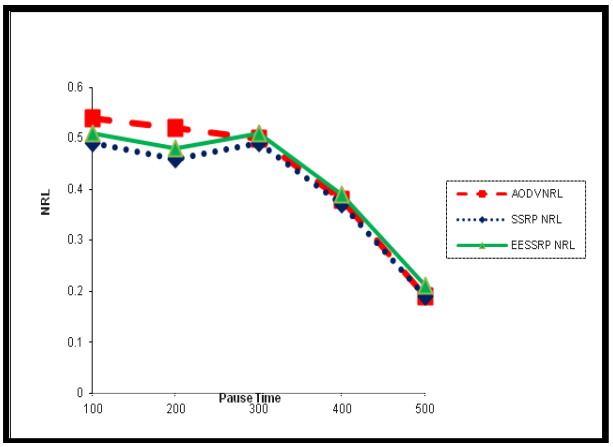


Figure12 : Normalized Routing Load (20 Nodes)

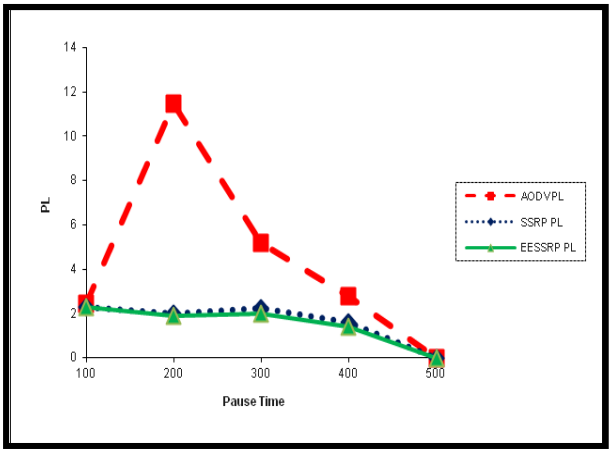


Figure 13 : Packet Loss (20 Nodes)

c) Simulation Results for 50 Nodes

All the performance metrics have been evaluated for EESSRP, SSRP and AODV protocols using 10 UDP connections. All nodes are moving at a fixed speed of 10 meters/second. Two malicious nodes have been introduced in the network scenarios which are moving at a speed of 5 meters/second. The pause time has been used as a varying parameter from 100 seconds to 700 seconds and the queue length is 150.

In figure 14, packet delivery fraction is shown with respect to pause time for EESSRP, SSRP and AODV. The observation is that EESSRP gives high packet delivery fraction that SSRP and SSRP gives high packet delivery fraction that AODV. Therefore, EESSRP protocol outperforms AODV in terms of better packet delivery.

In figure 15, average end to end delay has been presented with respect to pause time. When the pause time is between 100 seconds to 200 seconds, AODV has high average end to end delay than SSRP and EESSRP. When pause time is between 200 seconds to 400 seconds, EESSRP and SSRP has high average end to end delay than AODV. In end, when pause time is between 400 seconds to 500 seconds, EESSRP and SSRP has low average end to end delay than AODV.

Therefore, on an average, EESSRP almost touches AODV. Network throughput with respect to pause time has been shown in figure 16. EESSRP gives high throughput than SSRP and AODV. Therefore, EESSRP outperforms SSRP and AODV in terms of throughput.

Figure 17 shows normalized routing load by varying pause time. When the pause time is between 100 seconds to 300 seconds, AODV shows higher normalized routing load than SSRP and EESSRP but when the pause time is between 300 seconds to 400 seconds, EESSRP gives higher normalized routing load than SSRP and AODV. In end, EESSRP, SSRP and AODV give almost same results. Concluding, it is inferred that EESSRP outperforms AODV in terms of normalized routing load.

In figure 18, AODV shows high packet loss than SSRP and EESSRP. Therefore, EESSRP outperforms than AODV and SSRP.

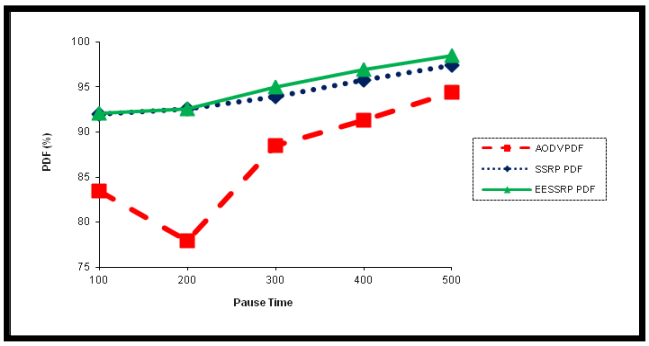


Figure 14 : Packet Delivery Fraction (50 Nodes)

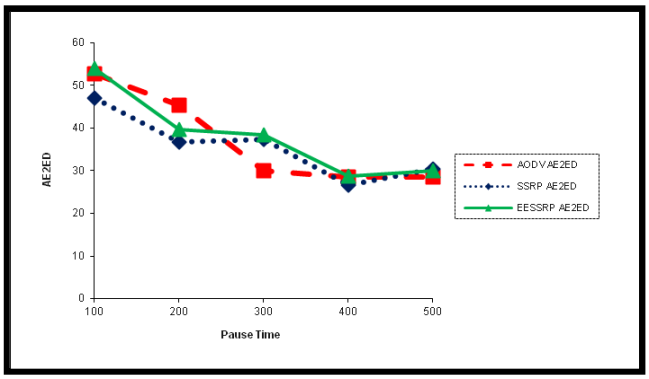


Figure 15 : Average END to End Delay (50 Nodes)

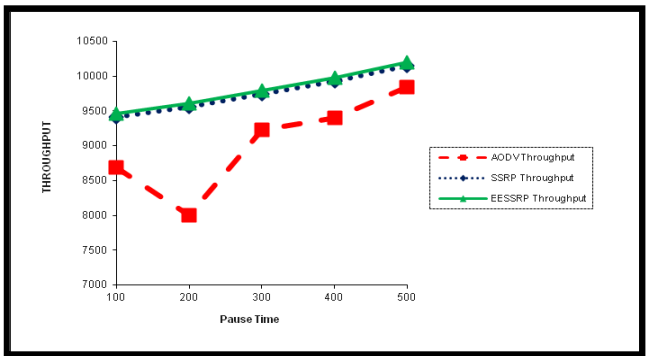


Figure 16 : Network Throughput (50 Nodes)

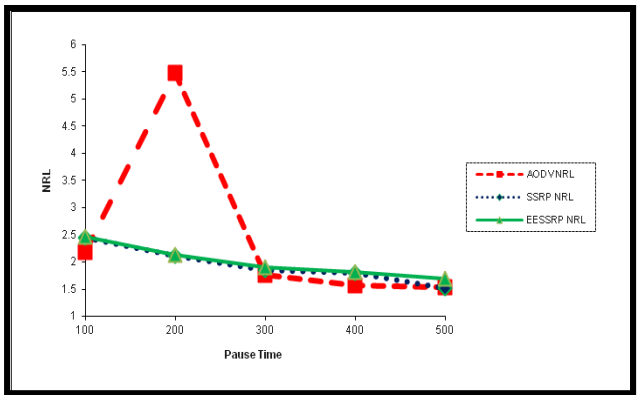


Figure 17 : Normalized Routing Load (50 Nodes)

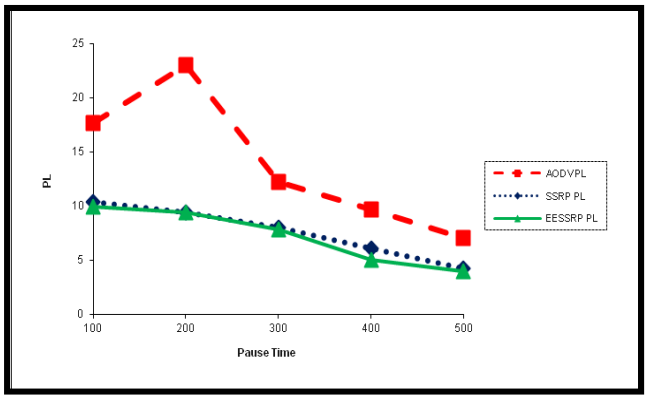


Figure 18 : Packet Loss (50 Nodes)

d) Simulation Results for 80 Nodes

All the performance metrics have been evaluated for EESSRP, SSRP and AODV protocols using 14 UDP connections. All nodes are moving at a fixed speed of 10 meters/second. Two malicious nodes have been introduced in the network scenarios which are moving at a speed of 5 meters/second. The pause time has been used as a varying parameter from 100 seconds to 950 seconds and the queue length is 150.

Figure 19 shows that packet delivery fraction for EESSRP and SSRP is much higher than that of AODV for all pause times and hence EESSRP outperforms AODV and SSRP in terms of better packet delivery. In figure 20, average end to end delay has been presented with respect to pause time. When the pause time is between 100 seconds to 675 seconds, AODV has high average end to end delay than SSRP and EESSRP but when it is between 675 seconds to 950 seconds, EESSRP and SSRP gives high average end to end delay than AODV. Concluding EESSRP outperforms AODV and SSRP initially but in end AODV starts outperforming SSRP and EESSRP. This issue is still under consideration. Network throughput with respect to pause time has been shown in figure 21. EESSRP gives high throughput than AODV and SSRP for all pause times and hence EESSRP outperforms AODV and SSRP in terms of better throughput.

Figure 22 shows normalized routing load by varying pause time. The bigger this fraction is the less efficient the routing protocol. When the pause time is between 100 seconds to 250 seconds, EESSRP and SSRP shows bigger NRL than AODV; when it is between 250 seconds to 400 seconds, AODV shows bigger NRL than SSRP and EESSRP. When pause time is between 400 seconds to 950 seconds, EESSRP and SSRP shows marginal bigger NRL than AODV. Although both the protocols give almost same results but still due to marginal difference between the results, on an average, AODV outperforms SSRP and EESSRP. In figure 23, the packet loss has been shown for both protocols with respect to varying pause time from 100 seconds to 950 seconds. In all cases, EESSRP gives very low packet loss than AODV and SSRP. So EESSRP outperforms AODV and SSRP.

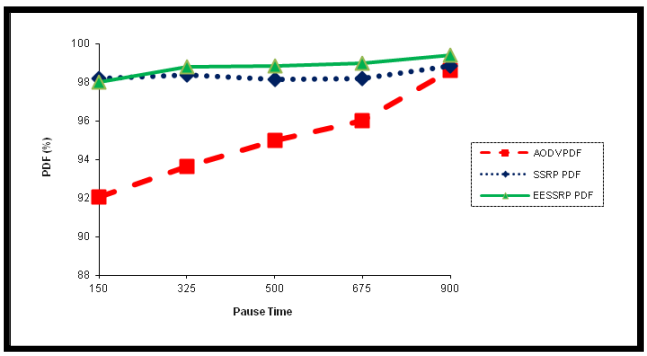


Figure 19 : Packet Delivery Fraction (80 Nodes)

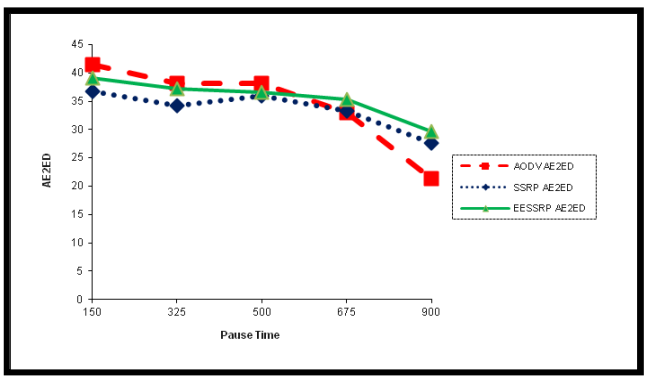


Figure 20 : Average End to End Delay (80 Nodes)

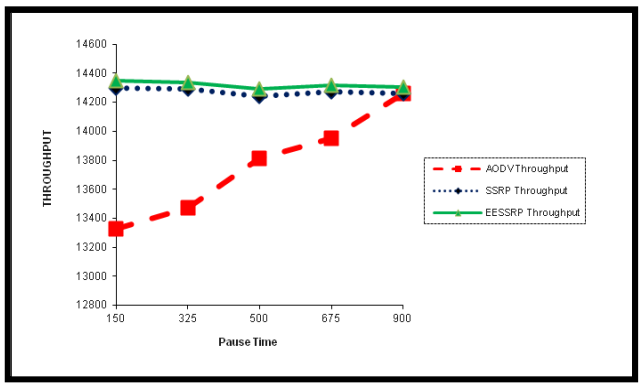


Figure 21 : Network Throughput (80 Nodes)

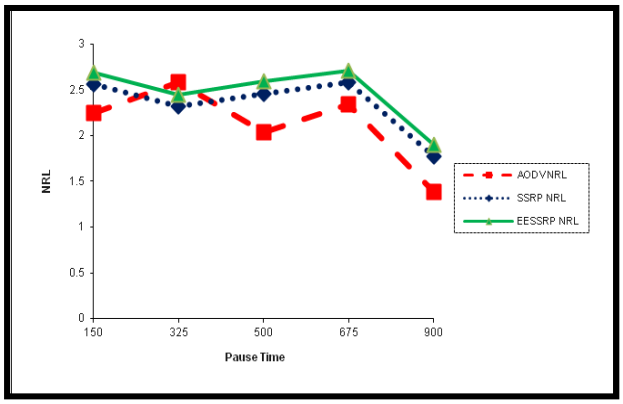


Figure 22 : Normalized Routing Load (80 Nodes)

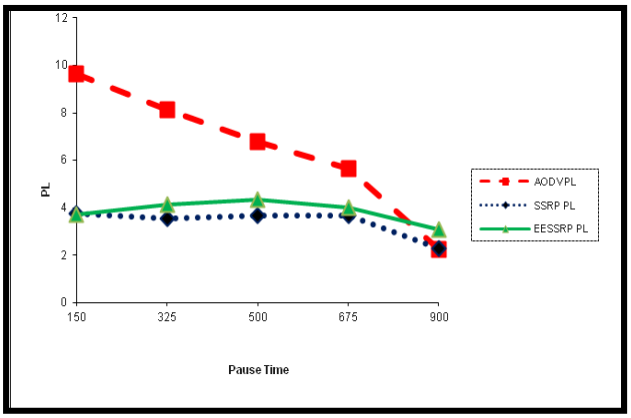


Figure 23 : Packet Loss (80 Nodes)

VII. Conclusion and Future Scope

Results have been derived from a series of experiments conducted on network simulator NS-2.34. The following conclusions have been made:

a) Energy Efficient

The proposed protocol, EESSRP, provides energy efficient routing over mobile adhoc networks in a very efficient way. It assumes that all nodes are capable of dynamically adjusting the transmission power used to communicate with other nodes. Battery power of a node is a precious resource that has been used efficiently in order to avoid early termination of a node or a network. The optimal route selection between source and destination is done on the basis of proper energy management. The proposed protocol balances energy efficient broadcast schemes in ad hoc network and maintains connectivity of mobile nodes.

b) Multifold Security Solution

The existing routing protocols are typically attack-oriented. They first identify the security threats and then enhance the existing protocol to conquer such attacks. Since the solutions are designed explicitly with certain attack models in mind, they work well in the presence of designated attacks but may collapse under unanticipated attacks. Therefore, a multifold network security solution has been developed in EESSRP that

offers multiple lines of defense against both known and unknown security threats and the performance of same has been evaluated with respect to AODV using various performance metrics viz. packet delivery fraction, average end to end delay, network throughput, normalized routing load and packet loss.

c) Robust and Stable

EESSRP satisfies the condition. It has been thoroughly checked many times using different scenes and changing loads. Since routers are located at different points, they can cause considerable problems when they fail. The proposed protocol takes care of the issue. The best routing algorithms is often the one that withstands the test of time and that proves stable under a variety of network conditions.

d) Best Packet Delivery Ratio

EESSRP is the best in terms of packet transmission. More packets are transmitted than any of the studied protocols. This is true even in case of changing scenario and fast moving nodes. So it is able to achieve one of the most important objectives of ad hoc networks as successful packet delivery.

e) Optimal Path

EESSRP selects the optimum path. Routing protocols use metrics to evaluate what path will be the best for a packet to travel. Using routing table entries and making choice between active and week nodes, it is able to select a path that is stable. This proves the optimality of the protocol.

f) Simple

EESSRP can easily be implemented and executed. The simulation studies have been conducted on Pentium-IV with standard configurations. Though it is best performing under Linux environment but can be easily implemented on Windows platform also. Efficiency is particularly important when the software implementing the routing algorithm must run on a computer with limited physical resources. PAVNR suffices the purpose easily.

g) Rapidly Converging

EESSRP converges nicely and quickly. In all simulations, problem of looping never occurred. *Convergence* is the process of agreement, by all routers, on optimal routes. Slow convergence can cause routing loops or network outages.

h) Flexible

When a network segment gets down, as in the case of best protocols, EESSRP become aware of the problem and quickly selects the next-best path for all routes normally using that segment. It quickly and accurately adapt to a variety of network circumstances. It has been nicely programmed to adapt to changes in network bandwidth, router queue size, and network delay etc.

i) Minimum Route Computation and Overhead

EESSRP carries out this issue satisfactorily. Route computation should not involve the maintenance of global state, or even significant amounts of volatile non-local state. Also each node must only care about the routes corresponding to its destination, and must not be involved in frequent topology updates for parts of the network to which it has no traffic.

j) Route Repair

The route repair phase of EESSRP is unique as compared to other such protocols and outperform all in its category. It describes the maintenance process, which can be done as fast as possible. It describes the level of self organization in a network. The protocol uses local route repair of routing process.

k) Applicable

Many of the existing models on paper can go wayward in real life situations. Simulations of the EESSRP indicate its worth in real life scenarios as well.

VIII. Future Scope for Researchers

Ad hoc network routing research is still in progress. Outcome of the current research has exhibited the possibilities of further extensions. Some of the research work that can be carried out in future as an extension of current work is given below:

a) EESSRP should support Metropolitan area wireless ad hoc networking. For a real map, high number of nodes and suitable radio interface, a realistic earthquake scenario could be generated. The scenario considered is representing a maximum area of 1.5 KM square. Metropolitan area networking may require more area to be covered.

b) It should check the cases when nodes may be given less energy, so that partitioning behavior could be observed for different routing protocols. The nodes are given power status large enough to survive transmission. The other case may be taken when most of the nodes have depleting power factor. The effect of protocol may be checked in those cases.

c) It should support enhanced TCP connections. A transmission control protocol which is mobility enhanced [GOF00] could be implemented and used. In enhanced TCP connection, nodes are able to change speed while moving in the scenario and start moving at a new speed.

d) It should provide quality of service (QoS) [CHA01, MIR01, RAO98, SAJ00], which should be embedded in routing protocol. QoS is the ability of a network element (e.g. an application, host or router) to have some level of assurance often given in

terms of bandwidth or delay. It should be able to provide satisfactorily the level of Qos desired.

e) It should be able to handle cellular techniques, which could include the hand-over technique used for cellular networks [PER95, SCO97]. When a cellular phone moves from one cell to the other, the Base Station (BS) will detect this from the signal power and inform the Mobile Switching Centre (MSC) of that. The MSC will then switch the control of the call to the BS of the new cell, where the phone is located. This is called handover.

f) It should be able to work nicely for fading problems [PER95, SCO97]. Fading is the reduction of signal power. Fading is caused by many factors - the most important ones being multipath and shielding. Multipath fading is caused by the transmission of the signal along different paths and resulting in simultaneous reception. Depending of the amplitudes and phase of the signal, the result of this could be that the signals cancel each other completely or significant attenuation in the resultant signal. Shielding is the absence of field strength. Most common causes are tunnels, hills and inside certain buildings.

g) It should make use of diversity coding technique. The proposed protocol is an enhanced version of AODV. It has not been tested for source routing. An experiment may be conducted to check the performance of EESSRP for source routing also.

h) It should be able to support multicast transmission. Multicasting [GER00, PAU98, ROY99] is the transmission of packets to a group of hosts identified by a single destination address. Multicasting is intended for group-oriented computing. There are three primary functions that must be performed to implement IP multicasting: addressing, group management, and datagram processing / routing. It minimizes the link bandwidth consumption, sender and router processing, and delivery delay.

i) It should be able to increase the number of mobile nodes and to introduce more malicious nodes in the network scenario so that its impact on the network performance may be determined. The efforts can be made in the direction of improving hash functions to avoid collisions, using stronger hash keys by making them dependent on additional parameters like biometric credentials, passwords, IP addresses etc.

j) It should handle Mobile-IP [http:ENW, http:CIS]. Mobile IP provides users the freedom to roam beyond their home subnet while consistently maintaining their home IP address. This enables transparent routing of IP packets to mobile users during their movement, so that data sessions can be initiated to them while they roam; it also enables sessions to be maintained in spite of physical movement between points of attachment to the Internet or other networks.

k) It should be tested for fixed networks also. Also there should be a mechanism using a special addressing suitable for separation and merging of ad hoc networks.

References Références Referencias

1. Kush and S. Taneja, "Secured Routing over MANET with Power Management", Advances in Computing and Artificial Intelligence 2011, India, ACM Publisher, USA, pp. 144-149, 2011.
2. T. Karygiannis and L. Owens, "Wireless Network Security", NIST Special Publication, 800-48, November 2002.
3. S. Taneja and A. Kush, "Stable and Secured Routing Strategy for MANET with SSRP", Global Journal of Computer Science & Technology, USA, Volume 12, Issue 4, Version 1.0, pp. 20-32, 2012..
4. Kush A, Gupta P, "Power Aware Virtual Node Routing Protocol for Adhoc Networks", In International Journal of Ubiquitous Computing and Communication (UBICC), Vol 2 No. 3, pp55-62, South Korea 2007.
5. C. Parkins and E. Royer, "Adhoc on demand distance vector routing", 2nd IEEE workshop on Mobile Computing , pages 90-100, 1999
6. Chiasserini C. F., Chlamtac I., Monti P. and Nucci A., "Energy Efficient Design of Wireless Ad hoc Networks", Proceedings of Networking 02, pp. 376-386, 2002.
7. Adamou M. and Sarkar S., "A Framework for Optimal Battery Management for Wireless Nodes", Proceedings of IEEE INFOCOMP, pp. 1783-1792, 2002.
8. Chiasserini C.F. and Rao R.R., "Energy Efficient Battery Management", Proceedings of IEEE INFOCOM'00, vol. 2, pp. 396-403, 2000.
9. Kawadia V. and Kumar P. R., "Power Control and Clustering in Ad hoc Networks", Proceedings of IEEE INFOCOM'03, pp. 459-469, 2003.
10. Toh C. K., "Maximum Battery Life Routing to Support Ubiquitous Mobile Computing in Wireless Ad hoc Networks", IEEE Communications Magazine, vol. 39, No. 6, pp. 138-147, 2001.
11. Singh S., Woo M. and Raghavendra C. S., "Power-Aware Routing in Mobile Ad hoc Networks", Proceedings of ACM/IEEE International Conference on Mobile Computing and Networking, pp. 181–190, 1998.
12. Zheng R. and Kravets R., "On Demand Power Management for Ad hoc Networks", Proceedings of IEEE INFOCOMP, vol. 1, pp. 481-491, 2003.
13. Toh C. K., "Maximum Battery Life Routing to Support Ubiquitous Mobile Computing in Wireless

Ad hoc Networks", IEEE Communications Magazine, vol. 39, No. 6, pp. 138-147, 2001.
14. A. Kush, P. Gupta, and R. Chauhan, "**Stable and Energy Efficient Routing for Mobile Ad hoc Networks",** 5th International Conference on Information Technology: New Generations (ITNG), Las Vegas, USA, IEEE explore, DOI 10.1109/ITNG.2008.230, pp. 1028-1033, 2008.
15. Luo J. and Jha N. K., "Battery Aware Static Scheduling for Distributed Real Time Embedded Systems", Proceedings of IEEE DAC, pp. 444-449, 2001.
16. Li P.et al., "Power Control Network Protocol for Multirate Ad hoc Network", IEEE Transaction on Wireless Communications, Vol. 8, No. 4, pp. 2142-2148, 2009.
17. Chang J. H. and Tassiulas L. "Energy Conserving Routing in Wireless Ad hoc Networks", Proceedings of IEEE INFOCOM'00, pp. 22-31, 2000.
18. Wu J., Dai F., Gao M. and Stojmenovic I. , "On Calculating Power Aware Connected Dominating Set for Efficient Routing in Ad hoc Wireless Networks", IEEE/KICS Journal of Communication Networks, Vol. 4, No. 1, pp. 59-70, 2002.
19. Xue Y. and Li B., "A Location added Power Aware Routing Protocol in Mobile Ad hoc Networks", Proceedings of IEEE GLOBECOM'01, pp. 2837-2841, 2001.
20. Domingo M.C., Remondo D. and Leon O., "A Simple Routing Scheme for Improving Ad hoc Network Survivability", Proceeding IEEE GLOBECOM'03, pp. 718-723, 2003.
21. Laura Sanchez et al., "Energy and Delay-Constrained Routing in Mobile Ad hoc Networks: An Initial Approach", Proceedings of ACM International Workshop on Performance Evaluation of Wireless Ad hoc, Sensor and Ubiquitous Networks, pp. 262-263, 2005.
22. Chen Jie et al., "Energy Efficient AODV for Low Mobility Ad hoc Networks', Proceedings of Wireless Communications", Networking and Mobile Computing Conference (WiCom'07), pp. 1512-1515, 2007.
23. Senouci S. M. and Naimi M., "New Routing for Balanced Energy Consumption in Mobile Ad hoc Networks", Proceedings of ACM International Workshop on Performance Evaluation of Wireless Ad hoc, Sensor and Ubiquitous Networks, pp. 238-241, 2005.
24. Narayanaswami S., Kawadia V., Srinivas R. S. and Kumar P.R., "Power Control in Ad hoc Networks: Theory, Architecture, Algorithm and Implementation of the COMPOW Protocol", Proceedings of European Wireless Conference, pp. 156-162, 2002.
25. Xue Y. and Li B., "A Location added Power Aware Routing Protocol in Mobile Ad hoc Networks", Proceedings of IEEE GLOBECOM'01, pp. 2837-2841, 2001.
26. T. Karygiannis and L. Owens, "Wireless Network Security", NIST Special Publication, 2002.
27. William Stallings, "Cryptography and Network Security: Principles and Practice", Prentice Hall, 5th Edition, 2011.
28. Dahill B., Levine B. N., Royer E. and Shields C., "A secure routing protocol for ad hoc networks", Technical Report UM-CS-2001-037, University of Massachusetts, Department of Computer Science, 2011.
29. Hu Y. C., Johnson D. B., and Perrig A., "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad hoc Networks", Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and Applications, pp. 3-9, IEEE Computer Society, 2002.
30. Papadimitratos P. and Haas Z. J., "Secure routing for mobile ad hoc networks", SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS), 2002.
31. Zapata M. G., "Secure Ad hoc On-Demand Distance Vector (SAODV) Routing", IETF MANET Mailing List, Available at ftp://manet.itd.nrl.navy.mil/pub/manet/, 2004.
32. Papadimitratos P. and Haas Z. J., "Secure Link State Routing for Mobile Ad hoc Networks", Proceedings of IEEE Workshop on Security and Assurance in Ad hoc Networks, IEEE Press, pp. 27–31, 2003.
33. Hu Y. C., Perrig A. and Johnson D., "Ariadne: A secure on-demand routing protocol for ad hoc networks", Technical Report TR01-383, Rice University, 2001.
34. Kravets R., Yi S., and Naldurg P., "A Security-Aware Routing Protocol for Wireless Ad hoc Networks", ACM Symposium on Mobile Ad hoc Networking and Computing, 2001.
35. Georgios Kioumourtzis, "Simulation and Evaluation of Routing Protocols for Mobile Ad hoc Networks", Thesis, Master of Science in Systems Engineering and Master of Science in Computer Science, Naval Postgraduate School, Monterey, California, 2005.
36. Kawadia V. and Kumar P. R., "Power Control and Clustering in Ad hoc Networks", Proceedings of IEEE INFOCOM'03, pp. 459-469, 2003.

This page is intentionally left blank

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 12 Issue 10 Version 1.0 May 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Java File Security System (JFSS)

By Brijender Kahanwal, Kanishak Dua & Girish Pal Singh
Maharaja Ganga Singh University, Bikaner India

Abstract - Nowadays, storage systems are increasingly subject to attacks. So the security system is quickly becoming mendatory feature of the data storage systems. For the security purpose we are always dependent on the cryptography techniques. These techniques take the performance costs for the complete system. So we have proposed the Java File Security System(JFSS). It is based on the on-demand computing system concept, because of the performance issues. It is a greate comback for the system performance. The concept is used because, we are not always in need the secure the files, but the selected one only.

In this paper, we have designed a file security system on Windows XP. When we use the operating system, we have to secure some important data. The date is always stored in the files, so we secure the important files well. To check the proposed functionality, we experiment the above said system on the Windows operating system. With these experiments, we have found that the proposed system is working properly, according to the needs of the users.

Keywords : *File Security, S ecurity System, File Encryption, Information Security, On-demand computing.*

GJCST-E Classification: *D.4.6*

JAVA FILE SECURITY SYSTEM JFSS

Strictly as per the compliance and regulations of:

Java File Security System (JFSS)

Brijender Kahanwal [α], Kanishak Dua [σ] & Girish Pal Singh [ρ]

Abstract - Nowadays, storage systems are increasingly subject to attacks. So the security system is quickly becoming mendatory feature of the data storage systems. For the security purpose we are always dependent on the cryptography techniques. These techniques take the performance costs for the complete system. So we have proposed the Java File Security System(JFSS). It is based on the on-demand computing system concept, because of the performance issues. It is a greate comback for the system performance. The concept is used because, we are not always in need the secure the files, but the selected one only.

In this paper, we have designed a file security system on Windows XP. When we use the operating system, we have to secure some important data. The date is always stored in the files, so we secure the important files well. To check the proposed functionality, we experiment the above said system on the Windows operating system. With these experiments, we have found that the proposed system is working properly, according to the needs of the users.

Keywords : File Security, Security System, File Encryption, Information Security, On-demand computing.

I. Introduction

The access control is one of the fundamental security services in the computer system. It is a mechanism for constraining the interaction between users and protected resources. File is one of the important resources of the computer system. That must be protected from the unauthorized access that it can't be tempered or stolen by intruders. The file security can enforced using cryptographic techniques. With the help of these techniques the important files are encrypted and authorized users are given appropriate cryptographic keys.

The cryptographic techniques can be applied at any level of the storage systems because they use the layered architecture. The level may be the block or virtual one in the operating system. Basically, file management is an important task of the computer system. We have designed the Java File Security System (JFSS) [1-5] for files on the Windows XP.

The suggested file security system storing encrypted files using Rijndael Algorithm (AES) [6], so an unauthorized user can't access the important data. The encryption takes place for the selected files (important ones which requires the security) only.

We are using the concept of on-demand computing which results in the high performance of the computer system. The proposed system is working properly for all types of the files. In this paper there are more sections. Next section is section II which is about the related works. In section III, the design of the system is shown. In section IV, the evaluation is done. In section V, there is conclusion.

II. Related Works

So many approaches are applied to solve the problem of information security. The approaches may be the user space or kernel space or the combined one. The kernel approach is sensitive to implement because any small mistake done by the programmer can harm the overall funtioning of the system. The user space one is secure and competible with the system and the independent one and comfortable in the implementation and are the highly portable if we are using the best portable platform like Java.

There are so many implementations in the literature review and every one has there advantages and disadvantages with them. BestCrypt [7], is designed as a loopback device driver which creates a raw block device with a single file. The single file acts as a container (the backing store). There is an associated cipher key for each container. Cryptographic File System (CFS) [8], provides a transparent UNIX file system interface to directory hierarchies that are automatically encrypted with user supplied keys. It is implemented as a user level NFS server. User needs to create an encrypted directory and assign its key which is required for cryptographic transformations, when the directory is created for the first time. Transparent Cryptographic File System (TCFS) [9], works as a layer under the Virtual File System (VFS) layer, making it completely transparent to the application. The security is applied by means of the Data Encryption Standard (DES) algorithm [10].

III. Design

The main design goals of our research are as follows:

a) The proposed system should have better system performance as well as expand it for the existing file system.

Author α : Assistant Professor, CSE Department, GGGI, Dinarpur, Ambala, Haryana, INDIA. E-mail : imkahanwal@gmail.com

Author σ : Ex-B. Tech. Student, S. D. I. T. M., Israna, Panipat, Haryana, INDIA. E-mail : dua.kanishak@yahoo.co.in

Author ρ : Convener, CS and IT Department, Maharaja Ganga Singh University, Bikaner (Raj.), INDIA. E-mail : gpsbku@gmail.com

b) It should be independent of File System (it should not require the modifications in the other file systems or user applications).
c) It should offer strong storage security against most trivial and moderately sophisticated attacks.
d) It should be compatible with the future technology for separate key management just like smart cards for storing the encryption keys which are directly in the possession of authorized users.
e) It should be compatible with the existing file system services as the encrypted files should behave normally as of the other files within the system.
f) It should be developed as a user level file system and be convenient for users.

We have used the Windows XP operating system to design the functionality of file security system. The programming language to be used is the Sun Microsystems Java technology. To design it there is a function design form which has the necessary buttons on it.

The login form, that is used to login with the file security system. After entering the user id and password we are linking to the security execution program. We always need the user registration with the file security system. The registration is done by the program administrator who has the only permission to make number of users for the system. He or she will give the username and the password to the user. That is displayed in the Figure 3.1.

Figure 3.1: Login Display

After this user registration, he or she can login the system and use its functionality. The file encryption, decryption, about and help control form is appeared on the screen. It is shown in the Figure 3.2. It has the option to select the file to which the user wants to encrypt for the security feature. He or she can select any type of file and click on the encrypt button after that the encryption key is saved on the smart card is that is not available then the key is saved on the user specified location.

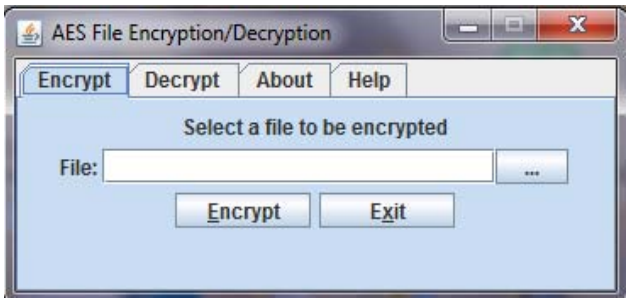


Figure 3.2: Encrytion tab display

The user may want to decrypt his previously encrypted file to use it. Then he or she have to make two selections one for the file and one for the key especialy the encryption key. Then the user will get the message to be successful or unsuccessful decryption. The successful message is shown in the Figure 3.3.

Figure 3.3: Decryption tab display

IV. Evaluation

We performe test and evaluation on the proposed file security system for files and the directories. For experiment the computer system was with the configurations as Pentium 4 processor, Windows XP operating system.

The system has been tested for its functioning. In the first login window the user enter his or her userid and the password. If that is correct then he or she will get a message login successful or not. As in the Figure 4.1 the login is a successful one.

Figure 4.1: A successful login window

In the next screen shot the user is going to select an important file that has the need of security. It

encryptes the specified file and save the encryption key to the smart card which is a sapeate location of storage from the encrypted file. It increses security of the data. It is shown in the Figure 4.2.

Figure 4.2: Encryption tab display

This is the Figure 4.3 which shows the decryption process of the system. It has two file selection buttons on it. One file selection button for the specified encrypted file to whom the user is going to decrypt. Another one is for the key selection of the specifed file. Because every file has its own independent key to encrypt or to decrypt it.

Figure 4.2: Decryption tab display

We have seen the file's look how it will behave after the encryption. The system is highly secure that we can cont delete the encrypted file and also con't change data which shows the integrity. The encrypted file's view is shown in the Figure 4.4.

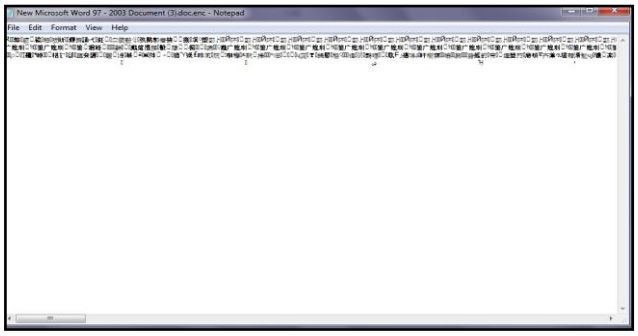


Figure 4.4: Display screen of an encrypted file

V. Conclusion

We have contributed in the desiging and development of a user space cryptographic file system. We have balanced the design goals like security, performance, convenient and independability of the system.

We have achieved the high security by including the support of the Rijndeal Algorithm (AES) and we have saved the keys on the portable smart cards for the documents which are important.

The performance is achieved with the help of on-demand computing concept which is that we are not going to encrypt all the files on the computer system, but we are going to encyrpt only the important documents only. It saves the performance overhead of the system.

The system is very convenient to the users as described in the study done in the refernce [2]. And the independability is achieved with the help of the Java technology which is highly portable. So the complete system is a highly independent of the configuration.

Acknowledgement

We would like to thank all the anonymous revieweres because of their valuable feedback and suggestions. We have developed a convenient system for the community.

References Références Referencias

1. B. Kahanwal, T. P. Singh, and R. K. Tuteja. "A Windows Based Java File Security System (JFSS)". International Journal of Computer Science & Technology (2011),Vol. 2, No. 3, pp. 25-29.
2. B. Kahanwal, T. P. Singh, and R. K. Tuteja, "Java File Security System (JFSS) Evaluation Using Software Engineering Approaches", International Journal of Advanced Research in Computer Science & Software Engineering (2012), Vol. 2, No. 1, pp. 132-137.
3. B. Kahanwal, T. P. Singh, and R. K. Tuteja, "Towards the Framework of the File Systems Performance Evaluation Techniques and the Taxonomy of Replay Traces", International Journal of Advanced Research in Computer Science (2011), Vol. 2, No. 6, pp. 224-229.
4. B. Kahanwal, T. P. Singh, and R. K. Tuteja. "Performance Evaluation of Java File Security System (JFSS)", Pelagia Research Library—Advances in Applied Science Research (2011), Vol. 2, No. 6, pp. 254-260.
5. B. Kahanwal, and T. P. Singh, "Towards the Framework of Information Security", Journal of Current Engineering Research (2012), Vol. 2, No. 2, pp. 31-34.

6. Department of Commerce: National Institute of Standards and Technology (NIST), " Federal Information Processing Standard (FIPS) PUB #197: Advanced Encryption Standard (AES)", 2001,NIST, Gaithersuburg, MD, USA.
7. Mick Bauer, Paranoid penguin, "BestCrypt: Crossplatform filesystem Encryption", Linux Journal, 2002, 98:117.
8. M. Blaze, "A Cryptographic File System for UNIX", in ACM Conference on Computer and Communications Security,1993, pp. 9-16.
9. G. Cattaneo, L. Catuogno, A. D. Sorbo, and P. Persiono, "The Design and Implementation of a Transparent Cryptographic File System for UNIX", in the proceedings of USENIX Annual Technical Conference: FREENIX Track, 2001, pp. 245-252.
10. Department of Commerce: National Institute of Standards and Technology (NIST), " Federal Information Processing Standard (FIPS) PUB #81: Data Encryption Standard (DES)", NIST, Gaithersuburg, MD, USA, 1980.

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 12 Issue 10 Version 1.0 May 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Enhancement of Confidentiality of Data Transmitted Over Covert Channel Using Grid Cipher Scheme

By Raju Singh Kushwaha

Sri Ram Murti Smarak College of Engineering & Technology, Bareilly, (U.P.), India

Abstract - In this fast developing world, the interchange of information is playing a key role. Everything needs information and processes them. This interchange of information needs an authentication, confidentiality and integrity. The security of information is provided many algorithms. There are vast numbers of algorithms for symmetry key cipher. All these algorithms have used either complicated keys to encrypt the plain text to cipher text or a complicated algorithms used for it. The level of security of algorithms is dependent on either number of iterations or length of keys. A comparative study have been made with RSA, DES, IDEA, BAM and other algorithms with frequency distribution, bit ratio to check the security level of proposed algorithm. Finally, a comparison has been made for time complexity for encryption of plain text and decryption from cipher text with above existing algorithms.

Keywords : *Plain text, cipher text, symmetric key algorithm, grid, RSA Algorithm time complexity and frequency distributions.*

GJCST-E Classification: *D.4.6*

Strictly as per the compliance and regulations of:

Enhancement of Confidentiality of Data Transmitted Over Covert Channel Using Grid Cipher Scheme

Raju Singh Kushwaha

Abstract - In this fast developing world, the interchange of information is playing a key role. Everything needs information and processes them. This interchange of information needs an authentication, confidentiality and integrity. The security of information is provided many algorithms. There are vast numbers of algorithms for symmetry key cipher. All these algorithms have used either complicated keys to encrypt the plain text to cipher text or a complicated algorithms used for it. The level of security of algorithms is dependent on either number of iterations or length of keys. A comparative study have been made with RSA, DES, IDEA, BAM and other algorithms with frequency distribution, bit ratio to check the security level of proposed algorithm. Finally, a comparison has been made for time complexity for encryption of plain text and decryption from cipher text with above existing algorithms.

Keywords : Plain text, cipher text, symmetric key algorithm, grid, RSA Algorithm time complexity and frequency distributions.

I. Introduction

Cryptography is the study of transmitting secret messages securely from sender to receiver. [4]The original text, called plain text it's encrypted form is called cipher text, which is sent to the receiver. The recipient decrypts the text to get the plain text. The model of secret key system, first proposed by Shannon ([4]) is shown in figure1.

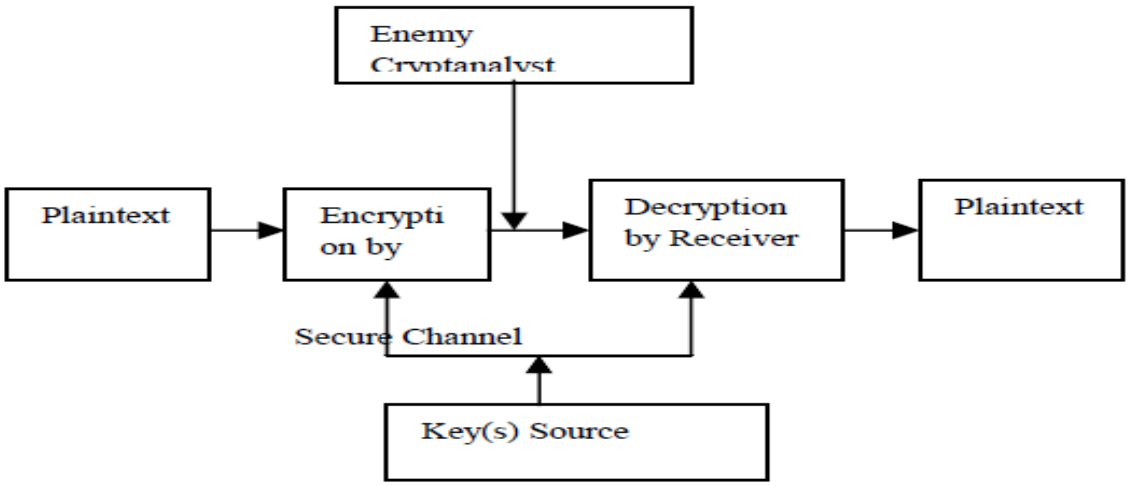


Figure 1: The model of secret key system proposed by shannon

There are many algorithms had developed to providing security of information but each of them having some merits and demerits. There is no single algorithm is sufficient to provide security. In this paper, an effort has been made to develop a new block cipher algorithms using a set of 16 grids where each grid is 4X4 matrix [2]. Each grid is capable to store 16 characters and finally, all ASCII characters value has been stored in grid set. The algorithm has been performing two steps. In first step, the plaintext has been broken into number of block eight characters. Each character from each block has been converted into bit stream and placed in the grid set. After placing all characters, new bit stream for each character of the block has been calculated using grid number, row number and column number. In second step, the stream bit is consist of eight bit for single character, calculate their decimal value and assigns the ASCII character for this decimal value.

Author : Assistant Professor Department of Computer Science Sri Ram Murti Smarak College of Engineering & Technology, Bareilly, (U.P.), India. E-mail : rajukushwaha36@gmail.com

Part 2 of the paper deals encryption technique. Part 3 deals with proposed technique. Part 4 consist of experimental results. Part 5 deals with Securities level testing for the proposed algorithm. Part 6 are Conclusions. At end of paper References are given.

[6]To ensure the security of encryption algorithm many effects have done. These are avalanche, bit ratio, non-homogeneity and time complexity. The avalanche effect means a small change in plain text (or key) should produce a significant change in cipher text. [4]The bit ratio effect means the changes the bit values from same position between plain text and cipher text. The non-homogeneity test is a technique to test non-homogeneity of the source and encrypted file. The time complexity defines how efficiently the proposed algorithm will encrypt the plain text and decrypt from encrypted text.

II. Literature Survey

[4] In this paper, the Frame based encryption process is proposed, this is also block cipher scheme which break the plain text into eight character size block. Find their positional value from the frame and put their corresponding ASCII value. This forms a 8-bit stream of data which is swapped with another string and generate their ASCII character. This character is send to the receiver.

[2] In this paper, the proposed algorithm used the 26 characters, 10 numerals and single space character. This form a block of 37 characters, when plain text is encrypted into cipher text the plain text character is taken their value from this block of 37 character and form a matrix of order 3*3. Select a Key matrix of same order and encrypt the data with this process and result is taken modulus by 37. Cipher text is generated and sends to the receiver.

[5] In this paper, the proposed algorithm compress the plain text with arithmetic algorithm the resultant value of compress data is encrypt with RSA algorithm, the cipher text is generated and send to the receiver.

Hill cipher's or linear block cipher is susceptible to cryptanalysis and unusable in practice, still serves an important pedagogical role in both cryptology and linear algebra. It is this role in linear algebra that raises several interesting questions [1].

In this paper, the proposed algorithm is a modified form of RSA algorithm named RSA1, which enhance the security of RSA algorithm. The resultant value of RSA algorithm is converted into corresponding ASCII character value and then send to the receiver. [7]

III. Proposed Work

The algorithms are based on the grid. A single grid consists of 16 characters. Then total number of grid is16 required for representing ASCII set. The total ASCII character are 256.

Algorithms:

a) Sender Prospects: Encryption

Step 1: Represent each character of plain text by another character which is equivalent a number, generated from reference grid model .Then, the substitute character is represented by the bit sequence (x,y,frame no).

Step 2: Grouping the modified plain text into blocks of eight characters. If modified test is not properly divided by eight then blank characters will be padded with last block.

Step 3: Convert each block into equivalent bit streams.

Step 4: This bit stream converted into Decimal equivalent.

Step 5: Apply RSA algorithm to encrypt this decimal value.

Step 5.1: Select two prime number P,Q;
Calculate n=P*Q;;
Calculate _(n)= (P-1)*(Q-1);
Select integer e; gcd(f(n),e)=1; 1<e<f(n);
Calculate d; d=e^-1 mod f(n);
Public key KU= {e, n};
Private Key KR= {d, n};

Step 5.2: Encryption
Plain text : M< n
Cipher Text : C=M^e (mod n);

Step 6: This Decimal value is changed into ASCII character. This is cipher Text.

Step 7: Repeat steps 2 to 5 until all characters of plain text become converted into cipher text.

b) Receiver Prospects

Decryption

Step 1: Take cipher text and extract ASCII Character Value individual.

Step 2: Change this value into decimal Equivalent.

Step 2.1: Decryption
Cipher Text : C
Plain Text : M = C^d (mod n);

Step 3: Convert this decimal into bit stream.

Step 4: First Two bit represent X-axis, Second two bit Represent Y-axis and remaining four bit represent grid number. Match bit stream with above process and take the ASCII value.

Step 5: Convert This ASCII Value into Character set.

Step 6: Recover Plain Text from Cipher Text.

IV. Result

a) Sender Prospects

Take the word "Crypto" encrypt this with the help of above algorithm.

Plain text	ASCII Value	(X,Y, Grid No)	Bit stream	Convert decimal No
C	67	0,3,3	00110011	51
R	114	0,2,6	00100110	38
Y	121	2,1,6	10010110	150
P	112	0,0,6	00000110	70
T	116	1,0,6	01000110	06
O	111	3,3,5	11110101	245

Apply RSA algorithm to encrypt this decimal value and the resultant cipher text is== 3&--F<õ

b) Receiver Prospects

Sender & Receiver both are well known algorithm & encrypted text is in ASCII Format. Receive the Cipher Text C= 3&--F<õ , Apply RSA algorithm to decrypt the cipher text in Decimal value format.

Decimal Value	Bit Stream	(X, Y, Grid No)	ASCII Value	Plain Text
51	00110011	0,3,3	67	C
38	00100110	0,2,6	114	R
150	10010110	2,1,6	121	Y
70	00000110	0,0,6	112	P
06	01000110	1,0,6	116	T
245	11110101	3,3,5	111	O

V. Conclusion & Future Scope

It is observed from the result the proposed algorithm is extremely efficient and a sufficiently strong encryption algorithm enhance the security of data transmitted over covert channel. A degree of freedom value of 256 ensures the maximum variety of characters in the cipher text which ensures its strength against an attack. Frequency Distribution also speaks the encrypted character evenly distributed from 0 to 255. So, it has been made more difficult for attacker to recover plain text from cipher text. This algorithm provide security over data in two ways , Firstly the arrangement of grid is only known by both parties only and secondly the key is used in RSA algorithm is also unpredictable by the intruders. There is some extra effort have made in grid and their storage format then this algorithm give more better result in terms of security and speed of encryption & Decryption.

References Références Referencias

1. C.E. Shannan, "Communication Theory of Security System", Bell, System Technical Journal, vol 28, pp.656-715, 1949.
2. Nalini. N and G. Raghavendra Rao," A New Encryption and Decryption Algorithm Combining the Features of Genetic Algorithms(GA) and Cryptography"
3. H. Feistel," Cryptography and Computer Privacy", Scientific American Vol. 228, no. 5, pp 15-23, 1973.
4. Uttam Kr Mondal, Satyendranath Mondal," Frame Based Symmetric Key Cryptography", Int. J. Advanced Networking and Applications Volume: 02, Issue: 04, Pages: 762-769 (2011)
5. Raju Singh, A.K.Vatsa"Confidentiality & Authentication Mechanism For Bio-Metrics Information transmitted over Low Bandwidth channel", International Journal of Network Security & it's Application Vol: 3, Issue: 3.
6. John C. Bowman, Math 422 Coding Theory & Cryptography, University of Alberta, Edmonton, Canada.
7. RSA-2 Algorithm Speed and Security enhancement through public key cryptography International Journal of Engineering Science & Technology Vol.2 (8), 2010, 3551-3556, J. SaiGeethaet. al.

This page is intentionally left blank

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 12 Issue 10 Version 1.0 May 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

QoS-Aware Web Service Selection Using SOMA

By Krithiga R.

Engineering and Technology Pondicherry University Pondicherry India

Abstract - It is important to deliver appropriate services to requested users. In case of unavailability of a user requestedcomposite service, enforces the system to invoke service selection that involves choosing individual concrete services towards service composition. The services are selected based on two criteria: i) functional based and ii) non-functional based. The former entails selection of services based on functional property that the service is dedicated to do and the latter elite selection of services based on the QoS attributes such as reliability, availability, cost, and response time. Several population-based and swarm-based optimization algorithms are widely used for the process of web service selection. In this work, we employ a stochastic optimization algorithm called Self Organizing Migrating Algorithm (SOMA) and compare its performance with GA and PSO. The comparative study evidences that SOMA produces promising results and is therefore able to select user requested service in an efficient manner.

GJCST-E Classification: *H.3.5*

Strictly as per the compliance and regulations of:

QoS-Aware Web Service Selection Using SOMA

Krithiga R.

Abstract - It is important to deliver appropriate services to requested users. In case of unavailability of a user requestedcomposite service, enforces the system to invoke service selection that involves choosing individual concrete services towards service composition. The services are selected based on two criteria: i) functional based and ii) non-functional based. The former entails selection of services based on functional property that the service is dedicated to do and the latter elite selection of services based on the QoS attributes such as reliability, availability, cost, and response time. Several population-based and swarm-based optimization algorithms are widely used for the process of web service selection. In this work, we employ a stochastic optimization algorithm called Self Organizing Migrating Algorithm (SOMA) and compare its performance with GA and PSO. The comparative study evidences that SOMA produces promising results and is therefore able to select user requested service in an efficient manner.

I. Introduction

Service Oriented Architecture (SOA) enables enterprises to quickly respond to business needs by rapidly developing required web services in anagile manner. Web services catch attention due to its wide applicability with the advent of new technologies. It stimulates dynamic, configurable software applications to improve the aggregated yield and promote reusability. The features of web service technology include interoperability, decoupling and just-in-time integration [9]. It is important to deliver appropriate services to requested users. When a user request cannot be addressed by a single service, enforces the system to invoke service selection, which involves choosing individual concrete services towards service compositionso as to deliver a composite service. Web service selection constructs new value-added utility through the integration of available concrete services. Each abstract task is an abstract representation of a service's functionality and contains many instances of concrete services dedicated for each abstract representation. A set of abstract tasks thereby constitutes the abstract functionality of a composite service and a set of concrete services each from an abstract representation constitutes the composite service.As many service providers offer services of similar functionalities, the existence of services incredibly increases and the implementation of those services considerably varies from each other. An implementation of a service may be better than other implementation in terms of some QoS criteria and may not be as good as of a service in terms of other QoS criteria. The service selection is an*np-hard* decision problem [7], on which concrete services should be selected such that the user's functional and non-functional requirements are met. Therefore, an efficient mechanism is needed to effectively choose appropriate services. Traditionally, two criteria are followed for web service selection: i) functional based ii) non-functional based. The former entails selection of services based on functional property that the services areintended to do and the latter elite selection of services based on the QoS attributes such as reliability, availability, cost, and response time [2]. It is difficult to select services from service registries in the case that the selection is solely based on functionality as thousands of services offer same functionality. The QoS is an important element of web services that determines the success or failure of a composite service and facilitates users to quantify the quality of the delivered service. Currently, most of the works use successive evaluation of different non-functional aspects in order to attribute a general "level of quality" to different composite web services and to select the best one from these services. The QoS of a web service may be defined and offered by different Service Level Agreements (SLA) between service providers and clients. In the Internet-based environment, the QoS of composite service is fluctuated due to the quality of concrete services, which are subjected to change with various factors [10]. In order to satisfy both functional and non-functional constraints, suitable concrete services need to be selected for service composition. The malfunction of a concrete service may cause flaws to the final product composite service. The concrete services are to be loosely coupled in order to co-exist with a range of other services that lasts for a session of period. The pre-requisites of web service selection mechanism typically comprises of service discovery, service orchestration and is to be done in such a way that the overall QoS is improved in the composite web service. The objective of the web service selection problem is to select an implementation for each of the abstract class in the composite web service such that the overall QoS is maximal. This type of web service selection problem is also called QoS-aware web service selection [9], which aims at finding the best combination of web service candidates in order to fulfill a given SLA. The fitness function includes a set of system-specific parameters to achieve user requested goals. The performance of service selection algorithm

Author : Department of computer science School of Engineering and Technology Pondicherry University Pondicherry India.
E-mail : rkrithiga.17@gmail.com

can have a great influence on the overall performance of the composed system.

In the literature, many researchers have proposed various techniques and employed it for web service selection problem. Techniques also have been modified or improved to be able to deploy for the problem-specific issues. Zongkai YANG et al proposed a dynamic web service composition technique that integrates the ant colony optimization and the genetic algorithm [12]. Jong MyoungKoet al proposed a constraint satisfaction based web service composition algorithm that combines tabu search and simulated annealing [4]. QoS is an important criterion for web service selection. Sathya et al explored various techniques of Quality of Service based Service Selection (QSS) and identified a number of QSS specifications and descriptions for service selection [8]. LailaTaher et alproposed a frame work based on QoS-IC (Information and Computatuion) that extends the functionality of QoS Manager Component of QoS-IC framework with QoS constraints [5]. Many issues and dimensions of web service selection problem have been focused. *Heejung Chang and kangsun Lee* [3] proposed a quality driven web service composition methodology for ubiquitous services using a multi-criteria quality model which involves quality of services (QoS), quality of contents (QoC) and quality of devices (QoD) that addresses transparency by the use of Event-driven Web service Composer (EWC) tool. *Okkyung Choi* and *SangYong Han*[6] introduced a novel intelligent web services algorithm for service discovery and execution called Integrated Matchmaking algorithm, which associates rule based and semantic based search for the effective construction of web services.

This paper introduces an efficient QoS-aware web service selection approach based on evolutionary computingand makes use ofspecially designed Self-organizing migrating algorithm (SOMA) for web-service selection problem. Among the existing four versions of SOMA, the *All-To-One* standard version is being considered for our work. This paper first presents a QoS-aware service selection model that incorporates weighted sum model for decision making process and employs SOMA to find the optimal solution. Further, in order to make the algorithm more appropriate for WSS problem, we redefine the parameters of SOMA and compare the performance with GA and PSO. The experimental results indicate that the proposed service selection approach based on SOMA significantly outperform the other algorithms in terms of efficiency and effectiveness.

The structure of the paper is as follows: In the preceding section, we firstly introduce the QoS Aware web service selection model. Section 3 discusses the service selection scheme based on SOMA. The experimental evaluations and performance comparison with GA and PSO are presented in section 4. Finally, section 5 concludes the paper.

II. Problem Formulation

In this problem formulation, we follow the conventional terminologiesused by the web service community. In the rest of paper,when we say abstract web service, we refer to the abstract functionality of a web serviceand when say concrete web service;it refers to the implementation details of an abstract web service. Further, in the section, we restrict our system model by consideringfour most popular QoS attributes. However, it can be easilyextended to include or excludeas many QoS attributes.

- A Composite Service (CS) is a collection of abstract services $\{S_1, S_2 \ldots Sn\}$that encompasses the overall functionality of a CS, where *n* represents the number of services required to construct a CS.
- An Abstract service is defined as an abstract representation of a service functionality and possess m instances of concrete services $\{s_{ij}\}\,(1 < i < m)\,(1 < j < n)$, where m represents the number of implementations or instances of an abstract service.
- A Concrete service s_{ij} is an instantiation abstract service and represents a functionality of a CS.

Each service provider must define the QoS model before delivering QoS aware service []. In our current study, four qualities attributes namely reliability, response time, availability and cost are considered as part of theWeb service parameters. These QoS attributes can also beapplied to evaluate QoS of the constructed business process. The values of these QoS parameters range between 0 and 1. The service provider holds a value for each QoS parameter. The customer requests a service provider for a service by specifying an upper and lower bound value for each QoS parameter. In particular, the lower bound is suggested for negative attributes such as execution price and execution time, and the upper bound is suggested for positive attributes such as reliability and availability. In order to evaluate the multi-dimensional quality of a given web service composition, we employ autility function called a Simple Additive Weighting technique (SAW), a weighted sum of each attributes for the QoS of a composite web service, which was introduced in the context of Multiple Criteria Decision Making (MCDM) [1].Before evaluating web services with the objective function, the QoS attributes need to be normalized and uniformly scaled using the (1) and (2).

$$q_i = \begin{cases} \frac{q_i^{max} - q_i}{q_i^{max} - q_i^{min}}, & \text{if attributes are negative} \\ 1 \end{cases} \quad (1)$$

$$q_i = \begin{cases} \frac{q_i - q_i^{min}}{q_i^{max} - q_i^{min}}, & \text{if attributes are positive} \\ 1 \end{cases} \quad (2)$$

Where q_i^{max}, q_i^{min} represents the lower and upper bounds provided by the user for a particular QoS attribute. $q_i$is the QoS value provided by the service provider. The overall objective function can be formulated as,

$$f(x) = \frac{1}{n}\sum_{i=1}^{n} q_i w_i$$

Where $\sum_{i=1}^{4} w_i = 1$ and denotes the interpretation user preferences in terms of weights for each attribute and $n$represents the number of QoS attributes involved. As end users specify the lower and upper bound values for QoS, services are declined if the user's constraints and requirements are violated.

III. Optimal Service Selection Using Soma

The Self Organizing Migrating Algorithm (SOMA) is a novel stochastic optimization technique (Zelinka, 2004) [SOMA], devised on the self-organizing, cooperative, competitive behavior of social group of animals searching for the best living condition. This algorithm which has been proved to converge towards the global optimum works on a population of candidate solutions and is initialized by a random distribution over the search space. The group of animals competitively searches for the best living condition and they cooperatively organizes their movement and migrates to a better living condition. In this algorithm, during a migration loop, no new generations of individuals are created but only the positions of the individuals in the search space are changed based on the two parameters, *perturbation* and *migration*.

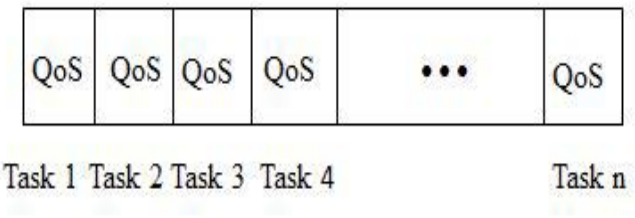


Fig. 1: Individual representation of a composite service (CS)

The SOMA is applied to WSSP and therefore firstly, the problem has to be encoded. Fig.1 shows the individual representation of a composite service. Each individual is represented by an array with the number of dimensions equals to the number of abstract tasks involved. Therefore, each individual is encoded as a composite service, which contains a combination or sequence of concrete services and dimension of the algorithm corresponds to concrete web services. The dimension holds appropriate QoS value of a particular concrete service that implements the functionality of the congruent abstract representation. SOMA holds the same initial population throughout the migration process and only the positions of the individuals are changed. Similarly, the problem does not change and evaluate concrete services during iterations. It just deals with the QoS values; Instead of the changing and trying out other combination of services, the system simply changes the values of the services. The change in the values of concrete services is homologous to the change of positions of individuals. After each migration, a configuration is selected by SOMA. The average QoS value of selected configuration is then calculated. The services are evaluated using the fitness function and may involve some constraints based on the user preferences. The problem can be a maximization or minimization and in our work the latter is employed. When user or domain specific non-functional attributes are used, the specification of the fitness function is left to the workflow designer.

The perturbation operation decides which values of services are subjected to change and which are not. The PRT vector that consists of 0's and 1's is responsible for this mechanism. A number 0 indicates that the values are not changed for a particular service and a value 1 indicates that the values are subjected to changes. This mechanism of deciding upon the formation of a composite service by retaining some of the QoS values of services while letting other services undergo change is done randomly. The randomization processes are always believed to lead to a better solution. The migration operation promises in drifting the values to an optimum solution by making it traverse in the direction of the leader (optimal solution). The output of the algorithm is a sequence of real number values that specifies the expected metric value of individual concrete services. The relevant services are chosen from the service registry, which makes up a composite service.

Algorithm WSS-SOMA

```
Randomly create an initial population of Pop Size
For n migrations do
Generate PRT vector
Evaluate population using fitness function
Select leader
For each individual j in population do
        store best solution of j into best fitness
        for k steps (k<= pathlength)
                migrate individual j towards leader
                Evaluate QoS at new position
        If new position is better than the best fitness
then
        new position becomes he best fitness
                end
end
move individual j to best position
end
```

end
output best.

IV. Experimental and Resultanalysis

SOMA is applied to detect the optimal configuration that satisfies service selection constraints and requirements. In order to show the performance of the proposed QoS aware WSS using SOMA, a test has been conducted. The experiment is conducted on a desktop computer with 2.80 GHz CPU and 2 GB RAM. In the experiment, we intend to create a composite service with 30 abstract tasks. Therefore, the searching process is done in 30-dimensions and the number of instance services available for each abstract task is set to 50. Several stopping criteria are employed to terminate the execution. In our work, the algorithm is executed for 25 runs and the maximum number of function evaluations is set to 12000. Similar setting is done for all algorithms for the purpose of comparison. An aggregation is then performed for each of the QoS parameters and the values are normalized using the fitness function. The PRT vector of SOMA is set to 0.1. The step size and the path length, which greatly affect the search process, are set to 0.11 and 2.2 respectively. The results of the experiment are show in the form a graph Figure: 2 that depict the performance of the proposed technique for 25 runs. Further comparing with GA and PSO, the advantages of SOMA are that SOMA is easy to implement and there are few parameters to adjust and the information sharing mechanism in SOMA is significantly different compared to GA and PSO.

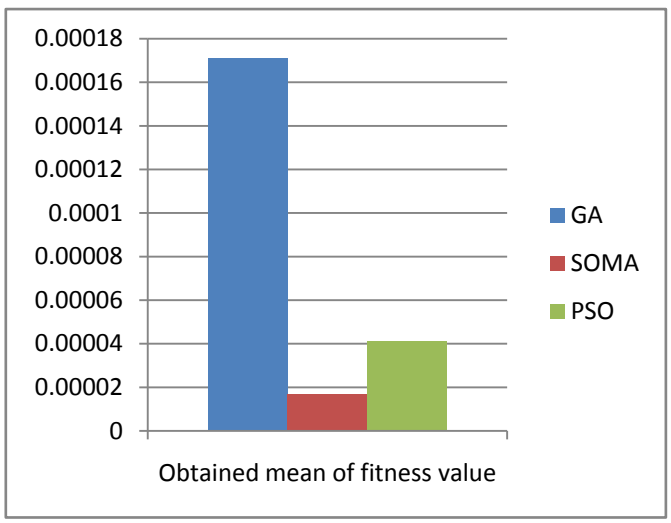


Fig. 2: The average fitness value on GA, SOMA and PSO

The experimental results indicate that the QoS optimization of service selection can be achieved by using SOMA. Along with the increase of migrations, the service configuration selected by SOMA gradually tends to an optimal configuration. The experimental result is shown in Fig 2. As our problem deals with minimization, it can be seen that SOMA has generated accurate results, comparatively. Although PSO almost perform in a better way, the difference between the performance of GA and SOMA is significant. The overall performance for WSSP can be written as SOMA>PSO>GA.

As it can be seen from the graph, the cost values obtained by SOMA are very close to the desired value, it is obvious that the proposed scheme QoS aware service selection is not only interoperable efficiently chooses the concrete services that satisfy the goals.

V. Conclusion

In order to satisfy multiple functional and non-functional constraints, suitable concrete services need to be selected for web service selection. Due to the complexity involved in the problem, we have presented an algorithmic approach for solving the optimal service selection problem by considering a stochastic optimization algorithm called SOMA and specially designed it suitable for WSS. Our approach is designed to accelerate the detection of optimal configuration at rapid convergence. The algorithm guarantees the resulting composite web service with maximal overall QoS that strictly conforms to the QoS constraints and user requirements. As a part of our future work, the algorithm has to be improved in order to survive in a ubiquitous environment. The mobility, adaptability and user preferences are to be formulated automatically as constraints.

References Références Referencias

1. Ching-Lai Hwang and K. Paul Yoon, editors. Multiple Attribute Decision Making: Methods and Applications, volume 186 of Lecture Notes in Economics and Mathematical Systems. Springer-Verlag, March 1981.
2. R. Dinesh Kumar and Dr.G. Zayaraz, "A Qos Aware Quantitative Web Service Selection Model", International Journal on Computer Science and Engineering (IJCSE), 2011.
3. Heejungchang and kangsunlee, "A Quality-Driven Web Service Composition Methodology for Ubiquitous Services", Journal of Information Science and Engineering, 2010.
4. JongMyoungKo et al, "Quality-of-service oriented web service composition algorithm and planning architecture", The Journal of Systems and Software, 2008.
5. LailaTaher et al, "Establishing Association between QoS Properties in Service Oriented Architecture", Proceedings of the International Conference on Next Generation Web Services Practices, 2005.
6. Okkyung Choi and SangYong Han, "Ubiquitous Computing Services Discovery and Execution Using a Novel Intelligent Web Services Algorithm", Sensors 2007.

7. Palanikkumar, D. and G. Kousalya, "An Evolutionary Algorithmic Approach based Optimal Web Service Selection for Composition with Quality of Service", Journal of Computer Science, 2012.
8. Sathya et al, "Evaluation of QoS Based Web-Service Selection Techniques for Service Composition", International Journal of Software Engineering (IJSE), Volume (1): Issue (5).
9. Tang, Maolin and Ai, Lifeng, "A hybrid genetic algori-thm for the optimal constrained web service selection problem in web service composition". In: Proceeding of the 2010 World Congress on Computational Intelligence, 18- July 2010, Centre de Convencions Internacional de Barcelona, Barcelona.
10. Xue-long Wang et al, "Service selection constraint model and optimization algorithm for web service composition", Information Technology Journal, 2011.
11. I. Zelinka, "SOMA—self organizing migrating algorithm," in New Optimization Techniques in Engineeri*ng*, B. V. BabuandG. Onwubolu, Eds., pp. 167–218, Springer, New York, NY, USA, 2004.
12. Zongkai YANG et al, "A Dynamic Web Services Composition Algorithm Based on the Combination of Ant Colony Algorithm and Genetic Algorithm", Journal of Computational Information Systems, 2010.

This page is intentionally left blank

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 12 Issue 10 Version 1.0 May 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Geographical Information System for Power Utilities

By Jalpesh Solanki & Utkarsh Seetha
Jodhpur National University

Abstract - GIS, Feeder Manager, CCC, SCADA, HT Network, LT Network.

GJCST-E Classification: *H.3.0*

Strictly as per the compliance and regulations of:

Geographical Information System for Power Utilities

Jalpesh Solanki [α] & Utkarsh Seetha [σ]

Abstract - GIS, Feeder Manager, CCC, SCADA, HT Network, LT Network.

I. Introduction

The Geographical Information system has been used worldwide for controlling and managing the business process and field operations. It also widely used for automation of the system. In this research we defined the scope of the GIS system in the current scenario and used the same to give maximum input to the current business application.

The major benefit to use GIS will be obtained only after the successful data captured for the entire HT/LT network and all the current electrical consumers. The GIS system gives error free automated inputs to the system for forecasting the future needs related to the electrical network as well as demand. This will generate automated reports to help the engineers to make the system error free and make the system up to date.

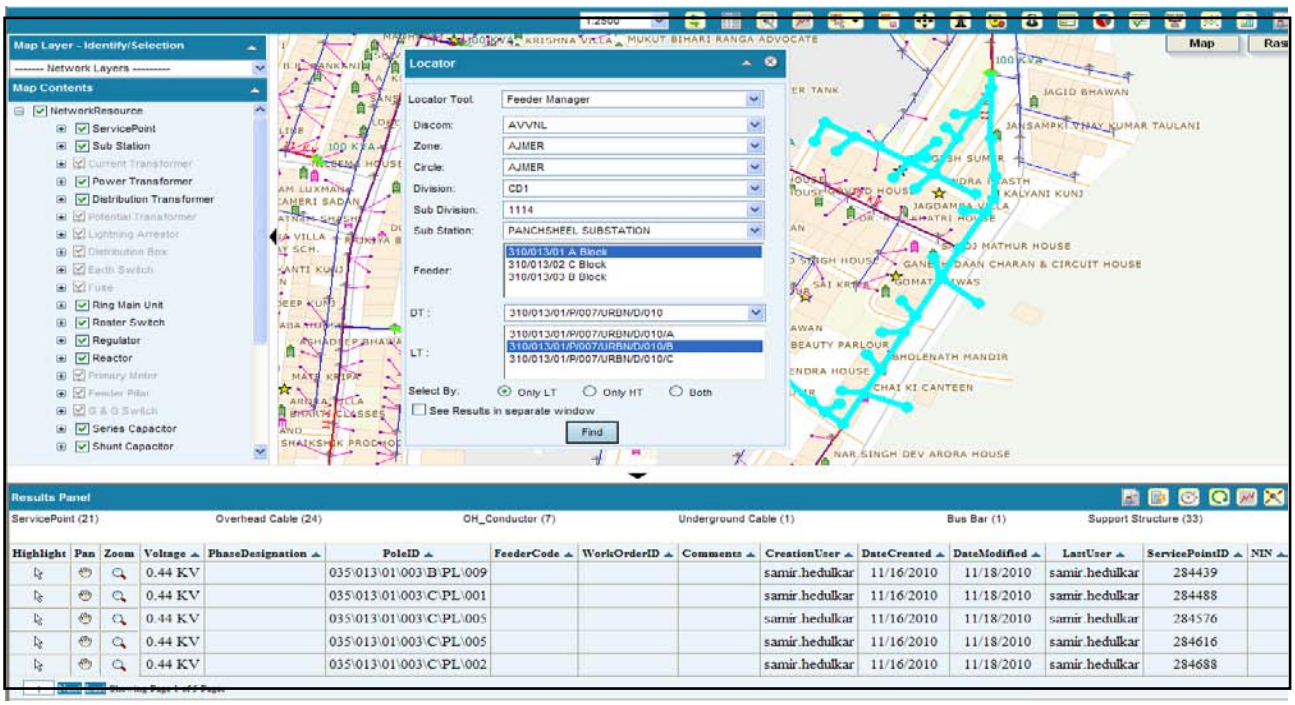
Geographic Information System consists of a system for capturing, storing, checking, integrating, manipulating, analyzing and displaying geo data related to positions on the Earth's surface and data related to attributes of the entities/Customers.

It pertains to both vector and raster GIS

This is achieved through GIS mapping to pre-defined scale, generation of intelligence electrical network maps and super imposing them on the land base GIS maps and through customization and / or development of application software.

Feeder Manager – LT option

1. Select Feeder Manager in the Locator Tool drop down.
2. Select the values in drop down DISCOM, Zone, Circle, Division, Sub Division and Sub Station.
3. Select a feeder in feeder List box.
4. Select 'Only LT' radio button.
5. Select any DT in DT dropdown.
6. Click on Find button.
7. This will highlight the features covered in specified LT and the attributes will be displayed in the results panel.



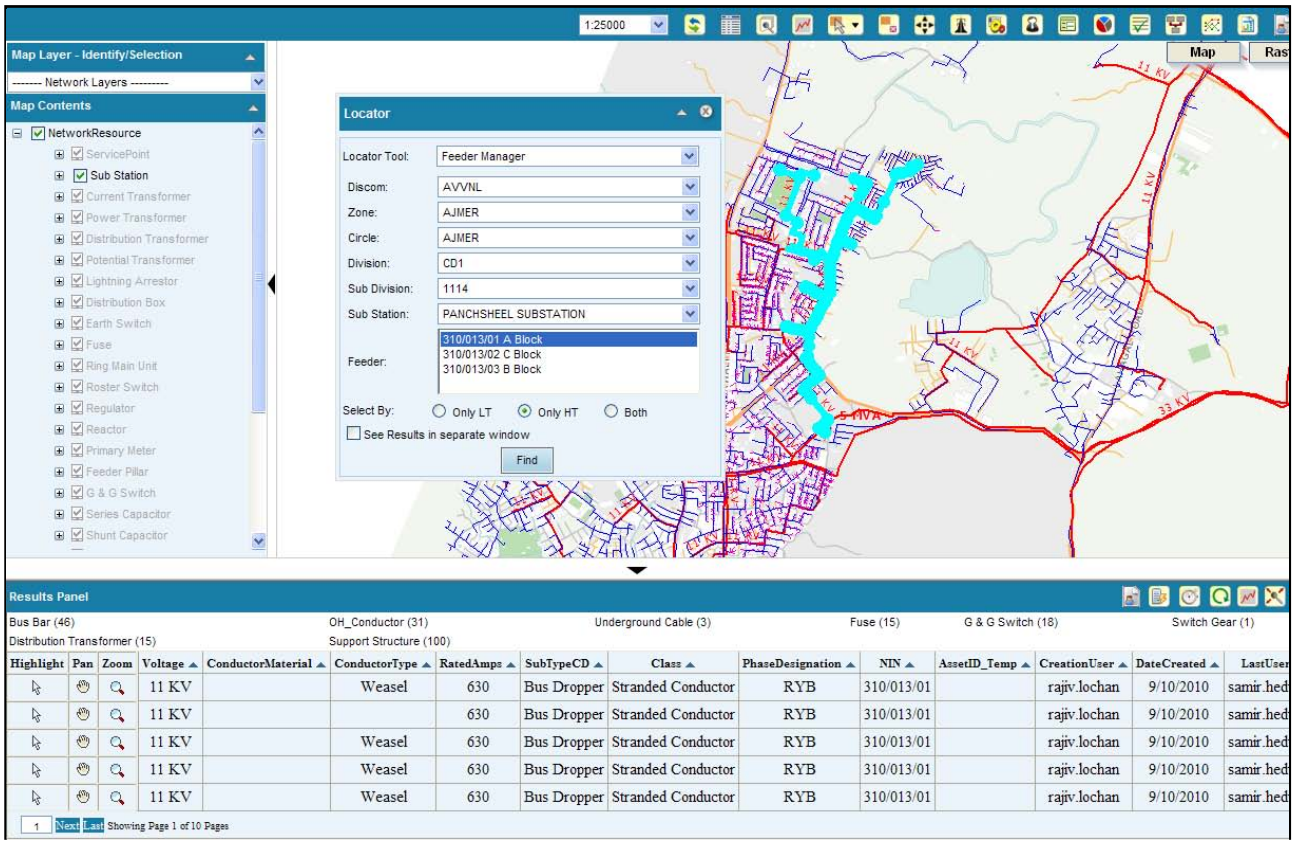
Feeder Manager - Features covered in LT

Author α : Research Scholar Jodhpur National University (Faculty of Computer Application).

Author σ : Restructured Power Development and Reforms Programme.

Feeder Manager – HT option

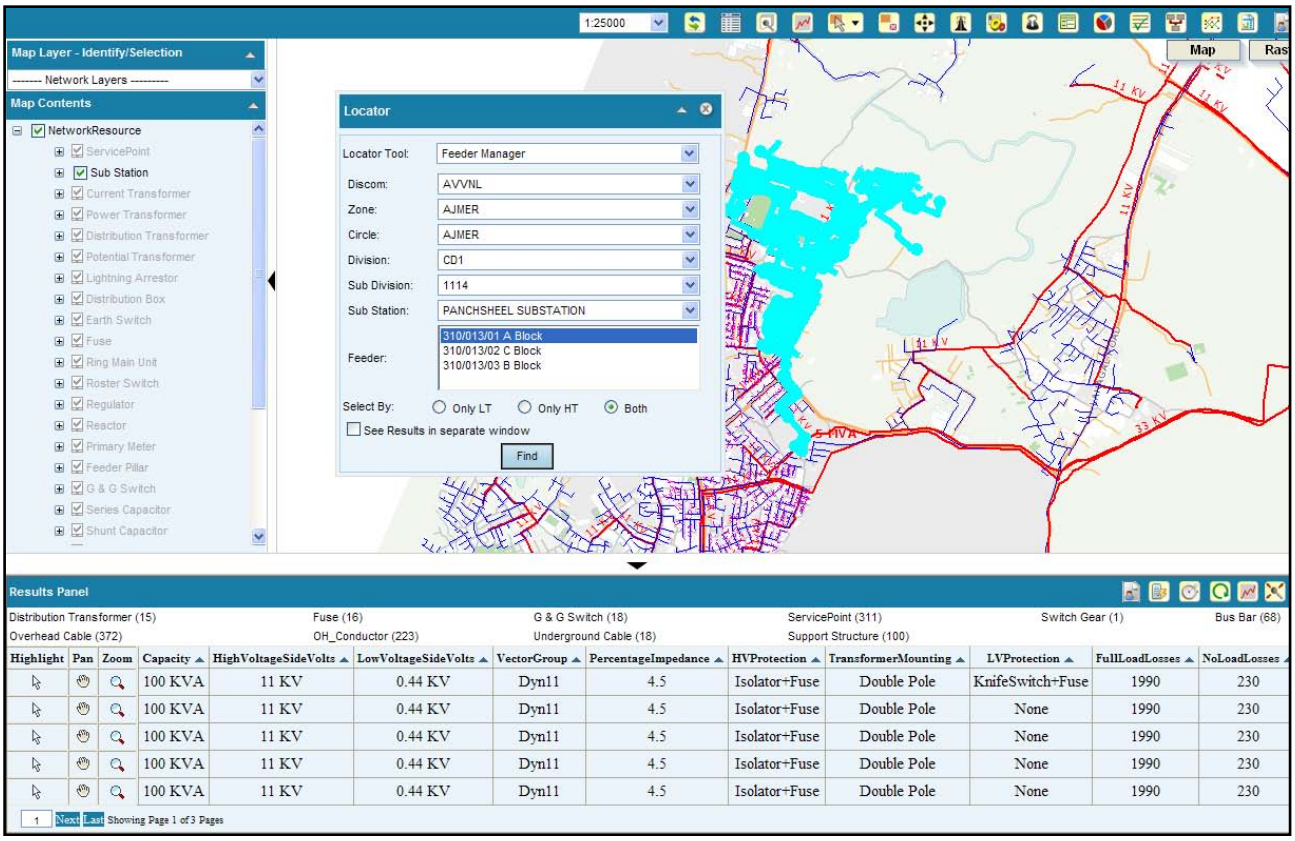
1. Select Feeder Manager in the Locator Tool drop down.
2. Select the values in drop down DISCOM, Zone, Circle, Division, Sub Division and Sub Station.
3. Select a feeder in feeder List box.
4. Select 'Only HT' radio button.
5. Click on Find button.
6. This will highlight the features covered in specified HT and the attributes will be displayed in the results panel.



Feeder Manager – HT Trace

Feeder Manager – Both option

1. Select Feeder Manager in the Locator Tool drop down.
2. Select the values in drop down DISCOM, Zone, Circle, Division, Sub Division and Sub Station.
3. Select a feeder in feeder List box.
4. Select 'Both' radio button.
5. Click on Find button.
6. This will highlight the features of specified Feeder covered in LT and HT network and the attributes of selected features will be displayed in the results panel.



Feeder Manager – Both option

a) Electric Trace

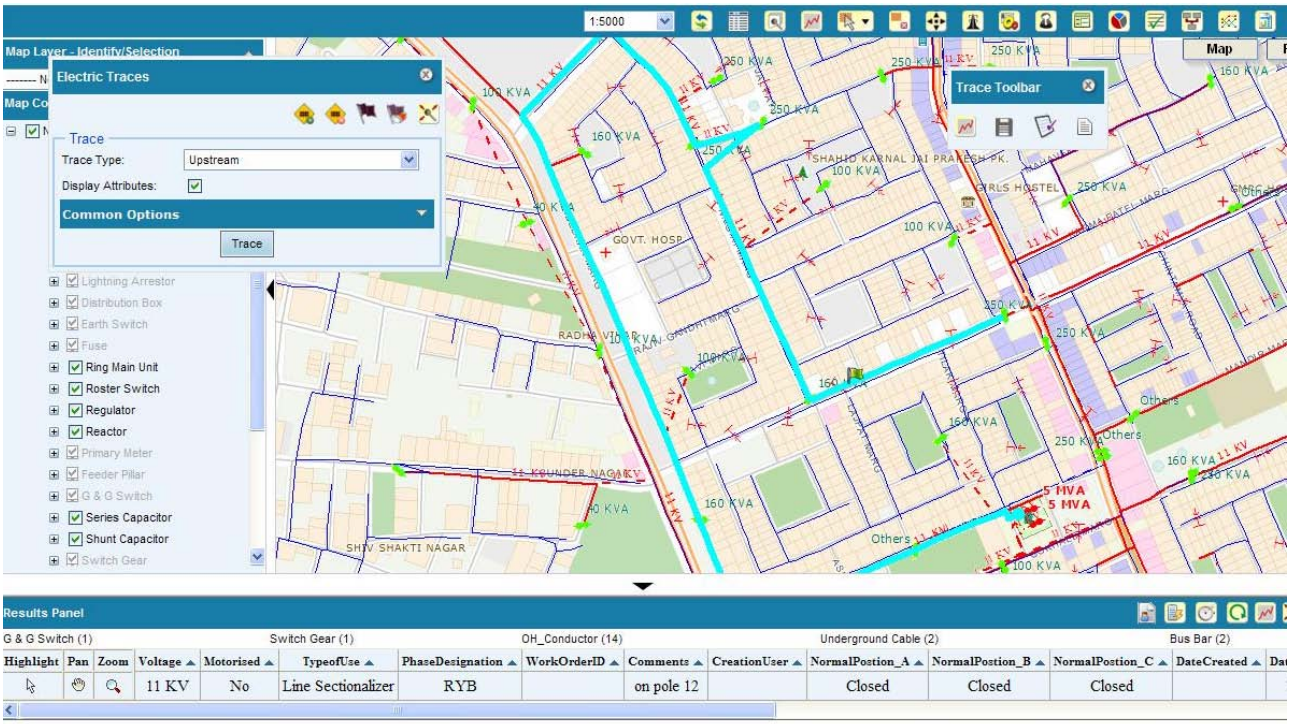
This functionality allows you to perform electric trace on electric network, save the trace result, load the trace result and calculate the length of Conductors and cable participating in trace

1. Click on Electric Trace tool
2. Trace tool bar open with option for Electric Trace, Save Results, Manage Results and Calculate Length.

i. *Electric Trace*

This functionality allow you to perform Upstream, Downstream, Upstream Protective, Downstream Protective, Distribution and Loop trace.

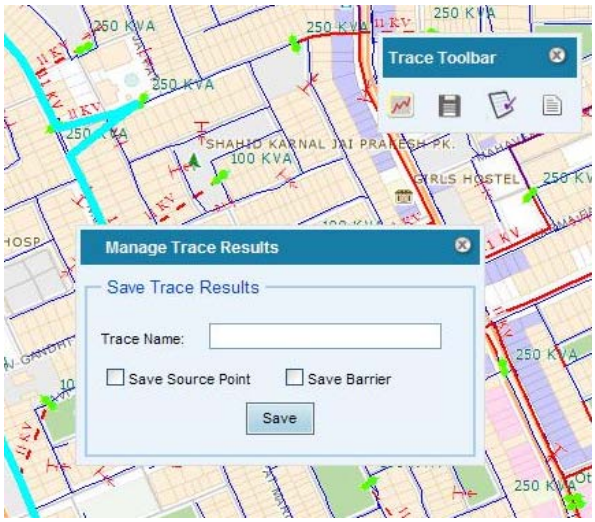
1. Click on Electric Trace tool.
2. Electric Trace dialogue box open.
3. Select a trace type.
4. Select other option depends upon the trace type.
5. Select trace phase.
6. Place flags and barrier on map.
7. Click on Trace button.
8. Feature participated in trace got highlighted in map and displayed in result panel



ii. *Save Results*

This functionality allow you to save the trace result with flags and barriers.

1. Perform Trace
2. Click on save results

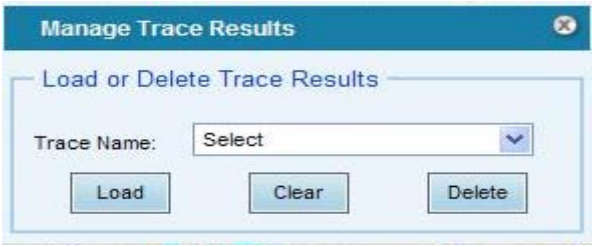


3. Enter Trace name.
4. Select any of the option 'Save Source Point' and 'Save Barrier'
5. Click on save button.
6. Trace result got saved

iii. *Manage Results*

This functionality allows you to load the saved trace result.

1. Trace result should be saved.
2. Click on Manage Results.



3. Select a Trace Name from Trace Name drop down.
4. Click on Load button.
5. Trace result got highlighted in map.
6. Click on Clear button.
7. Trace result got cleared from map.
8. Click on Delete button.
9. Confirmation message pop up.
10. Click on Ok button.
11. Selected trace result got deleted.

References Références Referencias

1. R-APDRP project, Power Finance Corporation of India 2009-2010
2. Ministry of Power, Government of India 2009-2010
3. Jaipur Vidyut Vitiran Nigam Limited, Jaipur 2009 – 2010
4. Ajmer Vidyut Vitiran Nigam Limited, Ajmer 2009 – 2010
5. Jodhpur Vidyut Vitiran Nigam Limited, Jodhpur 2009 – 2010
6. ITIA (Information Technology Implementation Agency), Restructured – Accelerated Power Development and Reform Programme (R-APDRP), Rajasthan 2009 – 2010.

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 12 Issue 10 Version 1.0 May 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Predilection Perspective of Peremptory Evaluation of Wireless Sensor Networks with Machine Learning Approach

By Jagadeeswara Rao.E, Nimmakayala.S.V.Srinivas & Dr.K.V.Ramana

JNTUK,Kakinada, A.P, India

Abstract - Data mining based information processing in Wireless Sensor Network (WSN) is at its preliminary stage, as compared to traditional machine learning and WSN. Currently researches mainly focus on applying machine learning techniques to solve a particular problem in WSN. Different researchers will have different assumptions, application scenarios and preferences in applying machine learning algorithms. These differences represent a major challenge in allowing researchers to build upon each other's work so that research results will accumulate in the community. Thus, a common architecture across the WSN machine learning community would be necessary. One of the major objectives of many WSN research works is to improve or optimize the performance of the entire network in terms of energy conservation and network lifetime. This paper will survey Data Mining in WSN application from two perspectives, namely the Network associated issue and Application associated issue. In the Network associated issue, different machine learning algorithms applied in WSNs to enhance network performance will be discussed. In Application associated issue, machine learning methods that have been used for information processing in WSNs will be summarized.

Keywords : *Wireless Sensor Network, Machine Learning, Data mining, Fusion Center*

GJCST-E Classification: *I.2.6*

Strictly as per the compliance and regulations of:

Predilection Perspective of Peremptory Evaluation of Wireless Sensor Networks with Machine Learning Approach

Jagadeeswara Rao.E [α], Nimmakayala.S.V.Srinivas [σ] & Dr.K.V.Ramana [ρ]

Abstract - Data mining based information processing in Wireless Sensor Network (WSN) is at its preliminary stage, as compared to traditional machine learning and WSN. Currently researches mainly focus on applying machine learning techniques to solve a particular problem in WSN. Different researchers will have different assumptions, application scenarios and preferences in applying machine learning algorithms. These differences represent a major challenge in allowing researchers to build upon each other's work so that research results will accumulate in the community. Thus, a common architecture across the WSN machine learning community would be necessary. One of the major objectives of many WSN research works is to improve or optimize the performance of the entire network in terms of energy conservation and network lifetime. This paper will survey Data Mining in WSN application from two perspectives, namely the Network associated issue and Application associated issue. In the Network associated issue, different machine learning algorithms applied in WSNs to enhance network performance will be discussed. In Application associated issue, machine learning methods that have been used for information processing in WSNs will be summarized.

Keywords : Wireless Sensor Network, Machine Learning, Data mining, Fusion Center.

I. Introduction

Wireless Sensor Network (WSN) is widely considered as one of the most important technologies for the twenty-first century [1]. In the past decades, it has received tremendous attention from both academia and industry all over the world. A WSN typically consists of a large number of low-cost, low-power, and multifunctional wireless sensor nodes, with sensing, wireless communications and computation capabilities. These sensor nodes communicate over short distance via a wireless medium and collaborate to accomplish a common task, for example, environment monitoring, military surveillance, and industrial process control. The basic philosophy behind WSNs is that, while the capability of each individual sensor node is limited, the aggregate power of the entire network is sufficient for the required mission.

Author α : M.Tech. Ad-hoc lecturer, SIT, JNTUH, Hyderabad. 500085, A.P, India. E-mail : jagadish513@gmail.com
Author σ : M.Sc CSE Department JNTUK, Kakinada, 533003, A.P, India. E-mail : nsvsrinivas@gmail.com
Author ρ : Professor, CSE Dept, JNTUK, Kakinada, 533003, A.P, India. E-mail : vamsivihar@gmail.com

II. Network Design Challenges and Routing Issues

The design of routing protocols for WSNs is challenging because of several network constraints. WSNs suffer from the limitations of several network resources, for example energy, bandwidth, central processing unit, and storage [1]. The design challenges in sensor networks involve the following main aspect:

a) Limited Energy Capacity

Since sensor nodes are battery powered, they have limited energy capacity. Energy poses a big challenge for network designers in hostile environments, for example, a battlefield, where it is impossible to access the sensors and recharge their batteries. Furthermore, when the energy of a sensor reaches a certain threshold, the sensor will become faulty and a malfunction can arise, which will have a major impact on the network performance. Thus, routing protocols designed for sensors should be as energy efficient as possible to extend their lifetime, and hence prolong the network lifetime while guaranteeing good performance overall.

b) Sensor locations

Another challenge that faces the design of routing protocols is to manage the locations of the sensors. Most of the proposed protocols assume that the sensors either equipped with Global Positioning System (GPS) receivers or use some localization technique to learn about their locations.

c) Limited Hardware Resources

In addition to limited energy capacity, sensor nodes have limited processing and also storage capacities, and thus can only perform limited computational functionality. These hardware constraints present many challenges in software development and network protocol design for sensor networks, which must not only consider the energy constraint in sensor nodes, but also the processing and storage capacities of sensor nodes.

d) Massive and Random Node Deployment

Sensor node deployment in WSNs is application dependent and can be either manual or random which

finally affects the performance of the routing protocol. In most applications, sensor nodes can be scattered randomly in an intended area or dropped massively over an inaccessible or hostile region. If the resultant distribution of nodes is non uniform, optimal clustering becomes necessary to allow connectivity and enable energy efficient network operation.

e) Network Characteristics and Unreliable Environment

A sensor network usually operates in a dynamic and unreliable environment. The topology of a network, which is defined by the sensors and communication links between the sensors, changes frequently due to sensor addition, deletion, node failures, damages, or energy depletion. Also, the sensor nodes are linked by a wireless medium, which is noisy, error prone, and time varying. Therefore, routing paths should consider network topology dynamics due to limited energy and sensor mobility as well as increasing the size of the network to maintain specific application requirements in terms of coverage and connectivity.

f) Data Aggregation

Since sensor nodes may generate significant redundant data, similar packets from multiple nodes can be aggregated so that the number of transmissions is reduced. Data aggregation technique has been used to achieve energy efficiency and data transfer optimization in a number of routing protocols [2] [3].

g) Diverse Sensing Application Requirements

Sensor networks have a wide range of diverse applications. No network protocol can meet the requirements of all the applications.

III. Background

Information processing in WSNs has three major steps [4] namely pre-processing, data aggregation and inference. Pre-processing is the first step of information processing, it includes simple actions performed on raw data such as signal conditioning (cleaning, compression, scaling and etc.), noise filtering and etc. Data aggregation is the process of aggregating data to the fusion centre or inference centre in WSN. Inference is a process of using machine learning techniques to extract hidden information out of the aggregated data. Most of current researches focus on applying machine learning algorithms to make inference (step three of information processing in WSNs), such as classifying a moving object in a surveillance WSN based on data gathered by the sensors, abnormal environmental event identification in an environment monitoring [5].

IV. Data Mining in Wireless Sensor Networks

One of the major objectives of many WSN research works is to improve or optimize the performance of the entire network in terms of energy-conservation and network lifetime. Most of the research activities focus on the design of efficient routing protocol at the network layer selection of low-power modulation scheme at the physical layer or adoption of power-saving modal of operation at data link layer to achieve energy-awareness in WSNs.

To illustrate how learning is relevant to decentralized inference and to discuss the challenges that WSNs pose, it will be helpful to have a running example at hand [6]. Suppose that the feature space X models the set of measurements observable by sensors in a wireless network. For example, the components of an element x belongs to X = IR may model coordinates in a (planar) environment, and time. Y = IR may represent the space of temperature measurements. A fusion center or the sensors themselves, may wish to know the temperature at some point in space-time; to reflect that these coordinates and the corresponding temperature are unknown prior to the network's deployment, let us model them with the random variable (X, Y). A joint distribution P X Y may model the spatiotemporal correlation structure of a temperature field. If the field's structure is well understood, i.e., if P X Y can be assumed known apriori, then an estimate may be designed within the standard parametric framework. However, if such prior information is unavailable, an alternative approach is necessary.

a) Model for Data Mining in WSN using Distributed Learning

Now let us pose a general model for distributed learning that will aid in formulating the problem and categorizing work with in the field. Suppose that in a network of m sensors, sensor i has acquired a set of measurements, i.e., training data, Si =X × Y. For example Si may represent a stationary sensor's measurements of temperature over the course of a day or a mobile sensor's readings at various points in space-time. Suppose further that the sensors form a wireless network, whose topology is specified by a graph. For example, consider the models depicted pictorially in Figure 1.

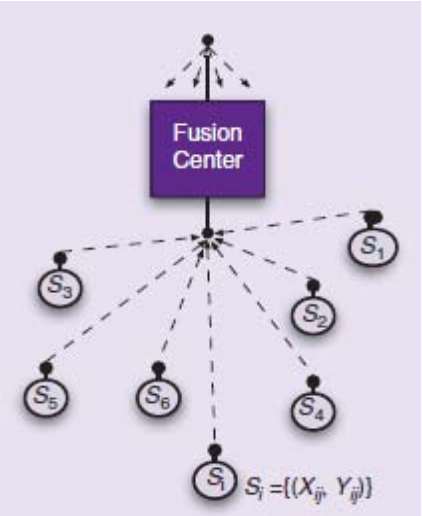


Figure1: Distribute Learning with Fusion Center

Each node in the graph represents a sensor and its locally observed data; an edge in the graph posits the existence of a wireless link between sensors. Note that the fusion center can be modeled as an additional node in the graph, perhaps with larger capacity links between itself and the sensors, to reflect its larger energy supply and computing power. Apriori, this model makes no assumptions on the topology of the network (e.g., the graph is not necessarily connected); However, the success of distributed learning may in fact depend on such properties.

Every sensor of the network can read a single value at time and send the data to the Fusion center using network back bone. Later, Distributed learning in WSNs with a fusion center would like to utilize the data which was collected locally to build the overall estimate of the continuously varying field. To achieve this goal divide the network into different clusters and elect the cluster head which is used to collect the data from its members and send the aggregated or summary information to the Fusion Center.

The second approach is in-network processing as shown in the Figure 2.Much of the work in distributed learning differs in a way that the capacity of the links is modeled. The typical assumption is that the topology of these networks is dynamic and perhaps unknown prior to deployment; a fusion center may exist, but the sensors are largely autonomous and may make decisions independently of the fusion center.

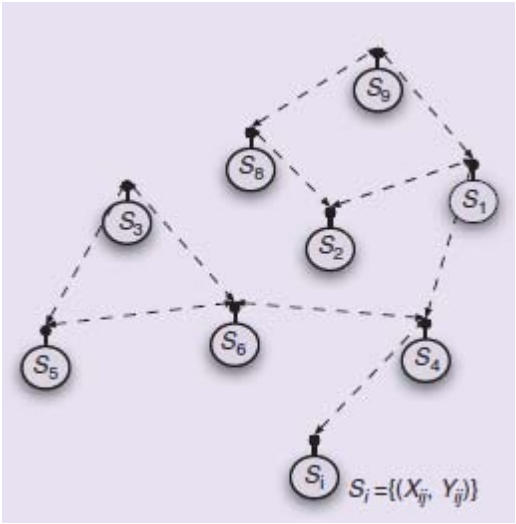


Figure 2: In-network processing

V. Conclusion

This paper surveys the machine learning techniques applied in WSN, from both Networking and Application perspectives. Data mining techniques have been applied in solving problems related to energy-aware communication, optimal sensor deployment and localization, resource allocation and task scheduling in WSNs. In Application domain, data mining methods are mainly used in information processing such as data conditioning, machine inference and etc.

References Références Referencias

1. D. E. D. Culler, and M. Srivastava, "Overview of sensor networks," IEEE Computer, pp. 41-49, 2004.
2. A. C. W. R. Heinzelman, and H. Balakrishnan,, "Energy-Efficient Communication Protocol for Wireless Microsensor Networks," presented at IEEE Proc. Hawaii Int'l. Conf. Sys. Sci., 2000.
3. M. M. Yong Wang, and Li-Shiuan Peh, "A Supervised Learning Approach for Routing Optimizations in Wireless Sensor Networks," 2006.
4. I. E. C. Chien, and C. McConaghy, "Low-Power Direct-Sequence Spread-Spectrum Modem Architecture For Distributed Wireless Sensor Networks," presented at ISLPED Huntington Beach, CA, 2001.
5. R. G. C. Intanagonwiwat, and D. Estrin, "Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks," presented at ACM MobiCom, Boston, MA, 2000.
6. S. R. K. Joel B. Predd, and H. Vincent Poor, "Distributed Learning in Wireless Sensor Networks - application issues and the problem of distributed inference," IEEE Signal Processing Magazine, 2006.

Global Journals Inc. (US) Guidelines Handbook 2012

www.GlobalJournals.org

FELLOW OF ASSOCIATION OF RESEARCH SOCIETY IN COMPUTING (FARSC)

- 'FARSC' title will be awarded to the person after approval of Editor-in-Chief and Editorial Board. The title 'FARSC" can be added to name in the following manner. eg. **Dr. John E. Hall, Ph.D., FARSC or William Walldroff Ph. D., M.S., FARSC**
- Being FARSC is a respectful honor. It authenticates your research activities. After becoming FARSC, you can use 'FARSC' title as you use your degree in suffix of your name. This will definitely will enhance and add up your name. You can use it on your Career Counseling Materials/CV/Resume/Visiting Card/Name Plate etc.
- 60% Discount will be provided to FARSC members for publishing research papers in Global Journals Inc., if our Editorial Board and Peer Reviewers accept the paper. For the life time, if you are author/co-author of any paper bill sent to you will automatically be discounted one by 60%
- FARSC will be given a renowned, secure, free professional email address with 100 GB of space eg.johnhall@globaljournals.org. You will be facilitated with Webmail, Spam Assassin, Email Forwarders, Auto-Responders, Email Delivery Route tracing, etc.
- FARSC member is eligible to become paid peer reviewer at Global Journals Inc. to earn up to 15% of realized author charges taken from author of respective paper. After reviewing 5 or more papers you can request to transfer the amount to your bank account or to your PayPal account.
- Eg. If we had taken 420 USD from author, we can send 63 USD to your account.
- FARSC member can apply for free approval, grading and certification of some of their Educational and Institutional Degrees from Global Journals Inc. (US) and Open Association of Research, Society U.S.A.
- After you are FARSC. You can send us scanned copy of all of your documents. We will verify, grade and certify them within a month. It will be based on your academic records, quality of research papers published by you, and 50 more criteria. This is beneficial for your job interviews as recruiting organization need not just rely on you for authenticity and your unknown qualities, you would have authentic ranks of all of your documents. Our scale is unique worldwide.
- FARSC member can proceed to get benefits of free research podcasting in Global Research Radio with their research documents, slides and online movies.
- After your publication anywhere in the world, you can upload you research paper with your recorded voice or you can use our professional RJs to record your paper their voice. We can also stream your conference videos and display your slides online.
- FARSC will be eligible for free application of Standardization of their Researches by Open Scientific Standards. Standardization is next step and level after publishing in a journal. A team of research and professional will work with you to take your research to its next level, which is worldwide open standardization.

- FARSC is eligible to earn from their researches: While publishing his paper with Global Journals Inc. (US), FARSC can decide whether he/she would like to publish his/her research in closed manner. When readers will buy that individual research paper for reading, 80% of its earning by Global Journals Inc. (US) will be transferred to FARSC member's bank account after certain threshold balance. There is no time limit for collection. FARSC member can decide its price and we can help in decision.

MEMBER OF ASSOCIATION OF RESEARCH SOCIETY IN COMPUTING (MARSC)

- 'MARSC' title will be awarded to the person after approval of Editor-in-Chief and Editorial Board. The title 'MARSC" can be added to name in the following manner. eg. Dr. John E. Hall, Ph.D., MARSC or William Walldroff Ph. D., M.S., MARSC
- Being MARSC is a respectful honor. It authenticates your research activities. After becoming MARSC, you can use 'MARSC' title as you use your degree in suffix of your name. This will definitely will enhance and add up your name. You can use it on your Career Counseling Materials/CV/Resume/Visiting Card/Name Plate etc.
- 40% Discount will be provided to MARSC members for publishing research papers in Global Journals Inc., if our Editorial Board and Peer Reviewers accept the paper. For the life time, if you are author/co-author of any paper bill sent to you will automatically be discounted one by 60%
- MARSC will be given a renowned, secure, free professional email address with 30 GB of space eg.johnhall@globaljournals.org. You will be facilitated with Webmail, Spam Assassin, Email Forwarders, Auto-Responders, Email Delivery Route tracing, etc.
- MARSC member is eligible to become paid peer reviewer at Global Journals Inc. to earn up to 10% of realized author charges taken from author of respective paper. After reviewing 5 or more papers you can request to transfer the amount to your bank account or to your PayPal account.
- MARSC member can apply for free approval, grading and certification of some of their Educational and Institutional Degrees from Global Journals Inc. (US) and Open Association of Research, Society U.S.A.
- MARSC is eligible to earn from their researches: While publishing his paper with Global Journals Inc. (US), MARSC can decide whether he/she would like to publish his/her research in closed manner. When readers will buy that individual research paper for reading, 40% of its earning by Global Journals Inc. (US) will be transferred to MARSC member's bank account after certain threshold balance. There is no time limit for collection. MARSC member can decide its price and we can help in decision.

AUXILIARY MEMBERSHIPS

ANNUAL MEMBER

- Annual Member will be authorized to receive e-Journal GJMBR 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) First, register yourself using top right corner of Home page then Login. If you are already registered, then login using your username and password.

(II) Choose corresponding Journal.

(III) Click 'Submit Manuscript'. Fill required information and Upload the paper.

(B) If you are using Internet Explorer, 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.

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 Swis 721 Lt BT.
- 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 three 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 Inc. (US) welcome the submission of original paper, review paper, survey article relevant to the all the streams of Philosophy and knowledge. The Global Journals Inc. (US) 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 Inc. (US) 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 Inc. (US) and Editorial Board, will become the copyright of the Global Journals Inc. (US).

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 Inc. (US) 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 Inc. (US), 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 Inc. (US) 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 Inc. (US) homepage at the judgment of the Editorial Board.

The Editorial Board and Global Journals Inc. (US) 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 Inc. (US) 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 Inc. (US) 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 Inc. (US).

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 Inc. (US) (Publication Prior to Print)

The Global Journals Inc. (US) 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 .

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 Inc. (US)

Please carefully note down following rules and regulation before submitting your Research Paper to Global Journals Inc. (US):

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 Inc. (US)

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 Inc. (US).

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

P

R

S

T

V

W

save our planet

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