

INTERNATIONAL JOURNAL OF
COMPUTER SCIENCE AND SECURITY (IJCSS)

ISSN : 1985-1553

Publication Frequency: 6 Issues / Year



CSC PUBLISHERS
<http://www.cscjournals.org>

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND SECURITY (IJCSS)

VOLUME 6, ISSUE 1, 2011

**EDITED BY
DR. NABEEL TAHIR**

ISSN (Online): 1985-1553

International Journal of Computer Science and Security is published both in traditional paper form and in Internet. This journal is published at the website <http://www.cscjournals.org>, maintained by Computer Science Journals (CSC Journals), Malaysia.

IJCSS Journal is a part of CSC Publishers

Computer Science Journals

<http://www.cscjournals.org>

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND SECURITY (IJCSS)

Book: Volume 6, Issue 1, February 2012

Publishing Date: 21 - 02- 2012

ISSN (Online): 1985 -1553

This work is subjected to copyright. All rights are reserved whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication of parts thereof is permitted only under the provision of the copyright law 1965, in its current version, and permission of use must always be obtained from CSC Publishers.

IJCSS Journal is a part of CSC Publishers

<http://www.cscjournals.org>

© IJCSS Journal

Published in Malaysia

Typesetting: Camera-ready by author, data conversion by CSC Publishing Services – CSC Journals, Malaysia

CSC Publishers, 2012

EDITORIAL PREFACE

This is first issue of volume six of the International Journal of Computer Science and Security (IJCSS). IJCSS is an International refereed journal for publication of current research in computer science and computer security technologies. IJCSS publishes research papers dealing primarily with the technological aspects of computer science in general and computer security in particular. Publications of IJCSS are beneficial for researchers, academics, scholars, advanced students, practitioners, and those seeking an update on current experience, state of the art research theories and future prospects in relation to computer science in general but specific to computer security studies. Some important topics cover by IJCSS are databases, electronic commerce, multimedia, bioinformatics, signal processing, image processing, access control, computer security, cryptography, communications and data security, etc.

The initial efforts helped to shape the editorial policy and to sharpen the focus of the journal. Starting with volume 6, 2012, IJCSS appears in more focused issues. Besides normal publications, IJCSS intend to organized special issues on more focused topics. Each special issue will have a designated editor (editors) – either member of the editorial board or another recognized specialist in the respective field.

This journal publishes new dissertations and state of the art research to target its readership that not only includes researchers, industrialists and scientist but also advanced students and practitioners. The aim of IJCSS is to publish research which is not only technically proficient, but contains innovation or information for our international readers. In order to position IJCSS as one of the top International journal in computer science and security, a group of highly valuable and senior International scholars are serving its Editorial Board who ensures that each issue must publish qualitative research articles from International research communities relevant to Computer science and security fields.

IJCSS editors understand that how much it is important for authors and researchers to have their work published with a minimum delay after submission of their papers. They also strongly believe that the direct communication between the editors and authors are important for the welfare, quality and wellbeing of the Journal and its readers. Therefore, all activities from paper submission to paper publication are controlled through electronic systems that include electronic submission, editorial panel and review system that ensures rapid decision with least delays in the publication processes.

To build its international reputation, we are disseminating the publication information through Google Books, Google Scholar, Directory of Open Access Journals (DOAJ), Open J Gate, ScientificCommons, Docstoc and many more. Our International Editors are working on establishing ISI listing and a good impact factor for IJCSS. We would like to remind you that the success of our journal depends directly on the number of quality articles submitted for review. Accordingly, we would like to request your participation by submitting quality manuscripts for review and encouraging your colleagues to submit quality manuscripts for review. One of the great benefits we can provide to our prospective authors is the mentoring nature of our review process. IJCSS provides authors with high quality, helpful reviews that are shaped to assist authors in improving their manuscripts.

Editorial Board Members

International Journal of Computer Science and Security (IJCSS)

EDITORIAL BOARD

EDITOR-in-CHIEF (EiC)

Dr. Haralambos Mouratidis
University of east London (England)

ASSOCIATE EDITORS (AEiCs)

Associate Professor. Azween Bin Abdullah
Universiti Teknologi Petronas,
Malaysia

Dr. Padmaraj M. V. nair
Fujitsu's Network Communication division in Richardson
Texas, USA

Dr. Blessing Foluso Adeoye
University of Lagos,
Nigeria

EDITORIAL BOARD MEMBERS (EBMs)

Professor. Abdel-Badeeh M. Salem
Ain Shams University
Egyptian

Professor. Sellappan Palaniappan
Malaysia University of Science and Technology
Malaysia

Professor Mostafa Abd-El-Barr
Kuwait University
Kuwait

Professor. Arun Sharma
Amity University
India

Dr. Alfonso Rodriguez
University of Bio-Bio
Chile

Dr. Debotosh Bhattacharjee
Jadavpur University
India

Dr. Teng li Lynn
University of Hong Kong
Hong Kong

Dr. Chiranjeev Kumar

Indian School of Mines University
India

Dr. Ghossoon M. Waleed

University Malaysia Perlis
Malaysia

Dr. Srinivasan Alavandhar

Caledonian University
Oman

Dr. Deepak Laxmi Narasimha

University of Malaya
Malaysia

Assistant Professor Vishal Bharti

Maharishi Dayanand University
India

Dr. Parvinder Singh

University of Sc. & Tech
India

TABLE OF CONTENTS

Volume 6, Issue 1, February 2012

Pages

1 – 18	Prevention of Phishing Attacks Based on Discriminative Key Point Features of WebPages <i>Mallikka Rajalingam, Salah Ali Alomari, Putra Sumari</i>
19 – 28	Using Cipher Key to Generate Dynamic S-Box in AES Cipher System <i>Razi Hosseinkhani, Seyyed Hamid Haj Seyeed Javadi</i>
29 – 33	Recourse Management Using a Fair Share Scheduler <i>Suja Cherukullapurath Mana</i>
34 – 42	Performance Evaluation of Reactive, Proactive and Hybrid Routing Protocols Based on Network Size for MANET <i>Ritika , Nipur</i>
43 – 52	Semantic Message Addressing based on Social Cloud Actor's Interests <i>Reem M. Bahgat, Akram Ibrahim Salah, Hamada I. Abdul Wakeil</i>
53 – 61	Algorithm Algorithm and Programme for Computation of Forces Acting on line Supports <i>Abdulaziz Salem Bahaidara</i>
62 – 78	A Micro-Mobility Management Scheme for Handover and Roaming <i>Debabala Swain, Siba Prasada Panigrahi, Prasanta Kumar Patra</i>
79 – 93	Audio Steganography Coding Using the Discreet Wavelet Transforms <i>Siwar Rekik, Driss Guerchi, Habib Hamam, Sid-Ahmed Selouani</i>
94 – 102	New Proposed classic Cluster Layer Architecture for Mobile Adhoc Network (cclam) <i>Kuldeep Sharma, Nikhil Khandelwal, Sanjeev Kumar Singh</i>

103- 110	Quality and Distortion Evaluation of Audio Signal by Spectrum <i>Er. Niranjan Singh, Dr. Bhupendra Verma</i>
----------	---

Prevention of Phishing Attacks Based on Discriminative Key Point Features of WebPages

Mallikka Rajalingam

*School of Computer Sciences
Universiti Sains Malaysia
Pulau Penang, 11800, Malaysia*

mallikka2002@yahoo.com

Saleh Ali Alomari

*School of Computer Sciences
Universiti Sains Malaysia
Pulau Penang, 11800, Malaysia*

salehalomari2005@yahoo.com

Putra Sumari

*School of Computer Sciences
Universiti Sains Malaysia
Pulau Penang, 11800, Malaysia*

putras@cs.usm.my

Abstract

Phishing is the combination of social engineering and technical exploits designed to convince a victim to provide personal information, usually for the monetary gain of the attacker (Phisher). Attempts to stop phishing by preventing a user from interacting with a malicious web site have shown to be ineffective. In this paper, present an effective image-based anti-phishing scheme based on discriminative key point features in WebPages. We use an invariant content descriptor, the Contrast Context Histogram (CCH), to compute the similarity degree between suspicious pages and authentic pages. To determine whether two images are similar, a common approach involves extracting a vector of salient features from each image, and computing the distance between the vectors, which is taken as the degree of visual difference between the two images. The results show that the proposed scheme achieves high accuracy and low error rates.

Keywords: Image Clustering and Retrieval, Anti-Phishing Mechanism, Digital Image Processing, Security

1. INTRODUCTION

Phishing is also known as "brand spoofing". It is pronounced as fishing. The word has its origin from two words "Password harvesting" or "fishing for passwords". Phishing is a type of deception designed to steal your valuable personal data, such as credit card numbers, passwords, account data, or other information. Phishing is a form of online identity theft associated with both social engineering and technical subterfuge. Attackers might send millions of fraudulent e-mail messages that appear to come from Web sites you trust, like your bank or credit card Company, and request that you provide personal information [25]. As scam artists become more sophisticated, so do their phishing e-mail messages and pop-up windows, they often include official-looking logos from real organizations and other identifying information taken directly from legitimate Web sites. When users unwittingly browse phishing pages and enter their personal information like user name and password their password will get stored in the attackers database and then users are redirected to original sites directly by way of phisher-controlled proxies. Phishing has thus become a serious threat to information security and Internet privacy [16]. To deceive users into thinking phishing sites are legitimate, fake pages are often designed to look almost the same as the official ones in both layout and content. Phishers might insert an arbitrary advertisement banner that redirects users to another malicious Web site if they click on it. So, phishing attacks have become a serious threat. To reduce phishing attacks there is a group called APWG (Anti Phishing Working Group)

which will have a list of phishing pages. If a user finds that the page he visits is a phishing page then he can report it to the APWG [10]. They will add that page in the list of phishing page. First to find whether the page is a phishing page or real page, we've developed a color based image comparison method. Color plays a vital role in an image. Even a small difference can be found by comparing images based on color.

Nowadays, the phishing attack has become a bigger problem. It results in stealing One's personal information like Gmail account and bank password. To avoid phishing attacks many methods are developed, but none of the method is more efficient enough to solve such this kind of problems and still the phishing attacks takes place. The method that we developed here is purely image-based [4]. Snapshot of the requested page is taken. The page is stored as an image then the next step is to get the original page snapshot which is also saved as an image. Then select the source image as well as the select the target directory which contains the images to be compared. The images are compared by using color ratio. The difference is noted and reported to the user. When the difference is zero then the page is not a phishing page. This anti phishing tool is very efficient because it compares the phishing and authentic pages based on the visual appearance level, instead of rather than using text-based analysis [7].

1.1 A Growing Problems in Phishing

The phish attack volume increased 33% in April to 36,557 attacks, continuing the growth trend from March. Phish attacks had been in general decline from August 2009 to February 2010, but now look set to return to the seasonal growth trend that has historically peaked in late Summer/early Fall [9]. In August 2009, for example, the high point of fast-flux phish attacks Produced 60,678 incidents. As shown in Figure. 1, the monthly attacks from April 2009 to April 2010 averaged 45,605. Phish attack volume has not returned to the level seen in April 2009, but note that this chart does not include branded malware attacks, which cybercriminals are likely to have launched during periods of lower phish volumes.

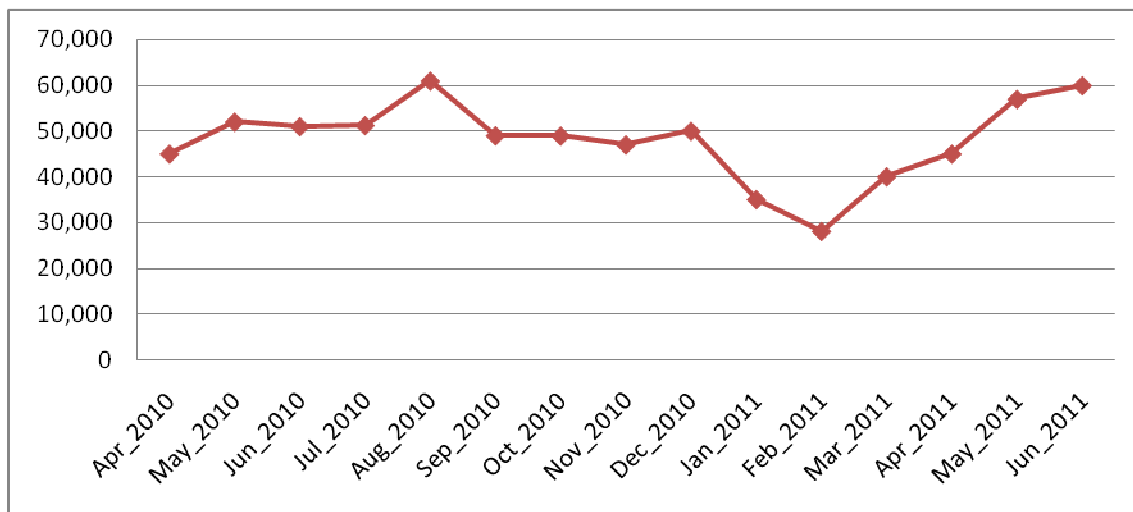


FIGURE 1: Monthly Phishing Attack

As shown in the Figure.2, the payment services sector was the primary sector favored by phishers accounting for 41% of phish attacks in April. The financial sector, historically the most popular phishing sector, accounted for 33% of phish attacks. The auction sector was targeted in 7% of attacks [8]. The "Other" category, which includes social networks, online gaming, online media, various Internet companies, as well as other organizations, accounted for 14% of attacks.

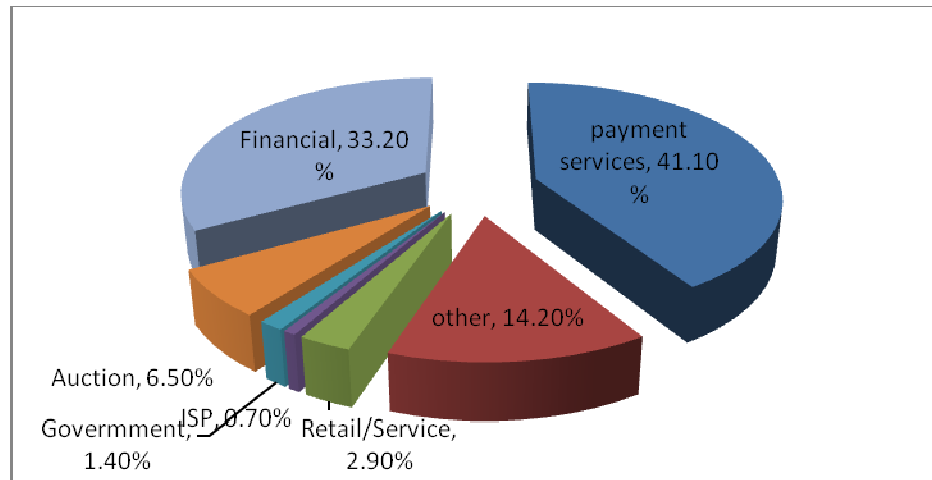


FIGURE 2: Phishing by Industry

1.2 Phishing Attack

Employ visual elements from target site. Most methods of phishing use some form of technical deception designed to make a link in an e-mail (and the spoofed website it leads to) appear to belong to the spoofed organization. Misspelled URLs or the use of sub domains are common tricks used by phishers [11]. Example: www.gmail.com – original link, www.gmai1.com – Fake link. Here are a few phrases that a phishing page may contain verify your account, businesses should not ask you to send passwords, login names, social security numbers, or other personal information through e-mail.

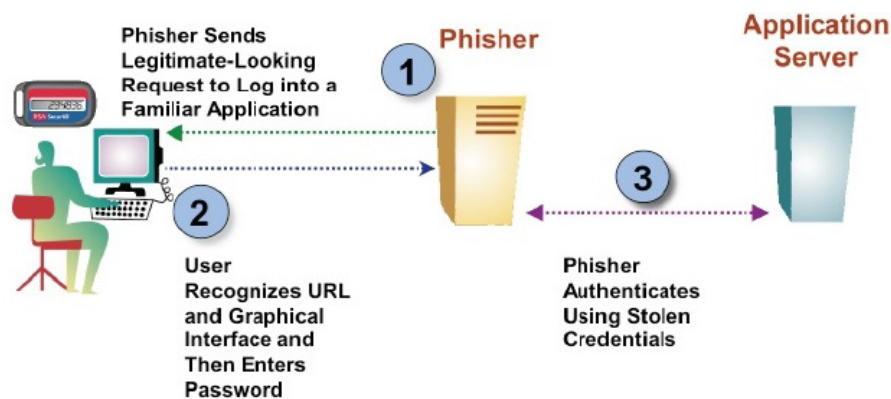


FIGURE 3: Phishing Attack

From the Figure.3, if you receive an e-mail from anyone asking you to update your credit card information, do not respond, this is a phishing scam. If you don't respond within 48 hours, your account will be closed. These messages convey a sense of urgency so that you will respond immediately without thinking. In the Figure.4, the phishing e-mail might even claim that your response is required because your account might have been compromised [3].

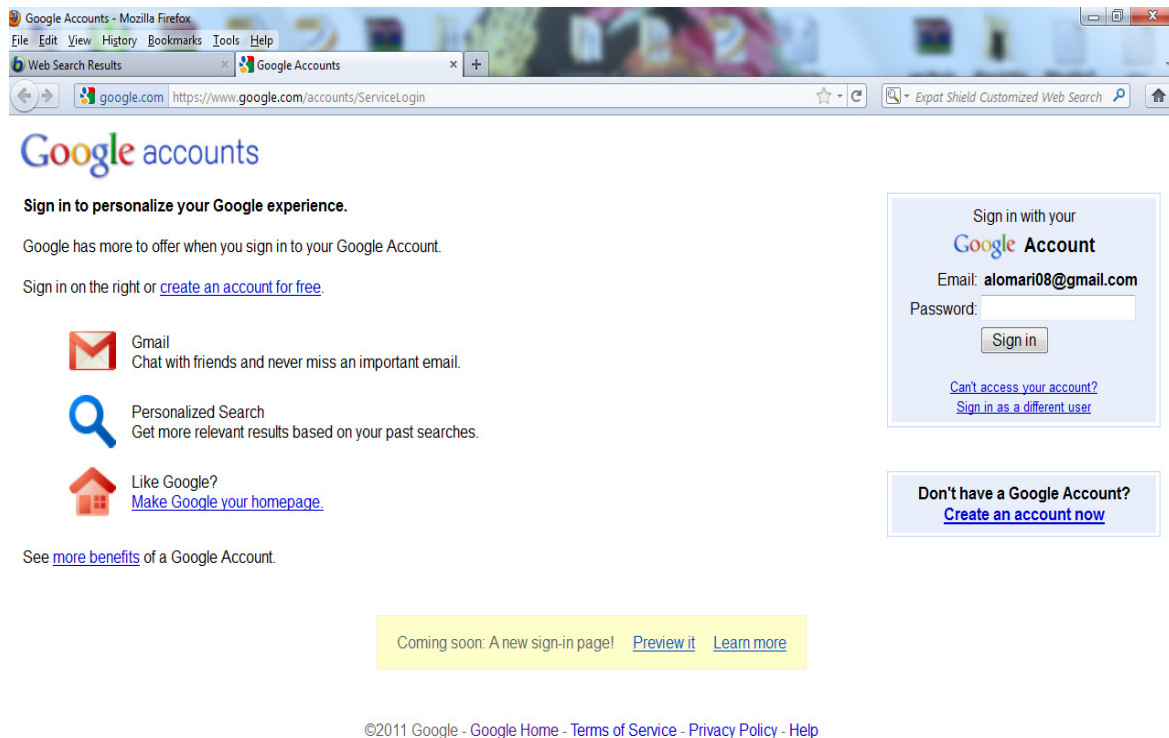


FIGURE 4: Phishing page

The above page looks like an original Gmail page. But it is a phishing page. Whenever this type of page appears before a user then the user enters the user name and password which gets stored in the attackers database. This type of attack will be a serious one if the attacker steals the user's bank user name and password and misuse it.

The remaining of this paper is organized as follows. Basic characteristics of phishing techniques and related works are described in section 2. The methodology and approaches of phishing attacks are discussed in section 3. Various performance testing techniques are in section 4. Results and outputs are in section 5. Then we summarize the whole procedure and draw conclusion in section 6.

2. RELATED WORK

In a SOPHOS white paper-2005, Phish Guru is an embedded training system that teaches users to avoid falling for phishing attacks by sending them simulated phishing emails. People access these training emails in their inbox when they check their regular email. The training emails look just like phishing emails, urging people to go to some website and login. If people fall for the training email that is, if they click on a link in that email. We provide an intervention message that explains that they are at risk for phishing attacks and offers tips they can follow to protect themselves. The training materials present the user with a comic strip that defines phishing, offers steps the user can follow to avoid falling for phishing attacks, and illustrates how easy it is for criminals to perpetrate such attacks [2].

Defending the weakest link, phishing websites detection by analyzing user behaviors, we have used a novel paradigm analysis of the users' behaviors to detect phishing websites. We have shown that it is an accurate method, discussed how it has been designed and implemented to be hard to circumvent, and have discussed its unique strength in protecting users from phishing threats. UBPD is not designed to replace existing techniques. Rather it should be used to

complement other techniques, to provide better overall protection. We believe our approach fills a significant gap in current anti-phishing technology capability.

The image matching is a fundamental problem in computer vision. The existing prevention and detection schemes to combat Phishing in multiple ways. The endless competition between computer virus writers and antivirus software developers, phishers will certainly strive to develop countermeasures against antiphishing solutions. In the existing content-based approach, this analyzes the HTML code and text on a webpage, proved effective in detecting phishing pages. However, phishers responded by compiling phishing pages with non-HTML components, such as images, flash objects, and Java applets. The existing system phisher may design a fake page which is composed entirely of images, even if the original page only contains text information. In this case, the suspect page becomes unanalyzable by content based anti-phishing tools as its HTML code contains nothing but HTML elements [6]. The drawback of existing systems are ineffective to stop phishing attacks, low degree of accuracy, high error rates, not susceptible to changes in webpage aspect ratio and colors used.

Juan Chen and Chuanxiong Guo proposed a new end-host based anti-phishing algorithm, which we call LinkGuard, by utilizing the generic characteristics of the hyperlinks in phishing attacks. These characteristics are derived by analyzing the phishing data archive provided by the Anti-Phishing Working Group (APWG). Because it is based on the generic characteristics of phishing attacks, LinkGuard can detect not only known but also unknown phishing attacks [21]. Bryan Parno, Cynthia Kuo, and Adrian Perrig proposed using a trusted device to perform mutual authentication that eliminates reliance on perfect user behavior, towards Man-in-the-Middle attacks after setup, and protects a user's account even in the presence of keyloggers and most forms of spyware. We demonstrate the practicality of our system with a prototype implementation [22]. A *spammer* is a person who creates spam messages. *Fraudsters* are people involved in Internet fraud, a practice indulged in by individuals who spam potential victims. It has been reported that in 2003 alone, personal losses amounting to more than 200 million dollars resulted from fraudulent intrusions [23]. Tom Jagatic, Nathaniel Johnson, Markus Jakobsson, and Filippo Menczer proposed context aware phishing, an attacker would gain the trust of victims by obtaining information about their bidding history or shopping preferences (freely available from eBay), their banking institutions (discoverable through their Web browser history, made available via cascading style sheets), or their mothers' maiden names (which can be inferred from data required by law to be public) [24].

In this paper we proposed detecting phishing pages based on the similarity between the phishing and authentic pages at the visual appearance level, instead of rather than using text-based analysis. We first take a snapshot of a suspect webpage and treat it as an image in the remainder of the detection process. We also propose image-based phishing detection scheme that uses the Color ratio and color modes such as RGB to compare images, finally after compared the result will show whether authentic webpage is phishing webpage or not. Our scheme can detect phishing pages with a high degree of accuracy.

2.1 Proposed Solution

Phishing attack has become a serious threat to internet users. It results in stealing one's personal information like Gmail password, bank password, etc. It is an illegal way. To reduce phishing attacks there are many methods developed to avoid phishing attack. The method proposed here is very different. It's purely based on image comparison rather dealing with old text based analysis anti-phishing mechanism. It compares original and authentic webpage images and produces the result [4] [5]. First snapshot of the suspected web page is taken and compared with original web page and the result of the comparison helps the user to identify the phishing page. The main objective of the project is to prevent phishing attacks. To make Online Banking and transaction of money more secured. To prevent the users of gmail, rapidshare, paypal, ebay, etc. getting hacked. To prevent the users loss of data in Internet.

3. METHODOLOGY AND APPROACH

There are four phases 1) Phishing attack demo 2) Web page snapshot 3) Image wizard 4) Comparison of web pages.

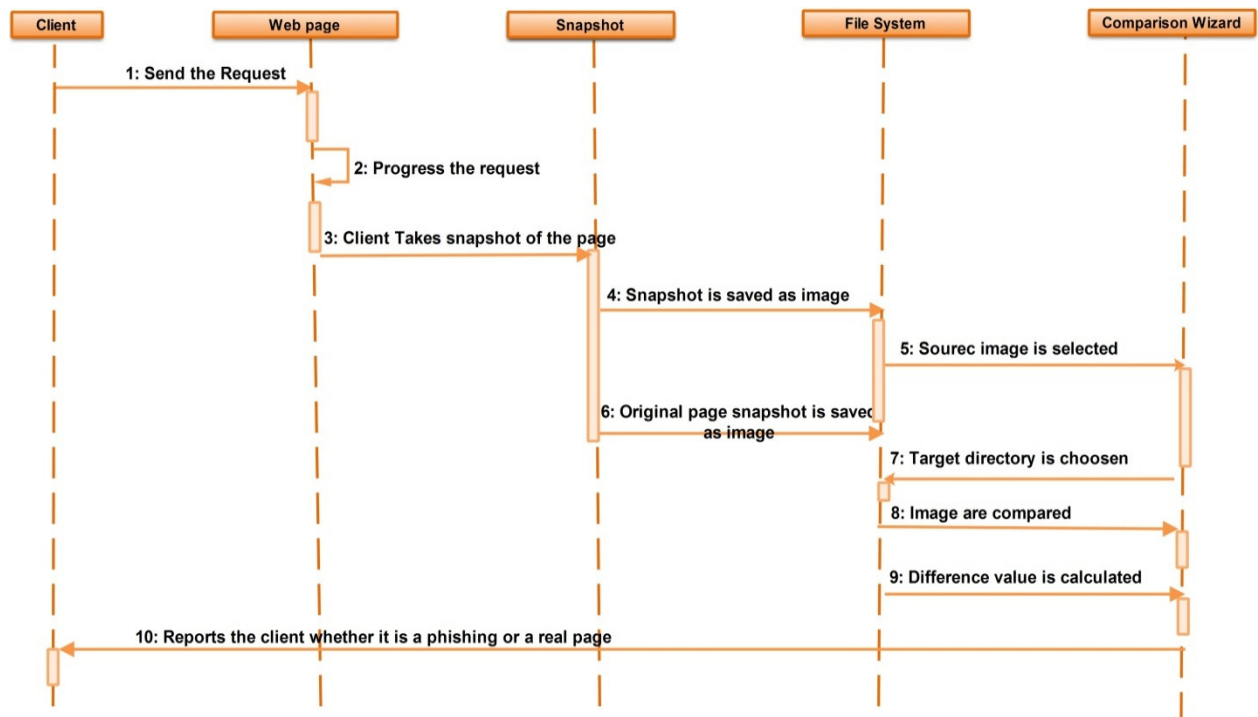


FIGURE 5: Sequence Diagram for Prevention of Phishing Attack

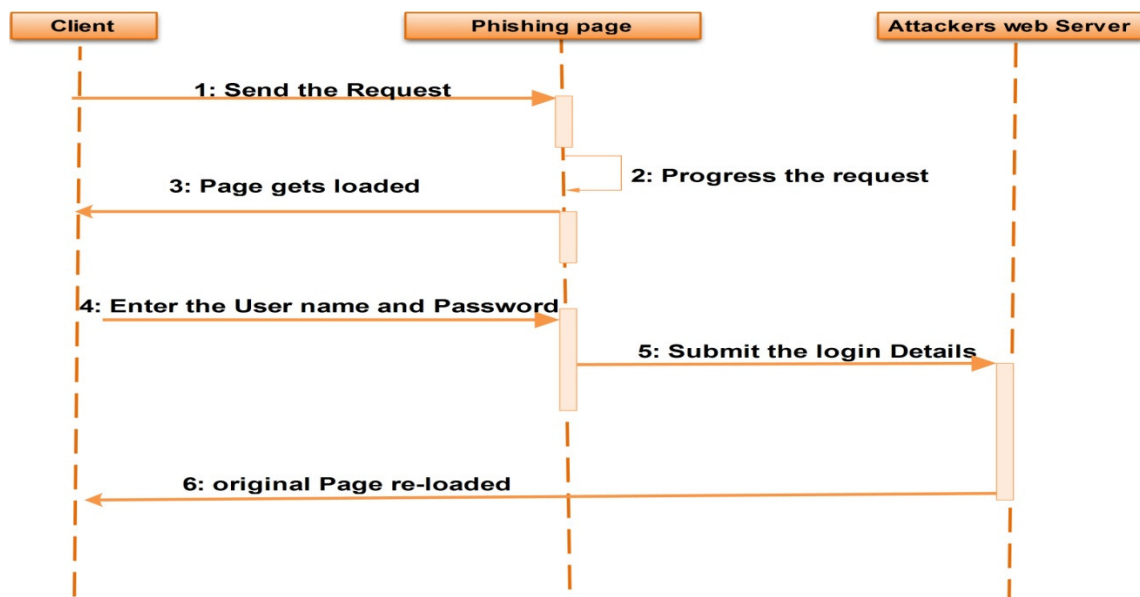


FIGURE 6: Sequence Diagram for Attack

3.1 Phishing Attack Demo

Phishing attack is performed to steal one's personal information. When a user requests a web page the phishers will send their web page which they have developed [13]. They will develop a

phishing page which will be same as that of the original page but there will be some slight differences. Attackers will send it to the user. For example, in the Figure.7 to steal the bank information of a particular user the attackers will send that "the account will expire within today if you fail to fill in the details in the given site" and a link will be provided below. The link which is given will not be the original bank's website. It will contain some official logos which will look similar to the original web site of a bank. Sometimes there will be change in the name of the website in just one character which will be hard for a user to find out. For example, www.ebay.com will be given as www.e6ay.com. Suddenly when the user sees a page with the above specified link they will believe it as an original page. Unknowingly the user enters their password or some personal information which will be taken directly to the phishers server and will get stored in their database. Later the attackers misuse the information given by the user. By using HTML and PHP script, this attack is carried out.

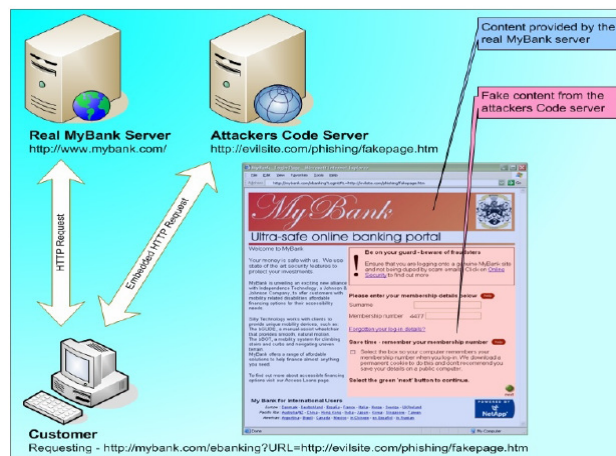


FIGURE 7: E-Banking Fake Page [26]

3.2 Web Page Snapshot

Next step is to take the snapshot of the authentic page. In Figure.9 shows the snapshot of the authentic page we use a tool which will take snapshot of webpage and save in the file system in the required image format. It should be saved only in any of the image format because the web page has to be compared with the original web page. Here specialized tool is needed because we can't take the snapshot normally using print screen key in keyboard. By using print screen key the user can take the whole windows environment and not the required web page alone. This will not give a correct result because if the snapshot of the original webpage image is taken in windows, and when the snapshot of the authentic page is taken in Linux operating system the environment differs and the result will be error prone. So, a tool is necessary to take the snapshot of the web page.

3.3 Image Wizard

Next is to design a wizard to compare the images. In Figure.10 shows the Wizard is designed in such a way that everything appears in the wizard is clear and systematic. Separators are used to clearly distinguish each one. The upcoming window gives instruction to proceed to next window. First the search image is selected and the target directory should be specified in the next step. The panels are designed user friendly and also image panels are used in this wizard to preview the images that are chosen already. If there are no images in the specified target directory the wizard is designed in such a way that an error will be displayed. So, that the user doesn't waste their time by going to the next step of comparing images. Other than that the wizard can get the settings from the user so that sometimes users can give the level of accuracy they needed while comparing images. If out of bound values are given then the wizard takes the default value that is specified. First the original image is taken from the directory which is already stored in that directory. Then we have to specify the target directory which contains similar images. In Figure.11

shows the wizard is designed in such a way that default setting can also be set in preferences window.

3.4 Comparison of Images

Next step is to compare the images. As said earlier in image wizard module user can give the ratio of the accuracy they need while comparing images [1]. First the user is allowed to enter the number of sections by which the image should be divided. Then the image is divided into blocks as given by the user. The target image is also divided into same number of blocks like the original image. The image is divided into blocks by using k-means algorithm. If the user gives “n” number of sections then both the images will be divided into “n*n” number of blocks. For example, if the user gives number of section=3 then both images will be divided into 9 blocks. Get the height and width of the both the images. In this wizard we can also give the number of overlapping value. Instead of taking and comparing each and every whole block, we can also compare blocks that are overlapping. So that can obtain a clear and error prone result. The overlapping value given by the user is taken and it is multiplied with the width and height of the image. By this way we can calculate for overlapping blocks also. Next step is to give the color ratio for the image. First the RGB values of both the images are obtained. Then the average value of the RGB color is obtained. In next step the standard deviation is obtained. Standard deviation determines the range of the colors.

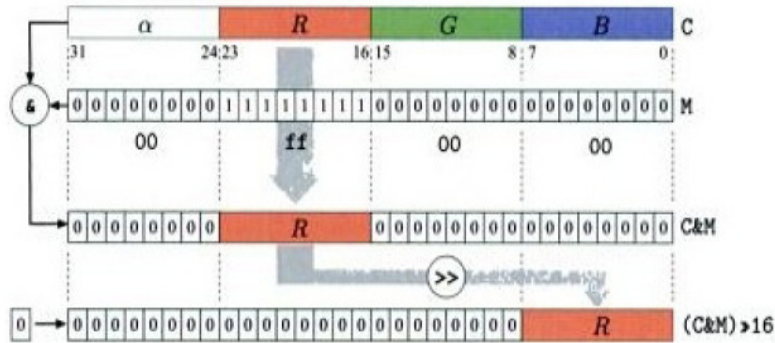


FIGURE 8: RGB Color Images

The Figure.8 shows how to find the RGB value, decomposition of a 32-bit RGB color pixel using bit operations. The R component (bits 16-23) of the RGB pixels C (above in the fig) is isolated using a bitwise AND operation (&) together with a bit mask $M = 0xff0000$. All bits except the R component are set to the value 0, while the bit pattern within R component remains unchanged. This bit pattern is subsequently shifted 16 positions to the right (>), so that the R component is moved into the lowest 8 bits and its value lies in the range of 0 to 255. During this shift operation, zeros are filled in from the left. The construction of an RGB pixel from the individual R, G and B values is done in the opposite direction using the bitwise OR operator (|) and shifting the bits left (<): $((\text{red} \& 0Xff) \ll 16) | ((\text{green} \& 0Xff) \ll 8) | \text{blue} \& 0Xff$. Masking the component values with 0Xff works in this case because except for the bits in positions 0 to 7 (values in the range 0 to 255), all the other bits are already set to zero. Thus the RGB value is obtained which is then converted into HSV mode. The average color ratios of both the images are obtained by using:

- Red average = sum of all the Red Pixels in the image R (P)/No. Of pixels in the image P
- Green average = sum of all the Green Pixels in the image G (P)/No. Of pixels in the image P
- B average = sum of all the Blue Pixels in the image B (P)/No. Of pixels in the image P

Where,

R (P) = RED component pixels,
 G (P) = GREEN component pixels,
 B (P) = BLUE component pixels,
 P = No. of pixels in the image

After finding the average value, each and every block of the source image is compared with the target image. By using standard deviation, it finds the amount the image is deviated from the average value. The difference between the average values is calculated. If the difference value is zero then the particular page is a real page. If the difference value is more than zero then the page is a phishing page. From the Figure.14, If it is a phishing page then the person can directly report it to the Anti-Phishing Work Group (APWG) using this tool by clicking the button “report phishing”. By clicking this button the user is redirected to APWG web site where the user can give the name of the link which is a phishing page. In this case, the other users will not be fooled by the same link.

4. PERFORMANCE ANALYSIS ON VARIOUS TESTING

There are two general categories of testing. Pre implementation and post implementation. The software testing for the process planning system has been done during the pre-implementation stage using various software testing strategies.

4.1 Unit Testing

The individual modules are tested for proper functioning and are found to be satisfactory as regard to the expected output from the module. The whole work is divided into modules and every module is tested independent of other modules and their functionalities. If the testing of the module requires sub divisions for accurate output they are permissible. The testing is carried out during programming stage itself. There are some validation checks for verifying the data input given by the user for the authentication purpose. The errors could be identified and debugged.

4.2 Interface Testing

After the modules are individually tested we confine the testing process to each and every interface which has been developed in the application since every interface is a master screen. During the interface testing, the GUI interfaces are tested accordingly as per their functionality prescribed. This testing would ensure the proper functioning of the interfaces as per the requirements demanded. Interface testing would improve the performance of the system

4.3 Black Box Testing

This testing focuses on the functional requirements of the software and also it enables the software engineer to drive the sets of input conditions that will fully exercise functional requirements for a program. It attempts to find error such as incorrect missing functions, interface errors, errors in data structures or external database, access, performance errors, initialization and termination errors. The software has been tested to drive a set of cases that satisfy the user requirements

4.4 Integrated Testing

The need for the integrated testing is to find the overall system performance, while testing the whole application there are chances of reoccurrence of errors because, previously all the testing techniques were used to test some individual modules. Now we would integrate all of them and would test for their compatibility as a whole for all the interfaces and the charting process because they are all interdependent on each other. The application has been tested for various kinds of inputs and has successfully passed.

4.5 Validation Testing

At the culmination of Black Box testing, software is completely assembled as a package and tested as a whole unit. Validation testing is where the requirements established as part of the software requirements analysis are validated against the software that has been constructed. It ensures that the software meets all the functional, behavioral and performance requirements. The application was tested on various inputs which authenticates the user as specified by the organization.

5. RESULTS AND OUTPUT

The result shows that the test of our methods is more efficient when compared with existing work. The test case shows the performance analysis with different parameters as shown in Table.1. This makes well to get appropriate output. An example for our test is Gmail original and Gmail fake pages as shown in Figure.15 and Figure.16 respectively.

Test Cases	Input	Expected Input	Output	Expected Output	Result
File name	Text file	Image file	Invalid	Image from the specified directory is loaded	Pass
Directory name	No files in the directory	Image files	No images in the directory	Select the required files from the directory	Pass
Color value	Color value>10&&color value<0.1	Color value<10&&color value>0.1	Invalid values	Values accepted	Pass
RGB or HSV	Nothing is selected	One radio button is chosen	Invalid value	Values accepted	Pass
Number of sections	Number of sections>100 and <1	Number of sections<100 and >1	Invalid values	Values accepted	Pass
Overlapping regions	Overlapping regions>100 and <0	Overlapping regions<100 and >0	Invalid values	Values accepted	Pass

TABLE 1: Performance based on difference parameter

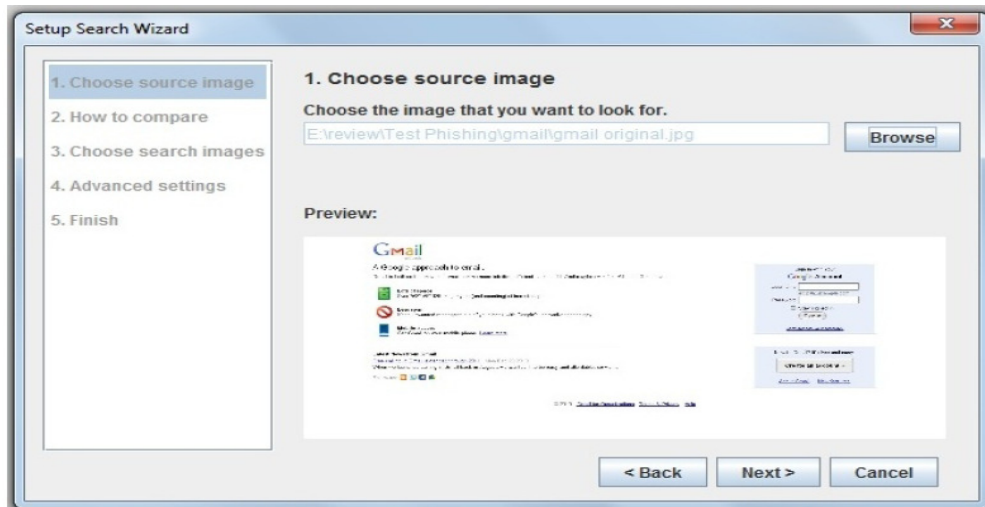


FIGURE 9: Choosing Source Image

In Figure.9, Choose the source image by clique the browse option to display the path. From the root directory required source can be identified.

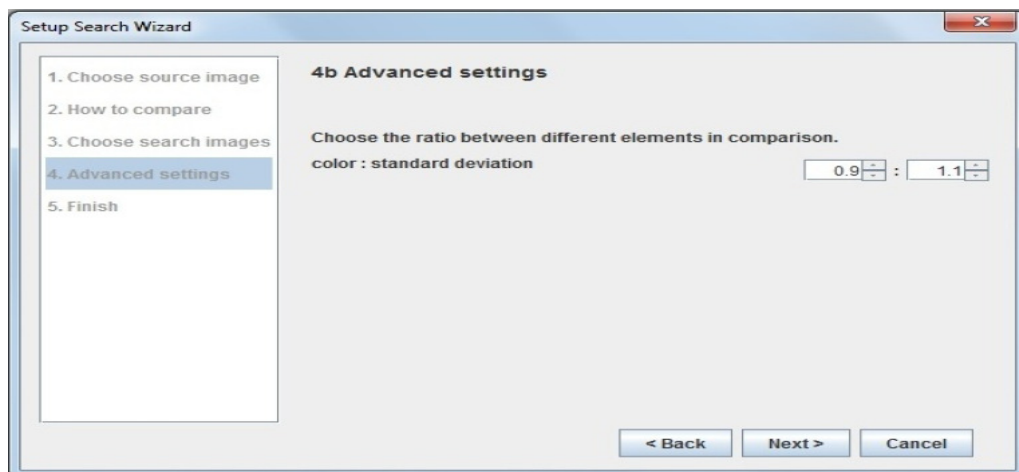


FIGURE 10: Choosing the Parameters

In Figure.10, shows the ratio between different elements in comparison for identification. The standard color deviation gives the appropriate ratio.



FIGURE 11: No Images in the Directory

In Figure.11, shows after selecting the root directory, the appropriate image has to be selected otherwise the pop-up menu will be displayed

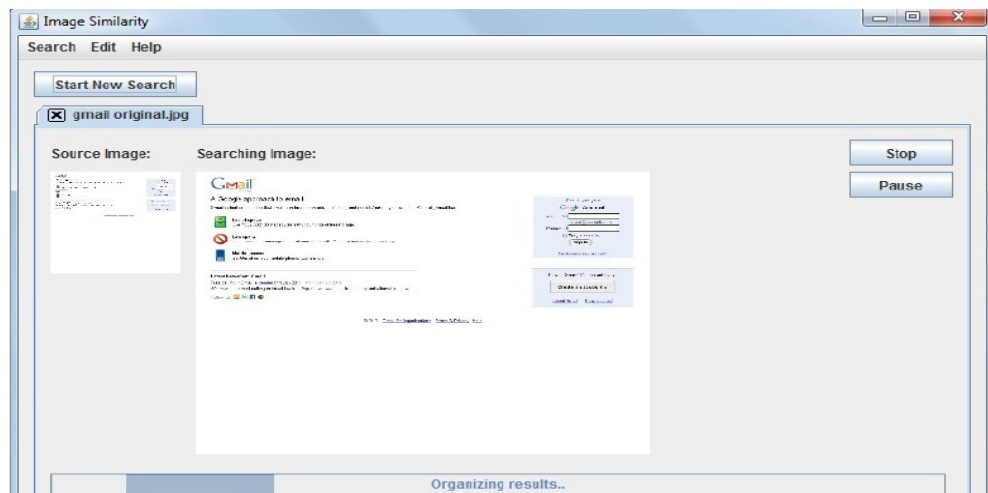


FIGURE 12: Image Similarity

In figure.12, Gives the similarity of search image and existing image. This method is the easy way of find the phishing page. This will improve the efficiency of the web page.

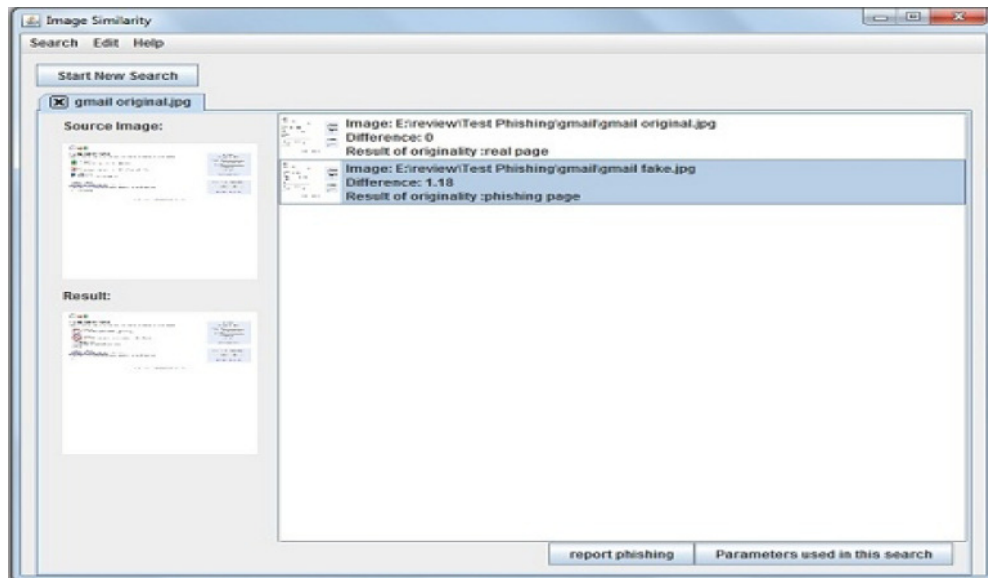


FIGURE 13: Displaying the Difference Value

In Figure.13, based on the difference values can identify the original and fake pages. If the difference value is 0, then real page will be displayed. The difference value is other than 0 will produce phishing page.

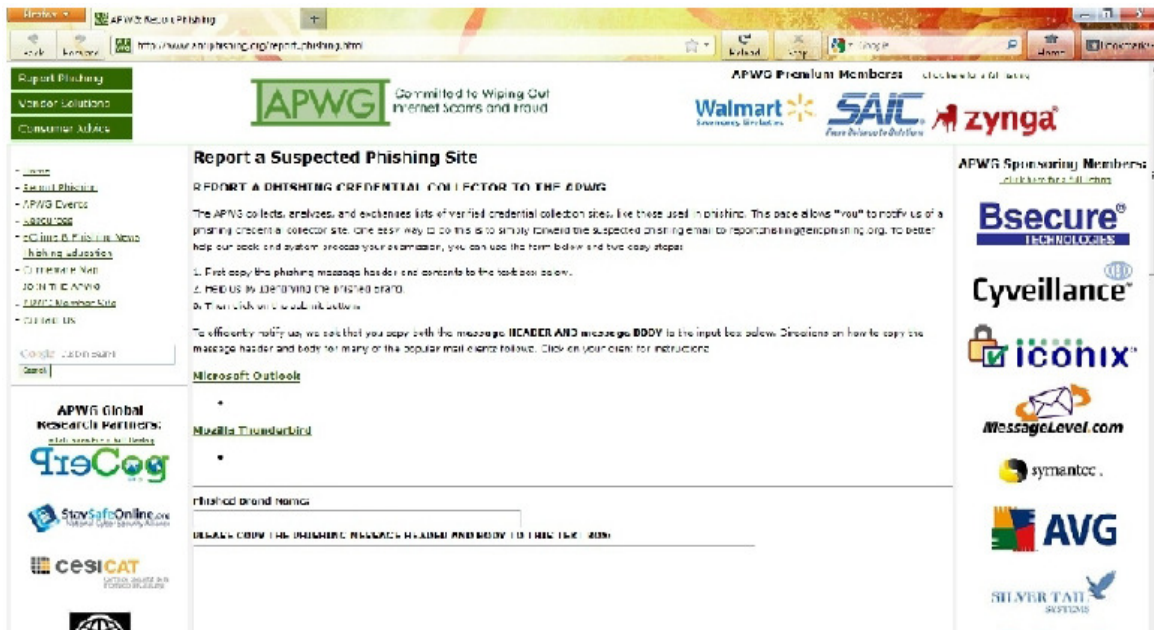


FIGURE 14: Reporting to the APWG site

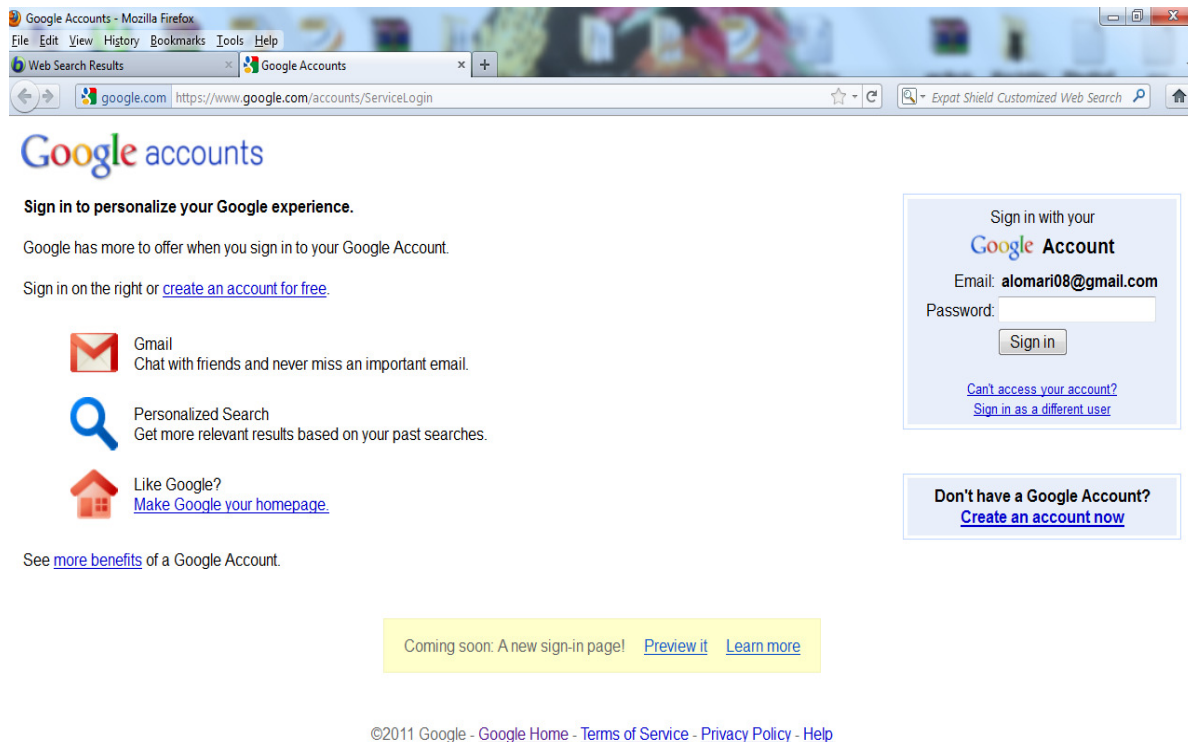


FIGURE 15: Gmail Original Page [www.google.com]

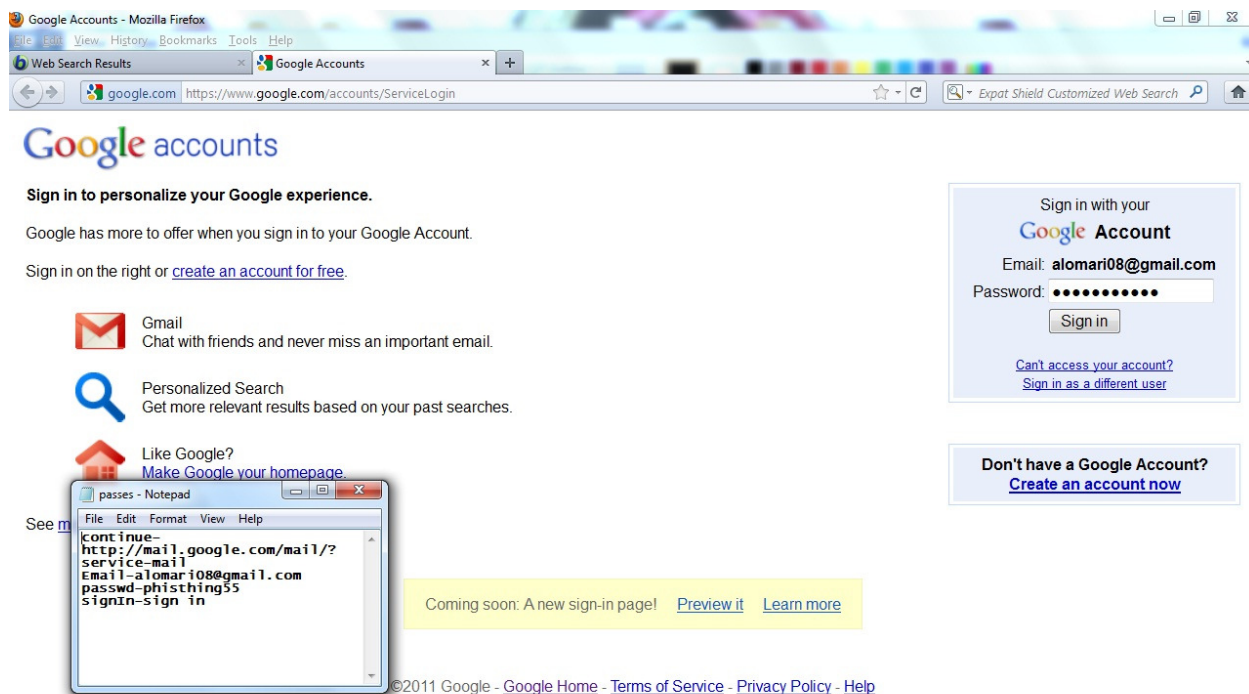


FIGURE 16: Gmail Fake Page

To prevent the phishing attack, the snapshot of the web page that appears before the user is taken. Then the web page is stored as an image in a directory. The anti-phishing tool takes the

snapshot of the original web page and stores it. The original page is chosen from the directory. Then both the images are compared. If the difference value is zero then the page is a “real page” else if the value is a non-zero then the page is a “phishing page”. If the page is reported as phishing page then select report to phishing button which redirects to APWG website where the user can report the page as phishing page and that page will be added to the list of phishing pages.

Techniques	Year	Proposed Work	Result
Spear Phishing	2005	Spear phishing is an e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data.	92.56%
CCH	2006	A contrast value is defined as the difference in intensity between a point and the salient corner.	98.19%
Whaling	2008	The cybercrime practice of phishing — masquerading online as a trustworthy source to try to steal people's sensitive information — is coming up against some serious competition in the form of "whalers".	96.37%
Spoofing	2004	Spoofing attack is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage.	98%
Tabnabbing	2009	Tabnabbing is a computer exploit and phishing attack, which persuades users to submit their login details and passwords to popular web sites by impersonating those sites and convincing the user that the site is genuine.	97.98%

TABLE 2: Phishing techniques compared with other related works

From the above table 2, The CCH performance is high when compared with other techniques like spear phishing, whaling, spoofing and tabnabbing. Tabnabbing is one of the recent techniques introduced in phishing attacks. Whaling is using for cybercrime of phishing, online information can try to steal by the people. Spoofing is well know phishing attacks used to identify false data, is used to improve the efficiency of the web page.

5.1 Non Functional Requirements

- **Portability:** This tool is platform independent; it can run in any operating system.
- **Efficiency:** It is very speed in nature because this tool does not contain any databases. So, CPU cycles will not be wasted in retrieving data from database.
- **Time:** Time is a main constraint in a work. The comparison is done only as per the requirements of the user.

- **Usability:** This tool is very easy to use because of its user friendly comparison wizard. Even a normal person can use it without any difficulty.
- **Scalability:** In future we can update the tool by adding some extra features. This tool will function properly irrespective of any update.
- **Performance:** It can perform high even if there are more images to compare.
- **Error Handling:** When there is no image in the specified directory then the wizard will tell the user as “no image”. It is robust in nature.
- **Accessibility:** It is easily accessible because it is in the universal language English.
- **Accuracy:** This tool can detect even a small difference between the images because it matches the color ratio of the images. So, it is highly accurate.
- **Capacity:** It can hold many numbers of images to compare.
- **Visibility:** The visibility is good. The font used is bigger in size. Each panel contains instructions which will lead the user to the next step.

6. CONCLUSIONS

Nowadays, all activities like banking, shopping, etc. are carried out only using internet. There are more chances for the phishers to steal the information from the user. So security plays a major role. This project is developed to prevent attacks like phishing attack. By this attack the attackers steal the personal information of a user and misuse it. To avoid phishing attack, here we proposed a color based image comparison method is developed. To prevent phishing attacks there are methods which are inefficient. All methods uses only text based comparison which is not error free because the attackers has started to insert images which looks similar to that of the original image. So, by text based comparison the difference between the real and the fake page cannot be found. Color is the most important feature in an image. So, in this project we have developed an image based comparison method which compares the images based on the color values. Only the company which created that website knows about the color range of the images present in the web page. None can design a fake web page similar to the original page with that same color range. So, by comparing images using color values will give an accurate result. Thus, this anti-phishing tool is highly efficient and error free. This anti-phishing tool can be used in online banking, online shopping and to maintain the mail accounts. Even when there is a small variation in the web page this tool can find it and report to the user and another main advantage is that the user need not waste time by searching internet to report the page to APWG. Instead a button is embedded in this tool which will redirect the user to the APWG web site. In Future work, can develop a fully automated crawling framework by using attribute-based phishing attacks that developed for testing, along with main experimental results.

7. ACKNOWLEDGMENT

Sincere thank and recognition goes to my advisor, Associate Professor, Dr. Putra Sumari, who guided me through this research, inspired and motivated me. We also thank the Universiti Sains Malaysia USM for supporting this research.

8. REFERENCES

- [1] A. Kannan, V. Mohan and N. Anbazhagan. "Image Clustering and Retrieval using Image Mining Techniques". *IEEE International Conference on Computational Intelligence and Computing Research*, vol.2, 2010
- [2] SOPHOS 2005, <http://www.sophos.com/whitepapers/sophos-phishing-wpuk.pdf>, accessed April 2011
- [3] M. Jakobsson, and S. Myers: 'Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft' Wiley, 2007
- [4] W. Burger and M. Burge. "Digital image processing: an algorithmic introduction using Java". Springer, Pages: 240-250, 2008

- [5] S.R. Kodituwakku et al. "Comparison of Color Features for Image Retrieval". *Indian Journal of Computer Science and Engineering*, vol.1, no.3, pp.207-211, 2004
- [6] APWG, <http://www.antiphishing.org/index.html>, accessed March 2011
- [7] Wikipedia, <http://en.wikipedia.org/wiki/Phishing>, accessed April 2011
- [8] Webopedia, <http://www.webopedia.com/TERM/P/phishing.html>, accessed April 2011
- [9] M. Aburrous, M.A.Hossain, Keshav Dahal and Fadi Thabtah. "Experimental Case Studies for Investigating E-Business Phishing Techniques and Attack Strategies". *Springer Science, Cong Comput 2010*, vol.2, No.242-253, April 2010
- [10] APWG. http://www.apwg.org/reports/APWG_GlobalPhishingSurvey_1H2009.pdf , accessed 8 August 2009
- [11] M. Chandrasekaran, K Narayanan and S Upadhaya,"PHONEY:Mimicking User Response to Detect Phishing Attacks", *To appear at TSPUC Workshop, affiliated with IEEE WoWMoM, 2005*
- [12] K. Chen, C. Huang and C. Chen. "Fighting Fishing With Discriminative Keypoint Features". *IEEE INTERNET COMPUTING*, 2009
- [13] K. Plossl, H. Federrath and T. Nowey. "Protection Mechanisms Against Phishing Attacks". *Proc, 2nd Intl.Conf. on TrusBus 05, LNCS 3592, Springer-Verlag, 2005*
- [14] M. Wu, R.C.Miller, S.L.Garfinkel, "Do security toolbars actually prevents phishing attacks?", *in CHI (to appear), 2006*. [online]. Available: <http://www.simson.net/ref/2006/CHI-security-toolbar-final.pdf>
- [15] S. Kierkegaard, "Swallowing the bait, hook, line and sinker: Phishing and Pharming and now rat-ting!", in *Managing Information Services in Financial Services* H.R. Roa, M. Gupta, S. J. Upadhaya, Eds.USA:IGI publishing, 2008, pp.241-253.
- [16] N.P. Singh. "Online Frauds in Banks with Phishing". *Journal of Internet Banking and Commerce*, vol.12, 2007
- [17] Phishtank. 2008 http://www.phishtank.com/phish_archive.php, accessed 14 November 2008
- [18] A. Abbasi and H. Chen. "A comparison of fraud cues and classification methods for fake escrow website detection". *Springer, Inf Technol March, 2009*
- [19] R. Kanthety and S. Saradhi. "Prevention of Phishing Attacks using Link-Guard Algorithm". *International Journal of Computer Science Issues (IJCSI)*. vol. 7, no. 2, suppl.4, 31p.March 2010
- [20] A. Martin, Na.Ba.Anuthamaa, M. Sathyavathy, Marie Manjari Saint Francois and Dr. Prasanna Venkatesan. "A Framework for Predicting Phishing Websites Using Neural Networks". *International Journal of Computer Science Issues (IJCSI)*. vol. 8, Issue 2, March 2011
- [21] Juan Chen and Chuanxiong. "Online Detection and Prevention of Phishing Attacks". *IEEE Communications and Networking, NSFC, 2005*
- [22] Bryan Parno, Cynthia Kuo, and Adrian Perrig. "Phoolproof of Phishing Prevention". *Financial Cryptography and Data Security, Springer, 2006*

- [23] Total Number of Fraud Complaints & amount paid. 2003,
http://www.consumer.gov/sentinel/states03/fraud_complaint_trends.pdf.
- [24] Tom Jagatic, Nathaniel Johnson, Markus Jakobsson, and Filippo Menczer. "Social Phishing". Communications of ACM, 2005
- [25] Thomas J. Holt and Danielle C. Graves. "A Qualitative Analysis of Advance Fee Fraud E-mail Schemes". International journal of Cyber Criminology, vol.1, issue.1, 2006
- [26] <http://mybank.com/ebanking>

Using Cipher Key to Generate Dynamic S-Box in AES Cipher System

Razi Hosseinkhani

*Computer Engineering Department Science and Research Branch
Islamic Azad University
Tehran, Iran*

r.hosseinkhani@nioc.ir

H. Haj Seyyed Javadi

*Department of Mathematics and Computer Science
Shahed University
Tehran, Iran*

h.s.javadi@shahed.ac.ir

Abstract

The Advanced Encryption Standard (AES) is using in a large scale of applications that need to protect their data and information. The S-Box component that used in AES is fixed, and not changeable. If we can generate this S-Box dynamically, we increase the cryptographic strength of AES cipher system. In this paper we intend to introduce new algorithm that generate S-Box dynamically from cipher key. We describe how S-Box can be generated dynamically from cipher key and finally analyze the results and experiments.

Keywords: Advanced Encryption Standard, AES, Dynamic S-Box Generation, S-Box

1. INTRODUCTION

Encryption has an important role in data protection. The importance of encryption realized with increasing communication. Encryption makes sense when data packets using open channels, which they can be reached by other devices or people, to transfer their contents.

Encryption is knowledge of changing data with cipher key by using cipher algorithms, so that someone who knows the cipher key and cipher algorithm can export the plain text from cipher text. The meaning of Encryption is not only hiding information, but also it means sending information with another form, so that ensure security of data.

An Encryption system contains set of transformations that convert plain text into cipher text. In the block cipher system, plain text converts into blocks that cipher algorithm applies on them to create cipher text.

The block cipher systems divided into two general principles: Diffusion and Confusion. In Diffusion principle, each bit of plain text converts into many bits. However, in Confusion principle, number of bits doesn't change and only transformations apply to plain text, hence in Confusion principle, size of plain text and cipher text is equal. Usually in both principles, using round repetition to create cipher text. Repeating a single round contributes to cipher's simplicity [1].

Cipher algorithms have the two general categories: Private Key algorithms and public key algorithms. Private Key algorithms using single key to encrypt plain text and decrypt cipher text in sender and receiver side. Private Key algorithm samples are: DES, 3DES and Advanced Encryption Standard (AES). Public Key algorithms, such as the Rivest-Shamir-Adleman (RSA), using two different key for encrypt plain text and decrypt cipher text in sender and receiver sides. Block cipher systems depend on the S-Boxes, which are fixed and no relation with a cipher key. So only changeable parameter is cipher key. Since the only nonlinear component of AES is S-Boxes, they are an important source of cryptographic strength. So we intend use cipher key to

generate dynamic S-Box that is changed with every changing of cipher key. That cause increasing the cryptographic strength of AES algorithm. Other systems using key-dependent S-Boxes have been proposed in the past, the most well-known is Blowfish and Khufu [2], [3]. Each of these two systems uses the cryptosystem itself to generate the S-Boxes.

In section 2, we briefly introduce the AES algorithm. In section 3, we study about the S-Box that used in AES. In section 4, we show that how S-Box will be generated from key and in the final section we analyze experiments and investigate about results.

2. ADVANCED ENCRYPTION STANDARD (AES)

This standard specifies the Rijndael algorithm, asymmetric block cipher can process data blocks of 128 bits, using cipher key with lengths of 128, 192, and 256 bits. Rijndael was designed to handle additional block sizes and key length, however they are not adopted in this standard [4].

2.1 Definitions

- **Cipher:** Series of transformations that converts plaintext to cipher text using the Cipher Key.
- **Cipher Key:** Secret, cryptographic key that is used by the Key Expansion routine to generate a set of Round Keys; can be pictured as a rectangular array of bytes, having four rows and N_k columns.
- **Ciphertext:** Data output from the Cipher or input to the Inverse cipher.
- **Plaintext:** Data input to the Cipher or output from the Inverse Cipher.
- **S-Box:** Non-linear substitution table used in several byte substitution transformations and in the Key Expansion routine to perform a one-for-one substitution of a byte value.

2.2 Algorithm Parameters, Symbols, and Functions

The following algorithm parameters, symbols, and functions are used throughout this standard:

- **AddRoundKey():** Transformation in the Cipher and Inverse Cipher in which a Round Key is added to the State using an XOR operation. The length of a Round Key equals the size of the State.
- **MixColumns():** Transformation in the Cipher that takes all of the columns of the State and mixes their data (independently of one other) to produce new columns.
- **Nb:** Number of columns (32-bit words) comprising the State.
- **Nk:** Number of 32-bit words comprising the Cipher Key.
- **Nr:** Number of rounds, which is a function of N_k and N_b (which is fixed).
- **RotWord():** Function used in a Key Expansion routine that takes a four-byte word and performs a cyclic permutation.
- **ShiftRows ():** Function is the Cipher that processes the state by cyclically shifting the last three rows of the State by different offsets.
- **SubBytes():** Transformation in the Cipher that processes the State using a non-linear byte substitution table (S-Box) that operates on each of State bytes independently.
- **SubWord():** Function used in the Key Expansion routine that takes a four-byte input word and applies an S-Box to each of the four bytes to produce an output word.

2.3 Cipher Algorithm

From the beginning of the Cipher, the input is copied to State array. After an initial Round Key addition, the State array is transformed by implementing a round function 10, 12, or 14 times (depending of key length), with the final round differing slightly from the first N_r-1 rounds. The final State is then copied to the output. The Cipher is described in the pseudo code in algorithm 1.

```
public word[] Cipher(byte[] plainText, byte[] cipherKey)
{
    state = new word[4];
    sBox = new newSbox(cipherKey);
    ks = new KeySchedule(cipherKey);
```

```

for (int i = 0; i < 4; i++)
{
    for (int j = 0; j < 4; j++)
    {
        if (state[j] == null)
            state[j] = new word();
        state[j].w[i] = plainText[i * 4 + j];
    }
}
AddRoundKey(0);
for (int i = 1; i < Nr; i++)
{
    SubBytes();
    ShiftRows();
    MixColumn();
    AddRoundKey(i);
}
SubBytes();
ShiftRows();
AddRoundKey(Nr);
return state;
}

```

ALGORITHM 1: Pseudo Code for Cipher

3. THE SUBSTITUTION BOX (S-BOX)

Substitution is a nonlinear transformation which performs confusion of bits. A nonlinear transformation is essential for every modern encryption algorithm and is proved to be a strong cryptographic primitive against linear and differential cryptanalysis. Nonlinear transformations are implemented as lookup tables (S-Boxes). An S-Box with p input bits and q output bits is denoted $p * q$. The DES uses eight $6 * 4$ S-boxes. S-Boxes are designed for software implementation on 8-bit processors. The block ciphers with $8 * 8$ S-Boxes are SAFER, SHARK, and AES.

For processors with 32-bit or 64-bit words, S-Boxes with more output bits provide high efficiency. The Snefru, Blowfish, CAST, and SQUARE use $8 * 32$ S-Boxes. The S-Boxes can be selected at random as in Snefru, can be computed using a chaotic map, or have some mathematical structure over a finite Galois field. Examples of the last approach are SAFER, SHARK, and AES. S-Boxes that depend on key values are slower but more secure than key independent ones (Schneier, 1996). Use of key independent chaotic S-Boxes are analyzed in which the S-Box is constructed with a transformation $F((X + K) \bmod M)$, where K is the key [5].

4. DYNAMIC S-BOX GENERATION FROM CIPHER KEY ALGORITHM

4.1 First Step

We need primary S-Box to generate dynamic S-Box, that should have 16 rows and columns. We use S-Box generation algorithm that introduced in AES, to create primary S-Box as follows [4]. Take the multiplicative inverse in the finite field $GF(2^8)$; the element $\{00\}$ is mapped to itself. Apply the following affine transformation (over $GF(2)$) that represent in following equation.

$$b'_i = b_i \oplus b_{(i+4) \bmod 8} \oplus b_{(i+5) \bmod 8} \oplus b_{(i+6) \bmod 8} \oplus b_{(i+7) \bmod 8} \oplus c_i$$

EQUATION 1: S-Box transformation

For $0 \leq i < 8$, where b_i is the i^{th} bit of the byte, and c_i is the i^{th} of a byte with the value {63} or (01100011). Here and elsewhere, a prime on a variable (e.g., b_i') indicate that the variable is to be updated with the value on the right. In matrix form, the affine transformation element of the S-Box can be expressed as:

$$\begin{bmatrix} b_0' \\ b_1' \\ b_2' \\ b_3' \\ b_4' \\ b_5' \\ b_6' \\ b_7' \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}.$$

FIGURE 1: Step 2 in S-Box generation in AES

4.2 Second Step

In this step, rows swapped with columns of primary S-Box in **GenerateDynamicSbox(cipherKey)** function. This function guarantees new S-Box remain one-for-one. This routine get cipher key as input and generate dynamic S-Box from cipher key. Note that in this paper if cipher key has 192 or 256 bits size, we use only first 128 bits of cipher key.

4.2.1 GenerateDynamicSbox Algorithm

```

1: void GenerateDynamicSbox(byte[16] key)
2: {
3:     byte rowIndex, columnIndex;
4:     byte shiftCount = GetShiftCount(key);

5:     byte[,] sBox = GeneratePrimarySbox();

6:     for(int i = 0; i < 16; i++)
7:     {
8:         GetProperIndex(key[i], out rowIndex, out columnIndex);
9:         ShiftRow(rowIndex, shiftCount, sBox);
10:        ShiftColumn(columnIndex, shiftCount, sBox);
11:        Swap(rowIndex, columnIndex, sBox);
12:    }
13: }
```

ALGORITHM 2: The **GenerateDynamicSbox** function generate dynamic S-Box form cipher key.

In line 4, **GetShiftCount(cipherKey)** get cipherKey as input and return number of shift that should be applied to rows and columns before replacing with each other.

In line 5, **GeneratePrimarySbox ()** generate primary S-Box according 4.1.

In line 6, start loop for 16 times (foreach byte of cipher key, only first 16 byte of cipher key is used).

In line 8, **GetProperIndex(cipherKey[i], out rowIndex, out columnIndex)** get byte of cipher key and return indexes of row and column that should be replaced with each other.

In line 9, **ShiftRow(rowIndex, shiftCount, sBox)** get row index of S-Box and shift each element of given row cyclically. It means if rowIndex = 0 and shiftCount = 1, first element of S-Box,

sBox[0,1] replace with sBox[0,0] and sBox[0,2] replace with sBox[0,1] ... and sBox[0,0] replace with sBox[0,15]. (The first index of sBox determine rowIndex and second one determine columnIndex).

In line 10, **ShiftColumn(columnIndex, shiftCount, sBox)** get column index of S-Box and shift each element of given column cyclically. It means if columnIndex = 0 and shiftCount = 1, first element of S-Box, sBox[1,0] replace with sBox[0,0] and sBox[2,0] replace with sBox[1,0] ... and sBox[0,0] replace with sBox[15,0].

In line 11, **Swap(rowIndex, columnIndex, sBox)** get row and column index and then swapped them with each other. For example if rowIndex = 5 and columnIndex = 4 the Swap function swapping element at sBox[0,5] with sBox[4,0] and sBox[1,5] with sBox[4,1] and ... and finally sBox[15,5] swap with sBox[4,15].

4.2.2 GetShiftCount Algorithm

This function get cipher key as input and return number of shift count as output. If cipher key larger than 128 bit, only first 128 should be used.

```

1: byte GetShiftCount(byte[16] cipherKey)
2: {
3:     byte customizingFactor = 0x00;
4:     byte shiftCount = 0;

5:     for(int i = 0 ; i < 16 ;i++)
6:     {
7:         shiftCount ^= (byte)((key[i] * (i + 1)) % (0xFF + 1));
8:     }

9:     return shiftCount ^ customizingFactor;
10:}

```

ALGORITHM 3: The **GetShiftCount** function used to get shift count before swapping rows with columns.

In line 4, **customizingFactor** value is in [0-255] range. This variable can customize the **GetShiftCount** return value and then customize **GenerateDynamicSbox**.

In line 5, start loop for 16 times (foreach byte of cipher key, only first 16 byte of cipher key is used).

In line 6, sign ^ means XOR operation and sign % means modulo in C#. This equation guarantees that changing only one bit of Cipher key cause changing the value of **shiftCount**.

In line 9, **shiftCount** XOR with **customizingFactor** that cause generate 256 different customizing states for **shiftCount** value.

4.2.3 GetProperIndex Algorithm

This function gets byte of cipher key and then return rowIndex and columnIndex as output. This function using Shuffle exchange algorithm that used in designing parallel algorithms [6].

```

1: void GetProperIndex (byte key, out byte rowIndex, out byte columnIndex)
2: {
3:     int[] rowUsedArray, columnUsedArray;

4:     rowIndex = key & 0x0F;
5:     columnIndex = key >> 4;

6:     rowIndex = Shuffle (rowUsedArray, rowIndex);
7:     columnIndex = Shuffle (columnUsedArray, columnIndex);

```

```

8:     rowUsedArray.Add(rowIndex);
9:     columnUsedArray.Add(columnIndex);

10:}

```

ALGORITHM 4: The *GetProperIndex* function pseudo code

In line 3, **rowUsedArray** and **columnUsedArray** variables are using for saving index that used in previous steps.

In line 4, sign & means AND operation in C#.

In line 5, sign >> means shift right n-times in C#.

In line 6, **Shuffle** function get **rowIndex** number and return next available **rowIndex** number if given **rowIndex** is in **rowUsedArray**.

In line 7, **Shuffle** function get **columnIndex** number and return next available **columnIndex** number if given **columnIndex** is in **columnUsedArray**.

In line 8, current **rowIndex** add to **rowUsedArray** array.

In line 9, current **columnIndex** add to **columnUsedArray** array.

This causes that every row and column only one time returns with this function thus every row and column is used for one time in **GenerateDynamicSbox**.

5. EXPERIMENTAL RESULTS

In general, S-Box is substitution table that get number and return another number. This action is nonlinear. In S-Box, n input bits are represented as one of 2^n different characters. The set of 2^n characters are then transposed to one of the others in the set. For example possible output 3×3 S-Boxes are shown in figure 2.

0	1	2		1	0	2		2	1	0		8	7	6
3	4	5		3	4	5		3	4	5	...	5	4	3
6	7	8		6	7	8		6	7	8		2	1	0

FIGURE 2: Possible 3×3 S-Boxes.

The character is then converted back to an n -bit output. It can be easily shown that there are $(2^n)!$ different substitution or connection patterns possible. Thus if n is large then the possible S-Boxes that can be generate is large. If the cryptanalyst want to decode AES algorithm he should try to generate possible S-Box and use them in *SubBytes* function in AES cipher system. The cryptanalyst's task becomes computationally unfeasible as n gets large, say $n = 128$; then $2^n = 10^{38}$, and $(10^{38})!$ possible S-Box can be generate which is an *astronomical* number.

$$(10^{38})! = \infty$$

EQUATION 2: Possible S-Box can be generate when $n = 128$

Experiment 1: We experimentally checked the difference measure of S-Box elements that only different between two bits depend on interval length. For generation random keys we use function that change only two bits of random byte of cipher key. The difference table illustrated in table 1.

Interval length	Avg. of difference	Std. of difference	Percentage of difference
8	229.5	20.4310687784211	89.6484375
16	225.0625	19.9280999261512	87.9150390625
32	227.9375	20.2244462422696	89.0380859375
64	223.96875	21.5037602839412	87.48779296875
128	225.4453125	21.9149424426299	88.0645751953125
256	228.4296875	20.8423338400948	89.2303466796875
512	227.072265625	21.7735331073363	88.7001037597656
1024	226.482421875	21.3572160638917	88.4696960449219
2048	227.00830078125	21.1134241069894	88.6751174926758
4096	228.115966796875	20.8932978239743	89.1077995300293

TABLE 1: The difference table between S-Box elements by changing 2 bits of cipher key's random byte.

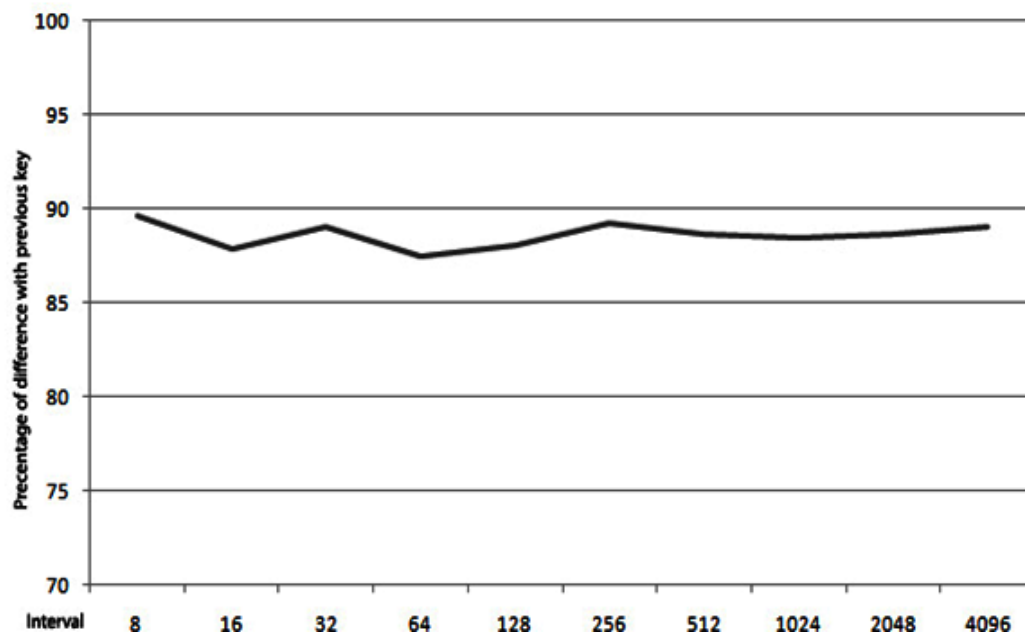


FIGURE 2: Plot of the difference of the S-Box elements with previous key

Experiment 2: The purpose is to verify GenerateDynamicSbox algorithm. Consider the 128 bit length secret key in the hexadecimal form. The key and S-Box2 is represent in table 2.

$$key_hex_1=\{5e,d3,f1,b4,7c,18,51,9a,ae,81,42,57,42,78,dc,8f\}$$

67	1E	77	7B	4B	4F	6F	46	1F	F8	6A	87	B9	71	60	CD
AD	99	85	AF	48	D5	81	0E	17	82	9C	C9	35	13	47	0C
E5	7C	B8	A4	E1	55	E3	DF	02	01	31	70	B0	B7	BD	C1
80	D4	8F	E2	BF	54	B2	68	3B	A1	18	0F	9A	03	DC	EC
D6	E6	AC	B3	3F	7A	22	C5	5E	1D	EB	CA	D2	A6	5A	A0
D0	EF	AA	FB	43	16	AE	07	7D	F9	0A	33	93	26	E9	44
9B	4D	53	D1	00	04	20	5B	5D	51	76	CB	DB	6E	4A	6B
25	AB	D9	E7	73	BA	9D	DA	59	12	74	C0	C4	F7	11	63
94	C7	ED	6C	27	61	CE	39	30	FA	08	C3	36	EA	7F	E8
19	A2	A8	05	52	D7	9F	8C	4C	BE	9E	96	3E	FE	8E	A7
49	D3	8B	38	F1	1C	B6	41	1A	E4	FD	F5	89	D8	24	CF
5F	72	37	6D	92	95	4E	FC	83	0B	65	45	0D	A5	14	3D
E0	2D	C2	3A	B1	06	B4	C6	2E	32	10	62	8D	34	DE	BC
CC	C8	B5	66	2F	58	F6	98	79	56	86	F0	2A	2B	57	3C
88	78	84	90	91	97	EE	5C	BB	DD	69	15	42	40	28	64
75	A3	F2	23	2C	50	7E	1B	29	F4	8A	21	A9	FF	F3	09

TABLE 2: The dynamic S-Box generated with key_hex1. (S-Box1)

We change only two bit of key_hex1, for example, $5e \rightarrow 5d$. The key and S-Box2 is represent in Table 3.

We find 225 different between S-Box1 and S-Box2 by changing only 2 bit of key, thus approximately %87 of second S-Box is changed. The difference of S-Box1 and S-Box2 elements is illustrated in figure 3.

$$key_hex_2=\{5d,d3,f1,b4,7c,18,51,9a,ae,81,42,57,42,78,dc,8f\}$$

4D	CA	D7	59	3F	50	DE	5B	BC	21	16	2D	3A	55	28	A9
82	7D	EB	FA	9E	FE	F0	51	E2	0C	72	68	A2	B9	99	73
E3	C5	B6	01	46	AA	5D	DA	42	F2	BE	B5	77	B7	52	F9
0D	9C	27	B2	B3	86	C7	FD	29	C0	6D	9A	7B	81	DC	EC
BF	AD	17	22	45	89	83	31	5E	35	2F	E6	64	A4	3B	69
D0	A1	7C	FB	43	65	AE	38	47	D9	24	87	67	26	02	E7
80	E1	BD	D4	00	7F	20	8F	61	23	11	05	6F	6E	4A	6B
2C	94	40	88	75	2E	D1	10	07	A0	F3	C9	E5	F7	19	CF
6C	04	66	25	62	30	54	39	C3	5F	09	ED	1F	EA	18	CB
48	A3	7A	12	92	FC	9F	F5	4C	53	76	8B	B8	06	AC	A7
A8	91	0B	1E	F1	C6	79	08	5A	E4	15	95	44	F8	D3	96
BA	70	37	0F	D8	8A	57	CC	1B	98	33	AF	D5	A5	85	8E
C2	B1	E8	DD	CE	41	32	71	4E	1A	E0	78	8C	A6	49	E9
13	C8	C1	1D	34	58	3E	6A	B4	56	2B	0E	9D	84	FF	3C
DB	7E	4F	EE	9B	97	4B	5C	BB	D6	14	74	60	0A	1C	D2
B0	DF	93	90	63	C4	EF	03	36	8D	2A	F4	CD	F6	AB	3D

TABLE 3: The dynamic S-Box generated with key_hex2.(S-Box2)

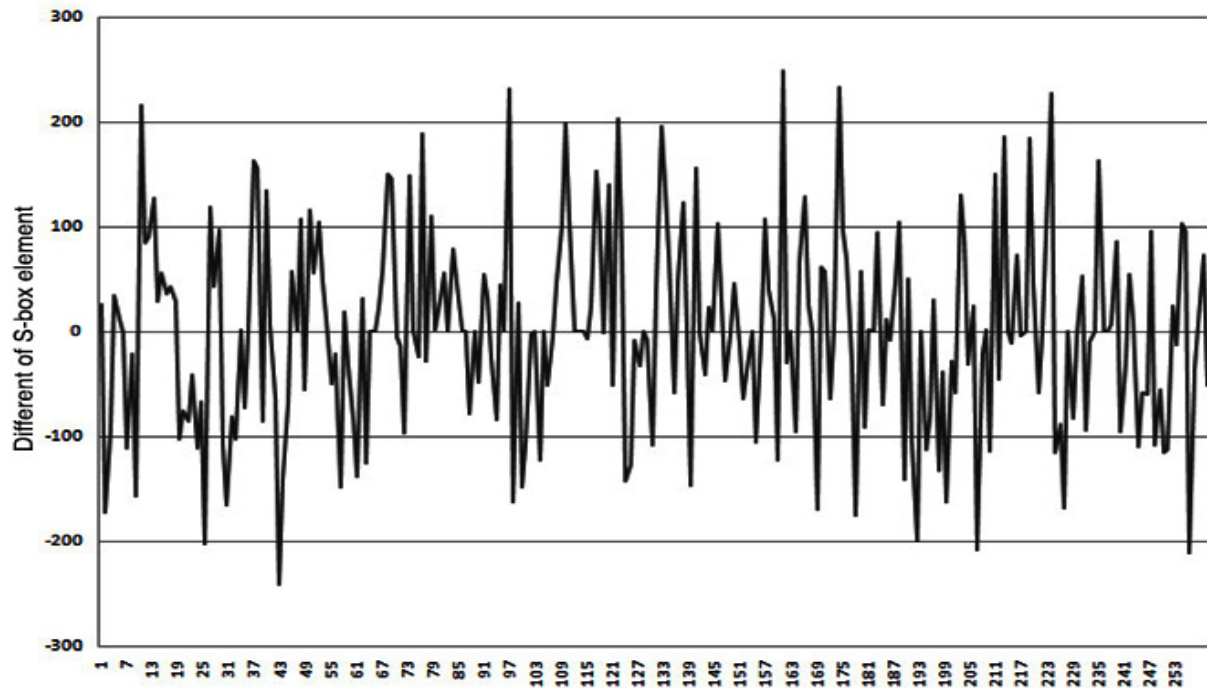


FIGURE 3: Plot of the difference of the S-Box elements (S-Box1 and S-Box2)

Experiment 3: We comparison *GenerateDynamicSBox* function with the older algorithm that was named *KeyDependantSBox* [5]. The *KeyDependantSBox* generates dynamic S-Box using random parameters by using iterative loop. The main property of S-Box is one to one attribute. *KeyDependantSBox* algorithm check every new generated S-Box element with the other elements that is generated sooner to avoid generate duplicate elements and satisfy one to one property of S-Box. The number of comparison in *KeyDependantSBox* presents in figure 4. In our *GenerateDynamicSBox* algorithm no need to check duplicate elements because original S-Box that is used in AES is one to one and we only substitute and move the original S-Box elements. Thus generated S-Box remains one to one.

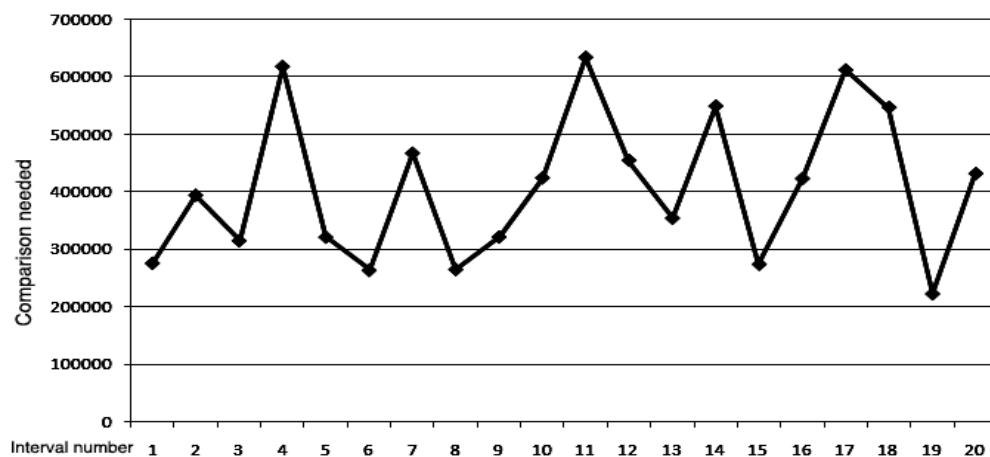


FIGURE 4: Number of comparison that needs to generate S-Box in KeyDependantSBox

6. CONCLUSIONS

We introduced a new algorithm to generate dynamic S-Box from cipher key. The quality of this algorithm tested by changing only two bits of cipher key to generate new S-Boxes. For that purpose we are testing difference of S-Box element by many intervals. This algorithm will lead to generate more secure block ciphers, solve the problem of the fixed structure S-Boxes and will increase the security level of the AES block cipher system. The main advantage of this algorithm is that many S-Boxes can be generated by changing Cipher key.

7. REFERENCES

- [1] Masuda, N. Jakimovski, G. Jakimovski, K. Aihara and L. Kocarev . “Chaotic block ciphers: from theory to practical algorithms” IEEE Trans. on Circuits and Systems – I: Volume: 53 Issue: 6 – 2006
- [2] B. Schneier. Applied Cryptography: Protocols, Algorithms, and Source Code in C, New York: Wiley. 1996
- [3] Merkle, R. Fast software encryption functions. In Advances in Cryptology: Proceedings of CRYPTO’90, Berlin: Springer-Verlag, 1991
- [4] Federal Information Processing Standards, “Advanced Encryption Standard (AES)” Publication 197, November 26 - 2001
- [5] Kazys KAZLAUSKAS, Janunius KAZLAUSKAS,” Key-Dependent S-Box Generation in AES Block Cipher System” , Inoformatica Volume: 20 - 2009
- [6] Michael J.Quinn, Designing efficient algorithms for parallel computers, University of New Hampshire, 1987

Recourse Management Using a Fair Share Scheduler

Suja Cherukullapurath Mana

*Computer Science Department, George Mason University
Fairfax, VA 22030*

scheruk1@masonlive.gmu.edu

Abstract

Resource management is a vital task of all operating systems. It is the responsibility of operating system to ensure that all programs requesting resources are getting resources in a timely manner. Various recourse allocation strategies are there which provide guidance for operating systems to make resource allocation decisions. This article studies about the resource management using a fare share scheduler. The fair share scheduler ensures that resources are allocated to programs in an efficient manner and this ensures fairness in resource allocation.

Keywords: Fairness, Fair Share Scheduling.

1. INTRODUCTION

Fairness is an important, challenging feature of any operating system resource scheduler, especially when there are a large number of programs waiting for resources. Real-time interactive and multimedia application servers will have a large number of service request occurring at the same time. A fair share scheduler is essential in this case to ensure that no processes starve indefinitely for resources. The fair share scheduler ensures that a specific portion of resources will be allocated to all programs [1]. The fair share algorithm requires that each user should be able to specify their required share of resources [1] and also no program should prevent the scheduler to allocate resources to other programs [1].

Similarly in a virtual machine environment where more than one operating system are running on a single machine, proper resource management is necessary to ensure good results.

Main objectives of a fair share scheduler are to ensure fairness, fast response time and load spreading without making any programs wait for too long. The users can view the fair share scheduler as a scheduler which ensures that all resources will be allocated in a fair manner. The resource allocation is defined based on the share and usage history [6]. A diagram showing users view of fair share scheduler is shown below [6]. In the diagram the word 'Share' means users authority to do work on a particular machine. A user with more shares can do more work than a user with fewer shares. The term 'Usage' indicates a measure of amount of work that each user performed in a particular system. So as per the user centric view, each user can expect to see that as their usages are increasing dynamically, their response time is getting worse' [6].

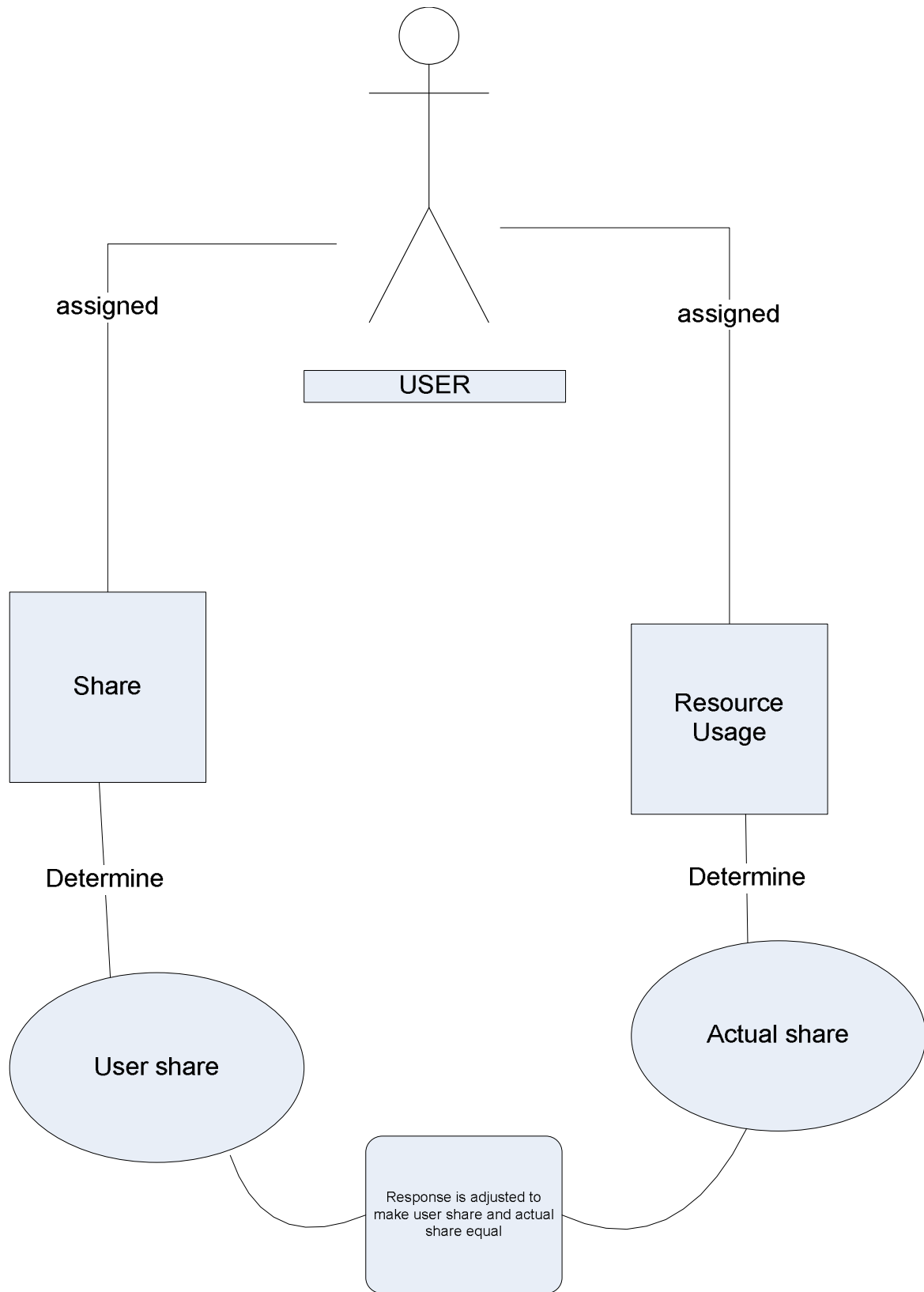


FIGURE 1: A user view of fair share scheduler

In some systems the resource allocation is done by a 'fixed budget' model [6]. As per this model of resource sharing, users have fixed budget allotted to them for resource usage. The budget will be reduced as they are using resources. In a nutshell this model ensures that processes whose owner is ready to pay more will get higher share of resources. To have better control over the allocation, certain constraints are being used. For example, there will be an upper limit for daily disk space usage, daily and weekly connect limits are also available[6].

The paper is organized in such a way that in the following sections it describes about the methodology of fair share scheduler, advantages and disadvantages of these methodologies, then some related works and research gaps followed by conclusion and future works.

2. METHODOLOGIES

The 'Fair share scheduling' ensures that each user is receiving required resources in a fair manner. That is the operating system is not just dividing available resources among available user, but doing the resource allocating on a need based manner. Various methodologies are being studied to ensure fair share allocations.

One methodology [6] describes concept of share from a user and a program perspectives. The user level scheduling involves steps like

- Usage of each user is updated by adding charges incurred by each process since last update and then adjust it by appropriate constant[6]
- Update resource consumption records[6]

The program level scheduler involves following steps

- . Activation of process: Update the cost encounter by currently running process and then select a process with lowest priority for running [6]
- Adjust priorities of process: According to the usage, share and number of active processes, adjust the priority of currently running processes.

Another method of determining share of each process towards resource usage is the lottery scheduling [8]. Lottery scheduling is an efficient way of implementing 'proportional share' resource management ensuring that each process will get resources proportional to their shares. In this scheduling resource rights are represented by lottery tickets and resources are allocated to a user with a winning ticket [8]. This scheduling methodology is fair probabilistically [8]. Resource allocation to each user is proportional to number of lotteries each process holds. The representation of resource right as lottery tickets is also helpful for modular resource management. To ensure that a user using only a fraction of its allocated resource is not preventing from getting CPU, a compensation ticket will be given to such users. This compensation ticket will raise the priority of user[8].

The following figure shows how lottery based scheduling works [8].

. Total tickets = 20

10th ticket is selected randomly for comparison.

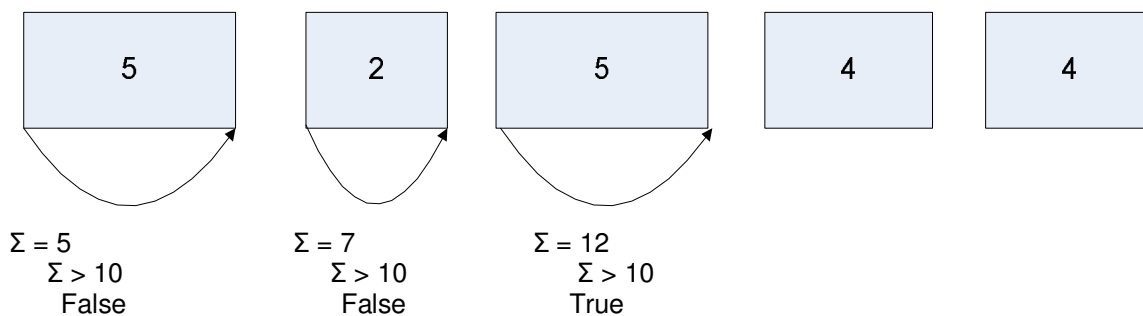


FIGURE 2: Lottery based scheduling example

Here five clients with tickets compete for resources. 10th ticket is randomly selected for comparison. Tickets sum is calculated until the comparison value is reached. In this case the third client is the winner [8]. Since the number of tickets each client possess is varying, ordering them in the descending order of number of tickets will reduce the average search time to a great extent.

Another fair share algorithm is the Virtual Time Round Robin which combine the benefits of round robin and fair queuing [9] algorithms. Implementation simplicity is the main advantage of this algorithm. The implementation of this algorithm involve following three steps[9].

- Clients are ordered in the run queue according to their share and their position in the queue changes only when their share changes [9].
- 'Starting from the beginning of the queue, run each clients in a round robin manner for a fixed time quantum'[9].
- If any client receive more than its proportional share during the execution of step 2, further executions will be skipped and the execution start again from the beginning of the queue[9].

2.1 Advantages and Disadvantages of Fair Share Methodology

Fair share scheduler is very effective in allocating resources in a reasonable way. These methodologies ensure fairness in resource allocation. It ensures that all processes will get resources that they want at some reasonable amount of time. Thus it increases response time for each process. Also this scheduler ensures that all resources of the machine are well utilized. The fair share scheduler also increases the system performance even during peak load time. In a nutshell it always guarantees a predictable performance level. But some methodologies like lottery scheduling some time results in selecting clients with more number of tickets always which will cause some other users to wait more than expected. Implementing mechanisms like 'moving forward' [8] can be very effective in resolving this problem.

3. RELATED STUDIES

Due to fact that resource management is a critical function of operating system, many studies have been performed to find an optimal scheduling algorithm which will allocate resources fairly. The paper [1] talks about a surplus fair share scheduling. This scheduler is very effective for allocating resources for a symmetric multiprocessor environment. The paper discusses about a weight re adjustment algorithm and surplus share scheduler to allocate operating system resources fairly [1]. Even though this method is very efficient and practical, it results in a large scale increases in the scheduling overhead.

Generalized process sharing is discussed in papers[2,3,4]. The generalized process sharing is based on a weight assigned to each processes. Resources will be allocated to processes based on its weight. Even though these schedulers are efficient in uniprocessor environment, it may cause indefinite starvation in multi processor systems. The paper [5] introduced the lottery scheduling which provide proper control over the execution rates of computation and also ensures proportional share, modular resource management. In [7] the paper introduces 'a FaRes system level mechanism for monitoring and utilizing that information to ensure fairness among set of Virtual Machines' sharing a set of resources.

The main difference between other resource management techniques and fair share scheduler is that it ensures very high fairness in resource allocation. In the case of priority scheduling a low priority processes will always need to starve. But in the case of fair share scheduler that processes is ensured to get resource at some point of time. Also it ensure that the most needed process will get resource soon and in a timely manner. Similarly in the case of round robin all processes will get a fixed time quantum of resources. So even if a high priority processes is not yet done with its execution, it has to relinquish its resources forcefully. Thus fairness will be lost in

this kind of resource allocation. On the other hand the fair share scheduler ensures that the process's resource requirements are satisfied properly.

4. CONCLUSION

Resource management using the fair share scheduler is very much successful in distributing resources effectively among multiple processes competing for resources. The 'share' for each user can be determined by various methodologies and implementation overhead for these methodologies are very less compared to poor resource distribution penalties. Future work includes using this scheduler for thread scheduling and memory management. By implementing similar methodologies for thread and memory management I believe the operating system efficiency can be increased to a great extend.

5. REFERENCES

- [1] A. Chandra, M. Adler, P. Goyal and P. Shenoy , "Surplus Fair Scheduling: A Proportional-Share CPU Scheduling Algorithm for Symmetric Multiprocessors " , (paper presented in Proceedings of fifth symposium on operating system design and implementation at Boston, Massachusetts , December 9-11 2002)
- [2] P. Goyal, X. Guo, and H.M. Vin." A Hierarchical CPUScheduler for Multimedia Operating Systems. In Proceedings of Operating System Design and Implementation " (paper presented at OSDI'96, Seattle, pages 107–122, October 28-31 1996.)
- [3] K. Duda and D. Cheriton. "Borrowed Virtual Time (BVT) Scheduling: Supporting Latency-sensitive Threads in a General-Purpose Scheduler " .(paper presented in Proceedings of the ACM Symposium on Operating Systems Principles (SOSP'99), Kiawah Island Resort, SC, pages 261–276, December 1999 .)
- [4] J. Nieh and M S. Lam." The Design, Implementation and Evaluation of SMART: A Scheduler for Multimedia Applications " .(paper presented in *Proceedings of the sixteenth ACM symposium on Operating systems principles (SOSP'97), Saint-Malo, France*, pages 184–197, December 1997.)
- [5] Carl A. Waldspurger _ William E. Weihl "Lottery Scheduling: Flexible Proportional-Share Resource Management", Comm. ACM 31(1) (Jan 1988.) , pp. 44–55,
- [6] A Cray X-MP , Henry, G. J. "The Fair Share Scheduler", Bell System Technical Journal, October, (1984).
- [7] Adit Ranadive, Ada Gavrilovska, Karsten Schwan , "[FaReS: Fair Resource Scheduling for VMM-Bypass InfiniBand Devices](#)" ,(paper presented in the Proceedings of the 2010 10th IEEE/ACM International Conference on Cluster, Cloud and Grid Computing ,Australia May 2010)
- [8] C. A. Waldspurger and W. E. Weihl, "Lottery scheduling: Flexible proportional-share resource management".(paper presented in 1st Symp. Operating Systems Design & Implementation, pp. 1–11, USENIX, Nov 1994.)
- [9] J. Nieh, C. Vaill, and H. Zhong, "Virtual-Time RoundRobin: An O(1) proportional share scheduler"(paper presented in . USENIX Ann. Technical Conf. at Boston, Massachusetts pp. 245–259, Jun25-30 2001.)

Performance Evaluation of Reactive, Proactive and Hybrid Routing Protocols Based on Network Size for MANET

Dr. Ritika

Associate Professor and Head MCA Department,
DIT, Dehradun-248001, Uttarakhand, INDIA.

riti_79@rediffmail.com

Dr. Nipur

Associate Professor, MCA Department
Kanya Gurukul Mahavidyalaya,
Dehradun, Uttarakhand, INDIA.

nipursingh@hotmail.com

Abstract

Ad hoc network is a collection of wireless mobile nodes where wireless radio interface connects each device in a MANET to move freely, independently and randomly. Routing protocols in mobile ad hoc network helps to communicate source node with destination node by sending and receiving packets. Lots of protocols are developed in this field but it is not easier to decide which one is winner. In this paper, we present investigations on the behavior of five routing protocols AODV (Ad hoc On demand distance vector), DSR (Dynamic Source Routing), DYMO (Dynamic MANET On demand), OLSR (Optimized link state routing) and ZRP (Zone routing protocol) based on IEEE 802.11CSMA/CA MAC protocol are analyzed and compared using QualNet simulator on the basis of performance metrics such as Average Jitter, Total Packets Received, Packet Delivery Ratio, End-to-End Delay, Throughput, Average Queue Length, Average time in Queue, dropped packets due to non availability of routes and Energy consumption in transmit and receive Mode. To test competence and effectiveness of all five protocols under diverse network scenarios costing is done by means varying load by varying CBR data traffic load, changing number of Nodes and mobility. Finally results are scrutinized in from different scenarios to provide qualitative assessment of the applicability of the protocols.

Keywords: MANETs, DSR, DYMO, AODV, OLSR, and ZRP, CBR.

1. INTRODUCTION

A Mobile ad hoc network is characterized as a network containing nodes that are self organizing and not bound to any centralized control like a base station. The mobile nodes with wireless radio interface are connected by wireless links where each device in a MANET is free to move independently and randomly with the capability of changing its links to other devices frequently. Mobile ad-hoc networks or "short live" networks control in the nonexistence of permanent infrastructure. Though, [1], [2], and [3] illustrates performance of the protocols. This paper throws lights on various experimental and analytical comparative results of AODV, DSR, DYMO, OLSR and ZRP obtained by Qualnet simulator for varying network type, Investigated performance of all five routing protocol uses CBR traffic under Random waypoint Mobility Model. The result draws some general conclusion by considering some vital metrics with MAC and physical layer model which can be helpful in research work of researcher for future references.

2. SIMULATION SETUP

In this scenario wireless connection of varying network size (20 nodes, 50 nodes, 100 nodes and 200 nodes) for MANET is used for comparison the performance of routing protocol (AODV, DSR, DYMO, OLSR, ZRP) and over it data traffic of Constant Bit Rate (CBR) is applied between source and destination. The nodes are placed randomly over the region of 700m x 700m. The 2, 5 and 10 CBR applications are applied in their respective network of size 20, 50 ,100 and 200 over

different source nodes and destinations nodes [20 nodes-> (9, 12) (10, 2), 50 nodes-> (47, 40, 24, 23, 44) (35, 49, 31, 46, 10), 100 nodes-> (99, 63, 47, 49, 73, 76, 29, 37, 86, 41) (13, 32, 2, 36, 8, 23, 75, 4, 70, 38) and 200 nodes->(107, 8, 32, 189, 9, 191, 75, 163, 176, 63, 20, 42, 180, 65, 51) (174, 3, 86, 4, 16, 85, 195, 190, 64, 17, 175, 41, 10, 118, 1)] to analyze the performance of AODV, DSR, DYMO, OLSR and ZRP routing protocols. The animated simulation of network size 20, 50, 100 and 200 are shown in FIGURE 1, FIGURE 2, FIGURE 3 and FIGURE 4.

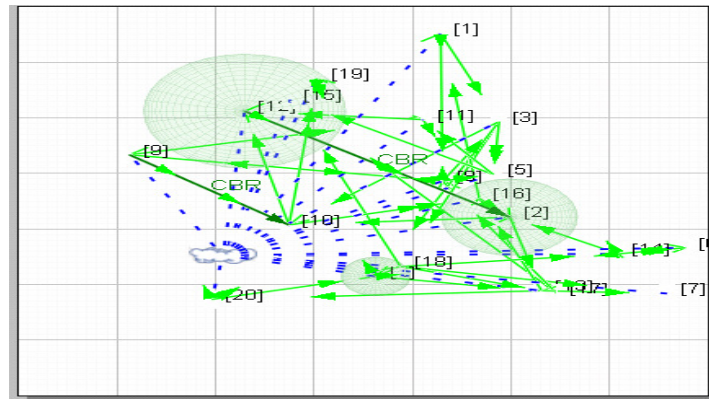


FIGURE 1: Animation view of 20 nodes with 2 CBR(s).

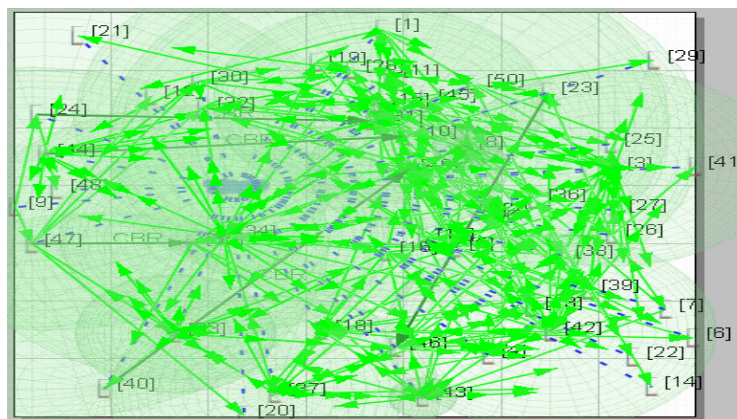


FIGURE 2: Animation view of 50 nodes with 5 CBR(s).

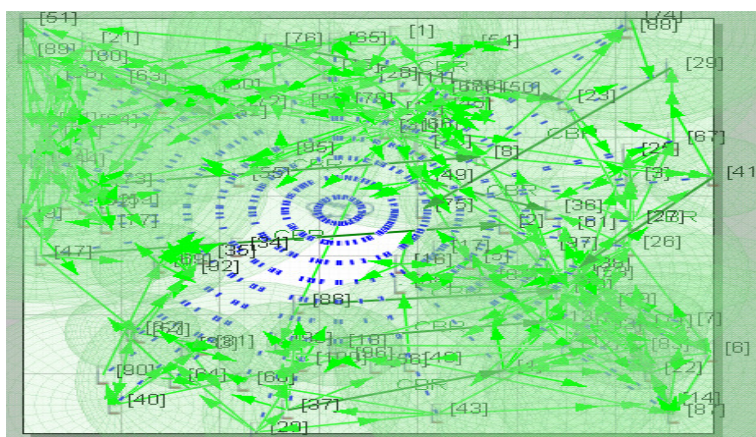


FIGURE 3: Animation view of 100 nodes with 10 CBR(s).

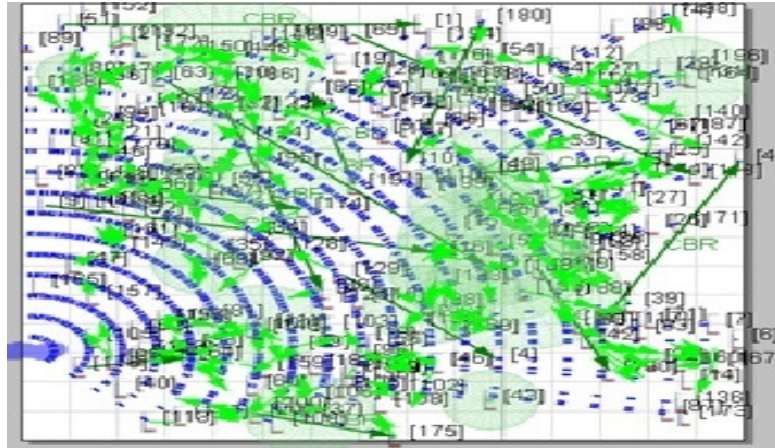


FIGURE 4: Animation view of 200 nodes with 15 CBR(s).

2.1 Performance Analysis: The simulations parameters are shown in Table1.

TABLE 1: Simulation Parameters for varying network where mobility of the nodes kept a constant

Parameters	Values
Simulator	QualNet
Protocols studied	AODV, DSR, DYMO, OLSR & ZRP
Number of nodes	20, 50, 100, 200 nodes
Simulation time	100 s
Simulation area	700*700 sq m
Node movement model	Random waypoint mobility
Traffic types	2, 5 ,10 & 15 CBR sources, respectively
Mobility of nodes	Min speed=1m/s ,Max speed=10m/s,
Rate of packet generation	20 packets/s
Size of packets	1000 bytes

The Qualnet 5.0.2 network simulator [6] is used to analyze the parametric performance of Dynamic Source Routing (DSR) [4, 5], Ad Hoc On-Demand Distance-Vector Protocol (AODV) [8][10], Dynamic MANET On Demand (DYMO) [7], Optimized Link State Routing (OLSR)[11] & Zone Based Routing Protocol (ZRP)[9] routing protocols. The IEEE 802.11[12] for wireless LANs is used as the MAC layer protocol. The performance is analyzed with varying nodes in network keeping traffic load and mobility constant. The results are shown in from FIGURE 5 to FIGURE 13.

3. PERFORMANCE METRICS

3.1 Average Jitter

This metric is calculated by subtracting time at which first packet was transmitted by source from time at which first data packet arrived to destination. This includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue, retransmission delays at the MAC, propagation and transfer times. We can observe that at density of 20 nodes all the four protocols except DSR have small jitter value than at density of 50 nodes. OLSR shows highest jitter and ZRP is next to it for high node density as shown in FIGURE 5. It can be established that

by analyzing effect of network size on jitter for all the five protocols, the jitter although small for small network increase as the network size increases.

Jitter is the variation in the time between packets arriving, caused by network congestion, timing drift, or route changes. But at high density network say for 200 nodes since query packets will be flooded throughout the network control overhead increases, it consumes more time to reconfigure the route if link failure occurs. Hence there will be more time variation between arrivals of packets results in more jitter value.

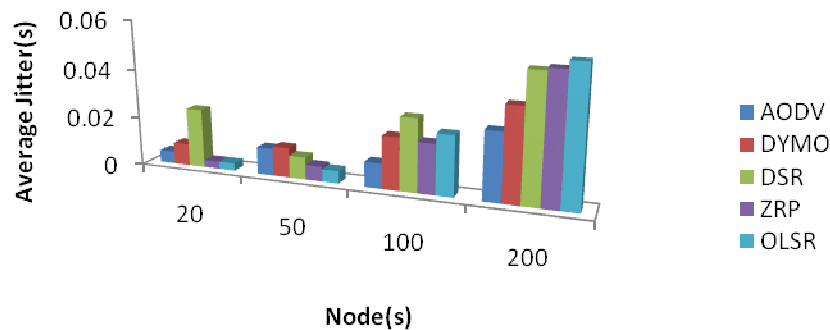


FIGURE 5: Graph [4.6.3.1.1]: IEEE 802.11-CBR Server: Average Jitter(s) for AODV, OLSR, ZRP Comparison-Node (10, 40, 80, 120) Variation Network.

4.6.3.1.2 Packet Delivery Ratio

It specifies the packet loss rate, which limits the maximum throughput of the network. The better the delivery ratio, the more complete and correct is the routing protocol. In the FIGURE 6 we can observe that when network density is less i.e for 20 nodes, numbers of packets delivered are more as compared at denser network of size 200 nodes. DSR has an edge over other protocols in successfully delivering data packets for varying node density. DYMO and AODV are close behind. All the three on demand routing protocols (AODV, DSR and DYMO) are winner in packet delivery statistic. OLSR as traditional wired protocol trail behind on demand protocols. Value for hybrid protocol ZRP is less because as number of nodes increase number of overlapping zones increases thus increases query messages.

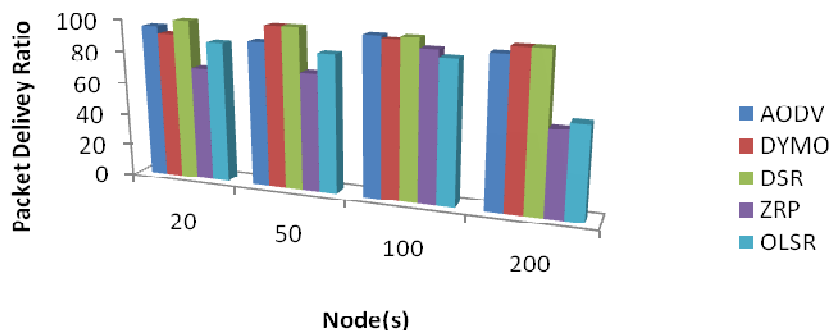


FIGURE 6: Graph [4.6.3.1.2]: IEEE 802.11-CBR Server: Packet Delivery Ratio for AODV, OLSR, ZRP Comparison-Node (10, 40, 80, and 120) Variation Network.

4.6.3.1.3 Average End-to End Delay

Delay metric specifies delays due to route discovery, queuing, propagation and transfer time. After studying the operation of AODV, DYMO, DSR, ZRP and OLSR we can observe that, end to

end delay is more in ZRP as compared to others. ZRP operation of route discovery uses additional time as it uses IARP, IERP and BRP leading to more number of control packets. When a destination node is not found in the local zone of the source node it initializes IERP. ZRP takes time for inter communication between IERP and IARP. Each node maintains routing table of their local zone. This adds unnecessary traffic in the network. This causes route acquisition delay. After discovering the route to the destination the data packets are encapsulated by two protocols. Hence it takes more time for data packet to reach to the destination.

Proactive protocol OLSR is next trailed to ZRP creates large end to end delay in dense network as it periodically exchange topology information to maintain end-to-end routes. For node density of 20, 50 and 100 nodes OLSR has least end to end delay as OLSR uses multipoint relays (MPRs), a node's one hop neighbor selected for forwarding packets, to reduce the control traffic overhead. DSR is behind OLSR as it uses source routing in which a data packet carries the complete path to be traversed, like when DSR starts route discovery it broadcasts RREQ packets to its neighbors. When neighbor node receives RREQ packet for particular destination it checks for the route destination in its Route Cache. If route to the destination is found then that intermediate node sends back the gratuitous RREP to the source node. Where this gratuitous RREP includes the source route to the destination. As it takes additional time to set reverse route to source node by intermediate nodes after receiving RREQ packets. Once the route is discovered in DSR entire source route is available at source node.

While in AODV only at intermediate nodes have the information about next hop neighbors along the discovered path. DYMO has least end-to end delay as sequence numbers used in DYMO makes it loop free. These sequence numbers are used by nodes to determine the order of route discovery messages and so avoid propagating stale route information in high density network. For node density of 20 and 100 average end to end delays of DSR and DYMO are higher than AODV, ZRP and OLSR as shown in FIGURE 7.

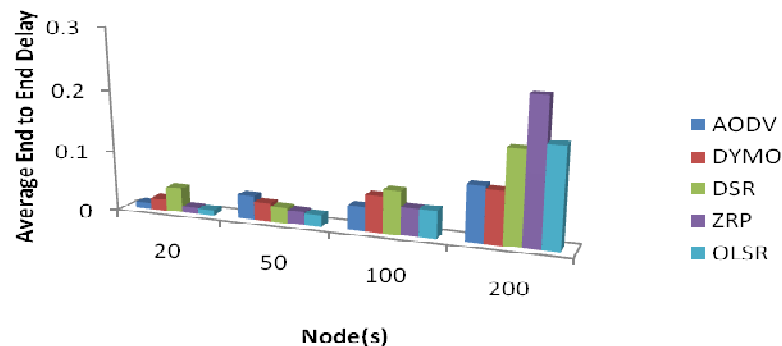


FIGURE 7: Graph [4.6.3.1.3]: IEEE 802.11-CBR Server: Average End to End Delay for AODV, OLSR, ZRP Comparison-Node (10, 40, 80, 120) Variation Network.

4.6.3.1.4 Throughput

Throughput is the average rate of successful data packets received at destination. As the number of the nodes increases in the network, route discovery becomes more complicated, because centralized node routing zones will highly overlap with each other, hence the route request queries will be flooded in to the network, and the intermediate nodes will send same route request queries multiple times, hence the route acquisition delay will have higher percentage as the number of nodes increases.

On demand routing protocols like DSR and DYMO shows good stable results on varying node density. AODV throughput decreases for high density networks. Zone routing protocol results are

painful for increase in node density as are compared to AODV, DYMO and DSR. This is as shown in FIGURE 8.

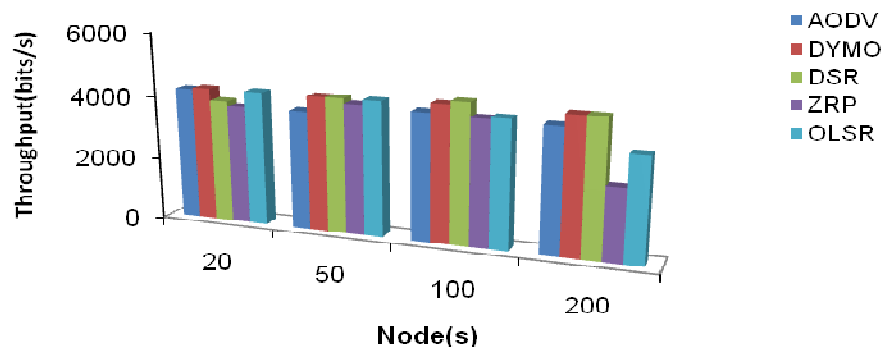


FIGURE 8: Graph [4.6.3.1.4]: IEEE 802.11-CBR Server: Throughput for AODV, OLSR, ZRP Comparison-Node (10, 40, 80, 120) Variation Network.

4.6.3.1.5 Average Queue Length

It is FIFO Queue Size (bytes) in MAC layers. The length of Queue depends on congestion and route discovery. For varying network size AODV builds small queues. DYMO is next following AODV builds queue of small size as shown in FIGURE 9. The lower performance of DSR of different density network is attributed to use of aggressive caching.

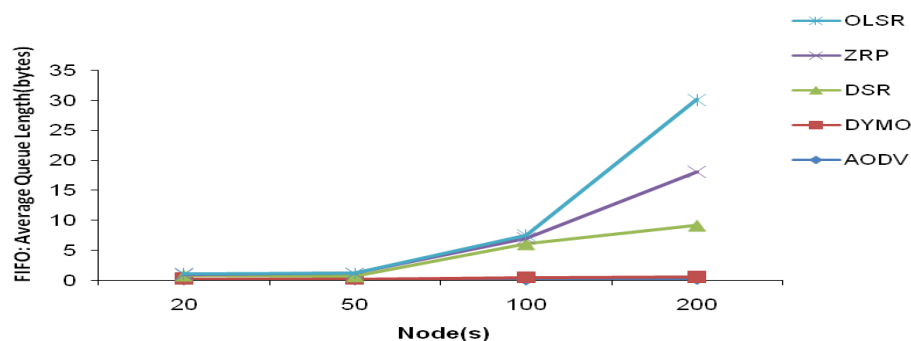


FIGURE 9: Graph [4.6.3.1.5]: IEEE 802.11-FIFO: Average Queue Length(bytes) for AODV, OLSR, ZRP Comparison-Node (10, 40, 80, 120) Variation Network.

Value for hybrid protocol ZRP is high because as number of nodes increase number of overlapping zones increases thus increases query messages. Thus lead to increase in control packets. Also there are chances that these query messages may be forwarded again inward instead of moving towards the destination. This unnecessarily adds build up queue and creates delay in the system. None of the protocol is dramatically worst than OLSR in dense network as OLSR hello messages which may become very large in dense networks since they contain a neighbor list.

4.6.3.1.6 Average Time in Queue

It describes average waiting time of packets to be forwarded or processed. Waiting time for packets in DSR is long as it builds long queue is attributed to use of aggressive caching. Next highest waiting time is for ZRP and OLSR packets as observed for denser networks. In rest of scenario for varying network size AODV, DYMO and ZRP show satisfactory result as shown in FIGURE 10. OLSR processing times of packets are larger in dense network of 200 nodes while negligible for network size of 20, 50 and 100 nodes.

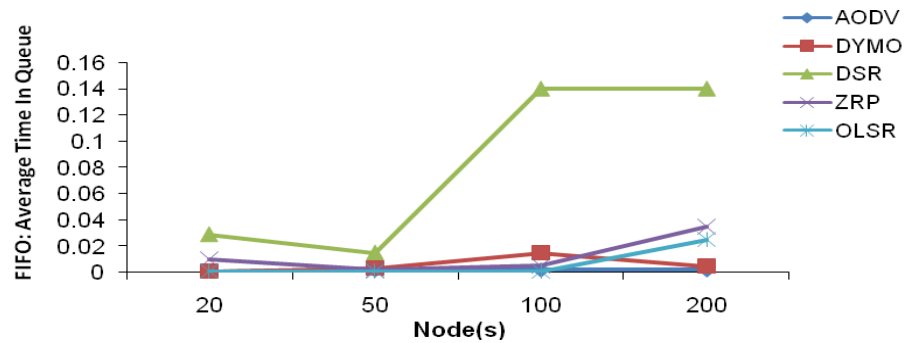


FIGURE 10: Graph [4.6.3.1.6]: IEEE 802.11-FIFO: Average Time in Queue for AODV, OLSR, ZRP Comparison-Node (10, 40, 80, 120) Variation Network.

4.6.3.1.7 Broadcast Received (802.11 DCF)/ Broadcast Packet Received Clearly (802.11 MAC)

IEEE 802.11 MAC describes total number of broadcast received and total number of successful broadcast received from the channel without errors. Values for broadcast received and broadcast received clearly are same as shown in FIGURE 11 and FIGURE 12. It has been observed that large number of broadcast has been received in ZRP and OLSR as both of them make use of proactive approach sends incremental dump to periodically exchange topology information. Broadcast Received clearly in AODV, DSR and DYMO are less due to their reactive nature.

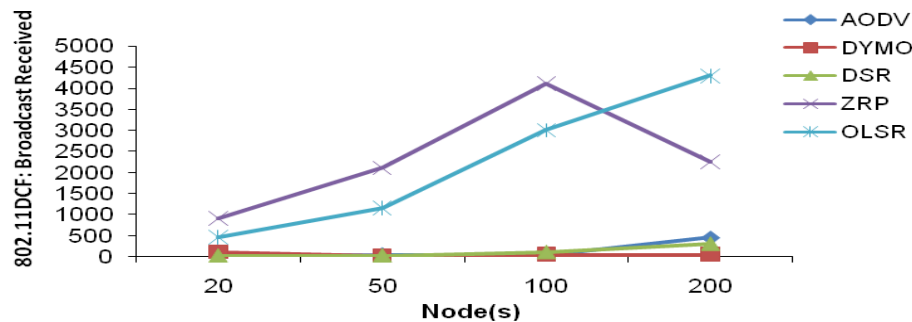


FIGURE 11: Graph [4.6.3.1.7]: 802.11DCF: Broadcast received for AODV, OLSR, ZRP Comparison-Node (10, 40, 80, 120) Variation Network.

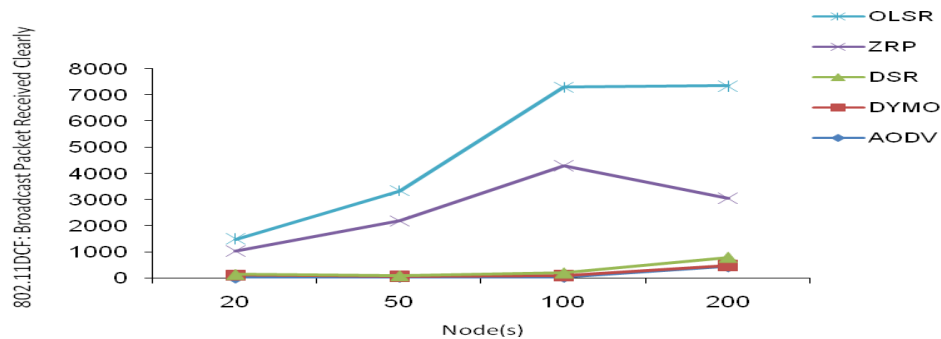


FIGURE 12: Graph [4.6.3.1.8]: 802.11MAC: Broadcast Packet Received Clearly for AODV, OLSR, ZRP Comparison-Node (10, 40, 80, 120) Variation Network.

4.6.3.1.8 Packets from/to Application layer

Small number of packets send from application layer are same for AODV, DYMO, DSR and ZRP for varying network size are shown in FIGURE 13 and FIGURE 14 while bulk of packets are send in OLSR. Same thing has been observed when packets are travelling from transport layer to application layer.

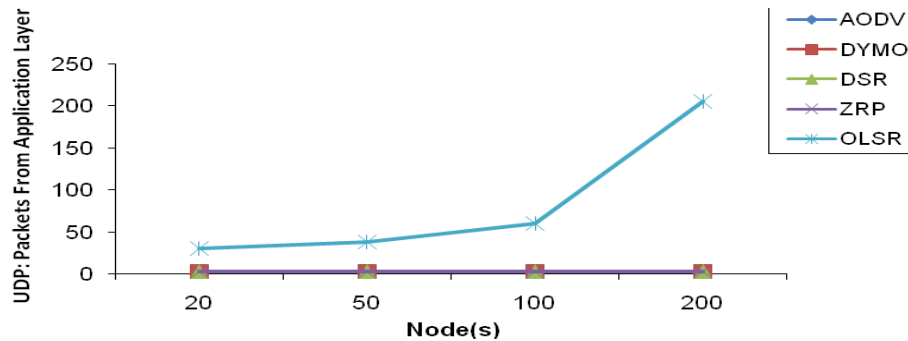


FIGURE 13: Graph [4.6.3.1.9]: UDP: Packets from Application Layer for AODV, OLSR, ZRP Comparison-Node (10, 40, 80, 120) Variation Network.

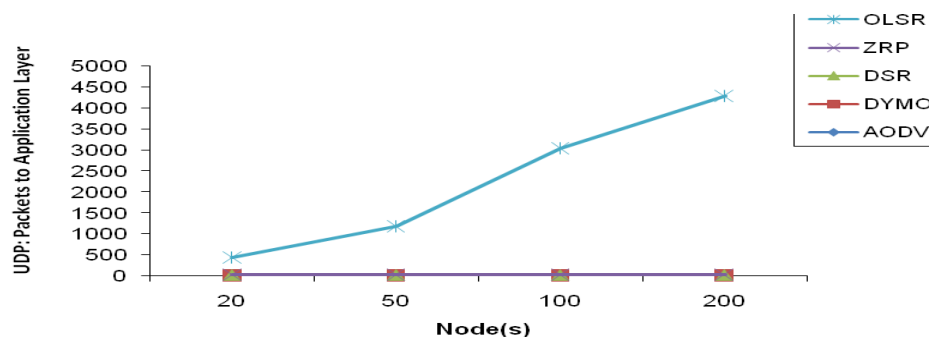


FIGURE 14: Graph [4.6.3.1.10]: UDP: Packets to Application Layer for AODV, OLSR, ZRP Comparison-Node (10, 40, 80, 120) Variation Network.

4. CONCLUSION

For varying network size with constant mobility to analyze the performance of AODV, DSR, DYMO, OLSR and ZRP: The analysis showed on demand routing protocols like DSR and DYMO shows good stable results of throughput on varying node density. AODV throughput decreases for high density networks. DSR has an edge over other protocols in successfully delivering data packets for varying node density. DYMO and AODV are close behind. DSR is better in transmission of packets per unit time and maximum number of packets reached their destination successfully with some delays. Whereas AODV & DYMO having almost same values in all of the performance metrics, they transmit packets with very less delay but transmits less packets to their destination as compare to DSR.

For high node density OLSR shows highest jitter and, ZRP and DSR are next to it. Average Jitter of DSR is high for varying network. End to end delay is more in ZRP as compared to others as ZRP operation of route discovery uses additional time as it uses IARP, IERP and BRP leading to more number of control packets. OLSR is next trailed to ZRP and DSR is behind OLSR as it uses source routing. Waiting time for packets in DSR is long as it builds long queue is attributed to use of aggressive caching which increases with increase in network size. Next highest waiting time is for ZRP and OLSR packets as observed for denser networks.

5. REFERENCES

- [1] M. Naserian, K.E. Tepe, and M. Tarique, Routing Overhead Analysis for Reactive Routing Protocols in Wireless Ad Hoc Networks, IEEE WiMob 2005, Vol.3, pp. 87-92, Montreal, Canada, August 2005.
- [2] P.P. Pham and S. Perrau, Performance Analysis of Reactive Shortest Path and Multipath Routing Mechanism With Load Balance, in Proceedings of IEEE Infocom 2003, pp. 251-259, San Francisco, USA, April 2003.
- [3] L. Viennot, P. Jacquet, and T.H. Clausen, Analyzing Control Traffic Overhead versus Mobility and Data Traffic Activity in Mobile Ad-Hoc Network Protocols, Wireless Networks, Vol. 10, Issue 4, pp. 447-455, July 2004
- [4] J. Broch, David A. Maltz, David B. Johnson, Y-Ch Hu and J Jetcheva, "A performance Comparison of Multi-hop Wireless Ad Hoc Network for mobile ad hoc networks", in Proc. 4th annual IEEE/ACM international conference on Mobile Computing and Networking, Dallas, Texas, U.S.Oct. 1998, pp. 85-97.
- [5] Josh Broch, David B. Johnson, David A. Maltz, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks". Draft, draft-ietf-manet-dsr-00.txt, October 1999. Work in progress.
- [6] Qualnet Simulator www.scalable-networks.com.
- [7] Ian D. Chakeres and Charles E. Perkins. Dynamic MANET on demand (DYMO) routing protocol. Internet-Draft Version 06, IETF, October 2006.
- [8] Charles E. Perkins, Elizabeth M. Royer, Samir R. Das, "Ad Hoc On-demand Distance Vector Routing", IETF Draft, 33 pages, October 1999.
- [9] Z. J. Haas and M. R. Pearlman, "Zone Routing Protocol for Ad Hoc Networks", tech. rep., Internet Engineering Taskforce (IETF), Nov. 1997
- [10] Charles Perkins, Elizabeth Royer, and Samir Das. "Ad hoc on demand distance vector (AODV) routing". IETF RFC No. 3561, July 2003.
- [11] A. Laouti, P. Muhlethaler, A. Najid and E. Plakoo: "Simulation results of the OLSR routing protocol for wireless network", INRIA Rocquencourt, Project Hipercom 2002.
- [12] IEEE, 1997, Wireless LAN Medium Access Control (MAC) and Physical layer PHY Specifications, IEEE Std. 802.11.

Semantic Message Addressing based on Social Cloud Actor's Interests

Reem M. Bahgat

r.bahgat@fci-cu.edu.eg

*Faculty of Computers and Information/
Department of Computer Science
Cairo University
Cairo, Egypt*

Akram I. Salah

Akramsalah.21@gmail.com

*Faculty of Computers and Information/
Department of Computer Science
Cairo University
Cairo, Egypt*

Hamada I. Abdul Wakeil

hamada.mabrouk@computer.miniauniv.edu.eg

*Faculty of Computers and Information/
Department of Computer Science
El_Minia University
El_Minia, Egypt*

Abstract

Wireless communication with Mobile Terminals has become popular tools for collecting and sending information and data. With mobile communication comes the Short Message Service (SMS) technology which is an ideal way to stay connected with anyone, anywhere anytime to help maintain business relationships with customers. Sending individual SMS messages to long list of mobile numbers can be very time consuming, and face problems of wireless communications such as variable and asymmetric bandwidth, geographical mobility and high usage costs and face the rigidity of lists. This paper proposes a technique that assures sending the message to semantically specified group of recipients. A recipient group is automatically identified based on personal information (interests, work place, publications, social relationships, etc.) and behavior based on a populated ontology created by integrating the publicly available FOAF (Friend-of-a-Friend) documents. We demonstrate that our simple technique can first, ensure extracting groups effectively according to the descriptive attributes and second send SMS effectively and can help combat unintentional spam and preserve the privacy of mobile numbers and even individual identities. The technique provides fast, effective, and dynamic solution to save time in constructing lists and sending group messages which can be applied both on personal level or in business.

Keywords: Wireless Communication, Short Message Service, FOAF, J2ME

1. INTRODUCTION

Despite sophisticated collaboration environments being around for a long time already, SMS is still the main means for distributed collaboration. People still use it for maintaining to-do lists, tracking, organization, etc. The major reasons for this may be grounded in the ease of use, the negligible learning effort to be able to use it, the universal availability, and that literally everyone has a phone device uses it and can be contacted and share information and Multimedia via messages.

Telephone numbers, like email addresses, are opaque identifiers. They're often hard to remember, and, worse still, they change from time to time. Mobile numbers are a means to send SMS, but sending individual personalized SMS messages to long predefined list of customers

can be very time consuming and problem of predefined lists is its rigidity and that it requires constant maintenance. The frequency of change adds overhead to the process, wireless communications such as variable and asymmetric bandwidth, and geographical mobility and high usage costs. It would be more effective to find a way to dynamically and automatically create and update those lists.

This paper provides a solution to this SMS sending problems. Our approach is to send SMS to groups of people, either their mobile numbers are saved in or not in your mobile device, by matching a particular set of attributes, e.g., all people who are interested in marketing in an organization, or all people in a specific work place who are interested in maintenance and knows someone. In other words creating the list semantically, meaning the lists are to be built based on customer characteristics or customer behaviors. So from this point of view we need some kind of technology to ensure that the group of people is defined.

The Semantic Web is not a separate Web but an extension of the current one, in which information is given well-defined meaning, better enabling computers and people to work in cooperation. Two important technologies for developing the Semantic Web are already in place: First, eXtensible Markup Language (XML). XML lets everyone create their own tags that annotate Web pages or sections of text on a page or any resource. Second, the Resource Description Framework (RDF) [1]. RDF used to express meaning of any resource and encodes it in sets of triples, each triple being rather like the subject, verb and object of an elementary sentence in which Subject and object are each identified by a Universal Resource Identifier (URI). The Resource Description Framework (RDF) technology such as the Friend-of-a-Friend (FOAF) [2] ontology that predicates a person's express properties such as name, email address, phone number, group memberships, employer, gender, birthday, interests, projects, and acquaintances, and also using the Meaning-of-a-Tag (MOAT) [3] Ontology represents the meaning of user resources.

Our method can be summarized as follows:

- We introduce a technique that utilizes Semantic Web metadata as well as social network techniques to discover a semantically specified group (community or group). Expansion of people extraction is out of the paper scope.
- We propose a technique to send SMS to semantically specified group of recipients.
- We conduct extensive experiments to demonstrate that our technique is effective.

The paper is structured as follows: Section 2 explains the preliminaries for the paper as follows: Subsection 2.1 gives an overview of how the recipients are extracted dynamically based on personal characteristics or behaviors. The Semantic Extraction Method is provided in Subsection 2.2. The Proposed Technique used for Sending Semantic SMS is introduced in Subsection 2.3. Subsection 2.4 shows our experimental results. Finally, conclusion and future work are presented in Subsection 2.5.

2. PRELIMINARIES

2.1 People Extraction Method

Recently, people use social networks to share the interests and contents, such as bookmarks, web blogs, questions/answers, photographs, music, and videos. Building user communities of the same interests, finding the domain experts in different subjects, identifying hot social topics, and recommending personal relevant contents is a fundamental problem of social networks.

Sending SMS to a specific group or community of people requires a method for collecting this group. There have been a plenty of methods and schemes aiming to find users with common interests. Zhao et al. [4] proposed a framework that focused on community extraction based on the strength on ties between members of a community and its ties to the outside world. Li et al. [5] proposed a social interest discovery approach based on user-generated tags. Mika et al. [6]

provided a method for extraction, aggregation and visualization of online social networks based on semantic technologies. Matsuo et al. [7] proposed a social network extraction system called *POLYPHONET*, which employs several advanced techniques to extract relations of persons, detect groups of persons, and obtain keywords for a person. Yan et al. [8] proposed an approach for community discovery based on the contents of social actors' personal interests and their social relationships.

Some of the above methods doesn't use the semantic technologies to form the communities, others used the semantic technologies to form the communities based on users interests but doesn't take in account the meaning of the users interests.

2.2 Semantic Extraction Group (SEGROUP)

We introduce a novel method that employs the semantic web technologies for reasoning with personal information extracted from the Friend-of-a-Friend (FOAF) documents that predicates a person's express properties such as name, email address, phone number, interests, projects, and acquaintances, as shown in FIGURE 1:

1. FOAF and Tag dataset: this dataset is collected by spidering the Semantic Web.
2. People discovery: based on the people's interests and other personal information.

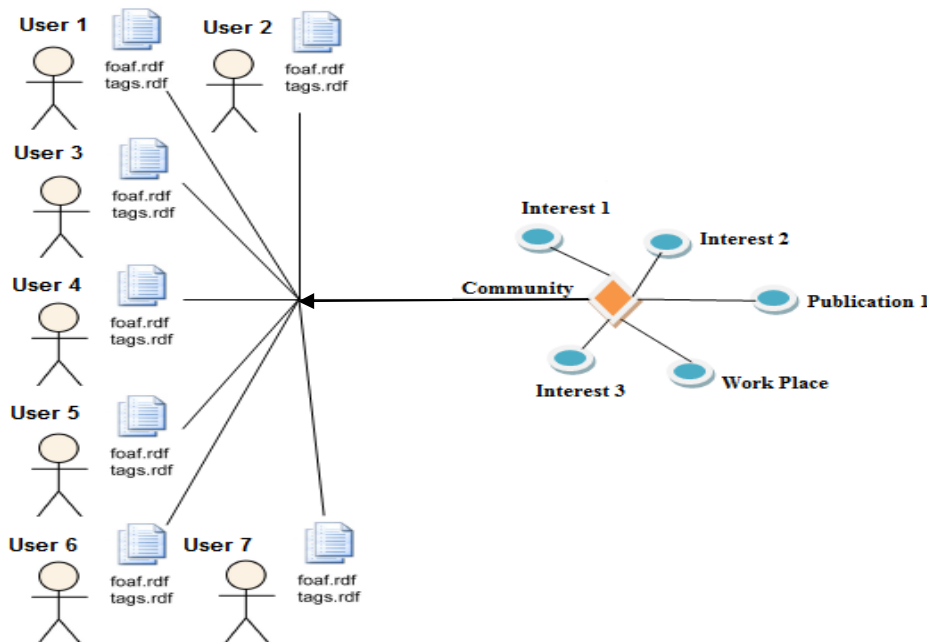


FIGURE 1: People Extraction Process

▪ FOAF and Tag Dataset

FOAF is a machine-readable ontology describing people, their activities, their relationships and objects. FOAF allows groups of people to describe social networks without a centralized database. FOAF is an extension to Resource Description Framework (RDF) and is defined using Web Ontology Language (OWL) [9].

By spidering the Swoogle Semantic Web [12] and collecting the information contained in FOAF files, we can build a large collection of data about people and their personal information. Ding et al. [10] gives a formal definition of a strict FOAF document *D* with the following four characteristic patterns:

1. *D* is a valid RDF document. This can be validated by a RDF parser.
2. *D* uses the FOAF namespace.

3. D contains an RDF graph pattern as shown in FIGURE 2. X and Z are two different instances of `rdfs:Resource` and Y is an instance of `rdf:Property` using FOAF namespace.
4. D defines only one instance of `foaf:Person` without referencing it as an object in any triples within D. D may additionally have some other instances of `foaf:Person`; however, each of them must be referenced as an object in at least one triple in D.

The above patterns, especially the fourth pattern, are quite strict and exclude many documents not dedicating to a person. Therefore, by removing the fourth pattern, Ding et al. [10] defined a general FOAF document as long as it contains of `foaf:Person`.

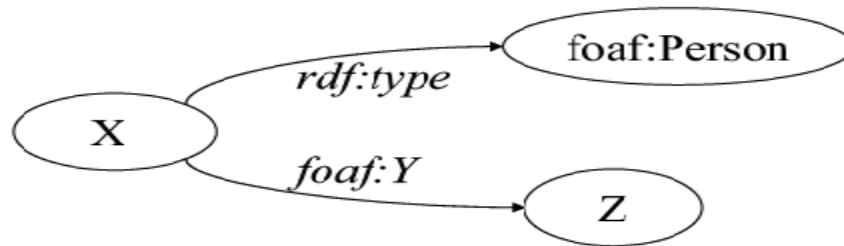


FIGURE 2: FOAF document pattern (image from [10])

▪ People Discovery

Shared Personal Information such as interests and other characteristics are a common method to discover people. But there is a problem faces the methods that depend on personal information, it is hard to extract the representative information from the FOAF properties because it is represented by URLs. One of the most important phenomena of Web 2.0 is **tagging**, that let users play an important role in the process of creating content. Tagging goes a step further by letting them control the way they organize it. Tags generated by users represent their apprehension of the content of the websites. They are more expressive and accurate than the features extracted by machine [5]. But there are other problems faces the methods that depends on tags are the ambiguity and heterogeneity of tags and their lack of machine-understandable. Meaning can be a problem for information retrieval, especially when people use tags that can have different meanings depending on the context.

A concept of the Meaning Of A Tag (MOAT) [3] Ontology that provides a Semantic Web framework to publish semantically-annotated content from free-tagging using URIs of Semantic Web resources such as URIs from DBpedia [14] or any knowledge base. Those URIs are used to identify everything (pages, people, documents, books, interests, etc.) in a unique and non-ambiguous way. An example of the MOAT Ontology is shown in FIGURE 3.

```

<moat:Tag rdf:about="http://tags.moat-project.org/tag/paris">
  <moat:name>![CDATA[paris]]</moat:name>
  <moat:hasMeaning>
    <moat:Meaning>
      <moat:meaningURI rdf:resource="http://dbpedia.org/resource/Paris_%28mythology%29"/>
      <foaf:maker rdf:resource="http://example.org/user/foaf/1"/>
    </moat:Meaning>
  </moat:hasMeaning>
</moat:Tag>
  
```

FIGURE 3: An example of MOAT Ontology (image from <http://www.patrickgmj.net/blog/alexandre-passants-moat-meaning-of-a-tag-project>)

We can use the Friend Of A Friend (FOAF) along with the Meaning Of A Tag (MOAT) Ontologies to represent the user information (foaf.rdf) and the user tags (tags.rdf), respectively and use the relationship between them on foaf:maker property in MOAT ontology to obtain related people who tagged a resource with the same tag name and to get related people who tagged a resource with the same meaning as shown in FIGURE 4 and 5 respectively. All further relevant information can also be easily retrieved in this simple way.

```
select DISTINCT ?maker ?tag_meaning ?tag_name where
{
    ?x foaf:maker ?maker.
    ?y moat:name ?tag_name.
    ?z moat:meaningURI ?tag_meaning.
    filter(?tag_name = "\"" + your_tag_name + "\"")
}
```

FIGURE 4: Querying MOAT for persons tagged a resource with the same tag name

```
select DISTINCT ?maker ?tag_meaning where
{
    ?x foaf:maker ?maker.
    ?z moat:meaningURI ?tag_meaning.
    FILTER regex(str(?tag_meaning), "\"" + your_tag_meaning_URI + "\", \"i\")
}
```

FIGURE 5: Querying MOAT for persons tagged a resource with the same meaning

2.3 The Proposed Technique for Sending Semantic SMS

The proposed technique has two principal processes.

1. Extracting the group(s) process (**SEGROUP**) that combines the content network and social network, and boosts Semantic Web technologies in current Web. Therefore we use the Friend-of-a-Friend (FOAF) ontology that is a first attempt at a formal, machine process-able representation of user profiles and friendship networks. FOAF profiles are created and controlled by the individual user and shared in a distributed fashion. Also the Meaning-of-a-Tag (MOAT) ontology that provides a Semantic Web framework to publish semantically-annotated content from free-tagging using URIs of Semantic Web resources in a unique and non-ambiguous way. Those two Semantic Web Projects FOAF (Friend of a Friend) and MOAT (Meaning of a Tag) can be combined to enable data portability between social media sites to allow us to create and extract the group(s) - the mailing list(s) - that define the SMS recipients.
2. Sending SMS to the selected group process. Sending SMS is no matter how it done, it can be from the mobile device directly or from joining a web site to send the messages. For this we build a server that deal with mobile program for sending.

The proposed technique uses a GUI based on J2ME [13] to set the criteria to collect the group(s) of recipient for the SMS. These criteria will send to a server build in Java. First, the server collects FOAF documents and its associated MOAT documents from the Semantic Web. Second, the server use the criteria send by the sender mobile to query the FOAF and MOAT documents for persons satisfy these criteria as shown in FIGURE 5.

The steps for the first process of the proposed technique can be described as follows:

<p>Step 1: Collect the FOAF and associated Tags files from the Web.</p> <p>Step 2: For each criterion (i.e., tag_name), query the Tags files to select similar persons who tagged their resources with the same criterion, and also select tagMeaningURI for this criterion.</p> <p> 2.1 If found then store the people's foaf.rdf URL in an array (i.e. person array) (with no duplication).</p> <p> 2.2 Use the tagMeaningURI to query tags files to select persons who tags have the same meaningURI, but not equal in tag names (i.e., the criterion).</p> <p> 2.2.1 Do 2.1.</p> <p> 2.3 If no person found then this criterion do not match any person.</p>

In step 2, because the resource may have different tag name according to the person created it, so if a person found who tag a resource with the querying tag name (criterion) we select the meaningURI and use this URI to query for persons who have a tag with this meaning.

The steps for the second process of the proposed technique can be described as follows:

<p>Step 1: Determine the criteria, the message, and the sender mobile number to select group of persons.</p> <p>Step 2: For each person in person array the server query the corresponding FOAF file to select the person phone number or email address and send their names to the sender mobile or a group of the names plus the number of people if large.</p> <p>Step 3: The sender mobile receives the person names whose satisfy the querying criteria, and have option to select some of them.</p> <p>Step 4: The server receives the selected person names and begin to send SMS to them.</p>

In step2, users could email large numbers of people and because each of the data ownership and authentication issues on the internet and inaccurate information. We therefore need safeguards to ensure that user errors won't result in a mass SMS spamming. Feedback to the user regarding his or her query definition could take the form of a list of people to which the SMS will be sent, assuming the number of people is sufficiently small that such a display is feasible. Otherwise, displaying the number of people to which the SMS will be sent along with a sample of those people could be useful. Such feedback would let the user catch errors in the query definition and give confidence that the SMS won't accidentally go to a large number of people for whom it's not meant.

2.4 Experimental Results

This section presents the results of evaluating the effective of the proposed technique that is based on J2ME. We consider the number of recipients as a criterion to evaluate the performance of the proposed method to generate community. The main purpose of the proposed technique is to semantically collect a specified group of recipients. We achieved this by selecting the recipients by using the proposed method for selection **SEGROUP** method. As FIGURE 6 shows the number of members in the community generated from a small tested FOAF and Tag dataset (1000 FOAF and Tag documents created manually). In clustering, the more we add factors that describe the group the more the number of members decreases.

Many of Social Network Sites provides FOAF profiles for their users in different formats such as Facebook, Twitter, Flickr, Myspace, Last.fm. And to exporting FOAF data from different sites as follows:

1. Facebook: <http://www.dcs.shef.ac.uk/~mrowe/foafgenerator.html>
2. Twitter: <http://semantictweet.com/>
3. Flickr: <http://apassant.net/blog/2007/12/18/rdf-export-flickr-profiles-foaf-and-sioc/>
4. And many more (Drupal 7, WordPress plug-ins, etc.).

Because of these differences we chose the format presented by the FOAF project as a standard format to create our dataset. Most of the FOAF profiles generated by social sites may not contains all properties of FOAF and also doesn't provide the tag files for their users, so we created a small FOAF and corresponding Tag dataset manually to use more of the FOAF properties. But the proposed technique can be applied on the FOAF documents collected from different social sites.

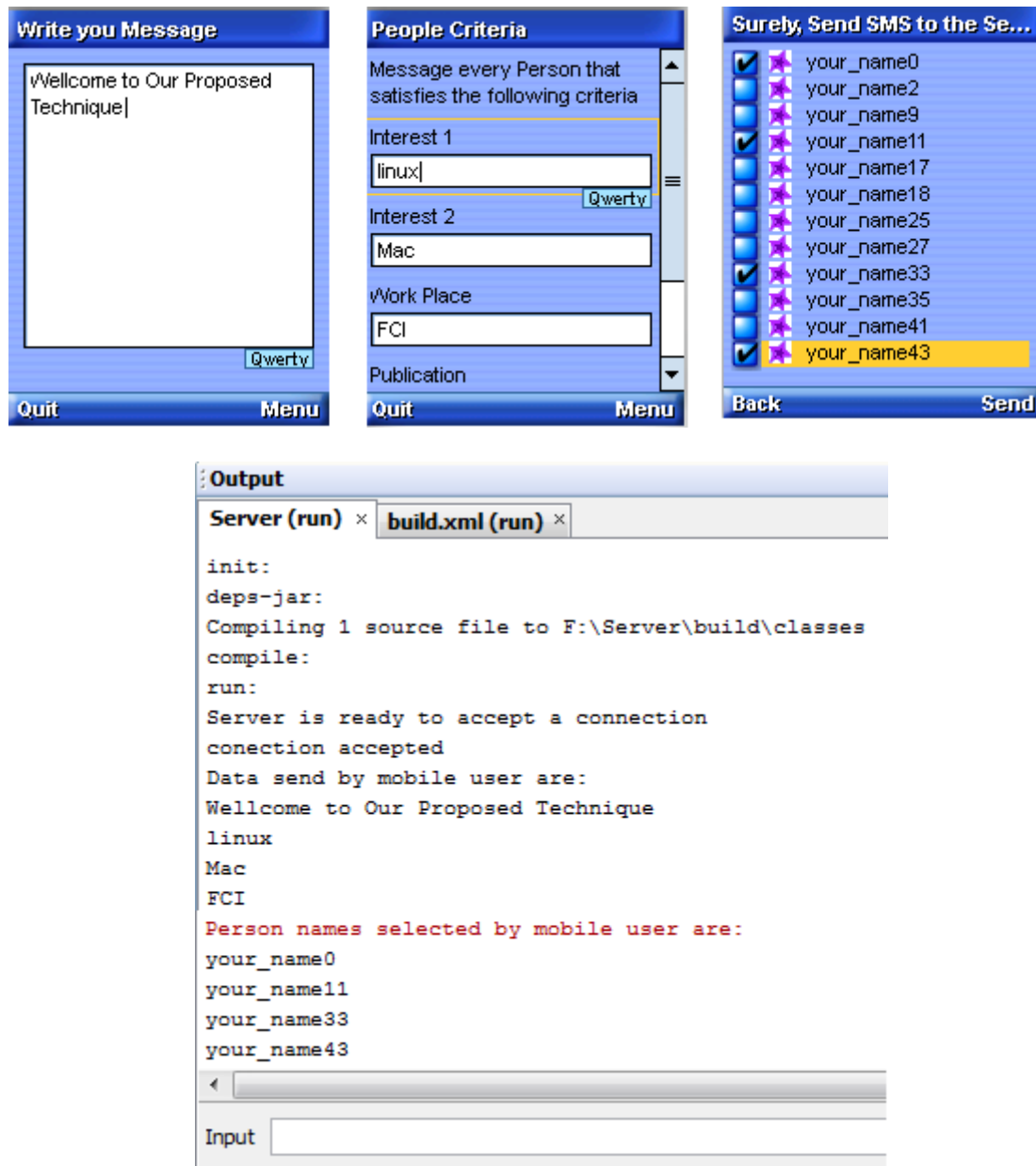


FIGURE 5: Simple example for the proposed technique

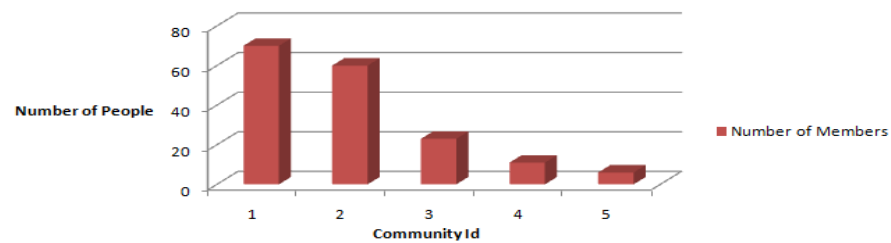


FIGURE 6: Community Size

Category	Type		System Type		User Info.					Community Types	
Method	User Centric	Object Centric	Centralized	Distributed	General Doc.	Network	Profiles	Registration Data	Others	Dynamic	Static
Community Extraction for Social Networks [4]	✓		✓			✓					✓
Tag Based [5]		✓	✓					✓	✓	✓	
Collective Contexts [15]		✓	✓		✓					✓	
Polyphonet [7]	✓		✓		✓						✓
Topic and Role [16]		✓	✓		✓				✓	✓	
Focused Social Extraction [17]	✓	✓	✓		✓			✓	✓		✓
Social Actor's Interests [8]	✓	✓		✓			✓			✓	
Flink [6]		✓		✓	✓		✓		✓	✓	
SEGroup	✓	✓		✓			✓			✓	

TABLE 1: Comparing between methods

TABLE 1 summarizes the main features of some of the semantic extraction methods. The main focus is on the following aspects:

1. Method Type: Means according what the social network is established?
 - 1.1 User Centric: Means detecting social interests based on the social connections among users.
 - 1.2 Object Centric: Means detecting social interests based on the common objects fetched by users.

2. System Type: Means the user profile who control it?
 - 2.1 Centralized: Means the information is under the control of the database owner.
 - 2.2 Distributed: Means the information (profiles) are created and controlled by the individual user and shared in a distributed fashion.
3. User Information: Means the user data are collected from what?
 - 3.1. General Document: Means the user interests are gathered from publications, email archives, and co-authors papers.
 - 3.2. Network: Means the social communities are extracted from the user network.
 - 3.3. Profiles: Means the social interests are gathered from the user profiles or user home page.
 - 3.4. Registration Data: Means the interests are gathered from the user registration data in social networks.
4. Community Type: Specify the ability to update and expand the community or not.

The main ideas of Web 2.0 is to let users play an important role in the process of creating content, so comparing the **SEGROUP** method with all methods that described as centralized in the above table we have better resulting to the **SEGROUP** since it support for the Web 2.0 technologies that contribute to improve the performance of user selection.

The **SEGROUP** method like Social actor's interests [8] from TABLE 1, like the Social Actor's Interests, the **SEGROUP** use the user generated tags to represent the contents. But instead of creating the tag file set (each tag file has representative words corresponding to a foaf:interest), the **SEGROUP** takes into account the meaning of tags to overcome the tag problems, to easy to meaningfully search, and compare or merge similar collective tagging data on different sources through the using of the Meaning-Of-A-Tag (MOAT) ontology that provides a uniform structure and semantics of a set of tags and promotes their global sharing. Using the tag meaning instead of tag file set will minimize the time and effort of search to discover a community. Also lead to discover users who are closer to what we search for.

2.5 Conclusion and Future Work

In this paper a new technique for sending SMS for semantically specified group of recipients is introduced. The proposed technique based on Web 2.0 Social Network application to extract the group of recipients using the FOAF documents and using MOAT ontology to represent the meaning for the user contents. The advantage of this technique First, the technique doesn't require the user to save long list numbers in her/his mobile device. In addition, the technique doesn't requires the user to update the list individuals by subscribe or unsubscribe them. The experimental results show that the technique can send SMS effective and can help combat unintentional spam and preserve the privacy of mobile numbers and even individual identities. Future work is required to add Security, solving the issues of ownership and authentication on the internet and using the mobile Agent to overcome the wireless network problems.

3. REFERENCES

- [1] S-F. Luis and F-G. Norberto. "The Semantic Web: Fundamentals and A Brief State-of-the-Art". The European Journal for the Information Professional Vol. VI, No. 6, December 2005.
- [2] "The FOAF Project". Internet: <http://xmlns.com/foaf/0.1/>, [2011, March].
- [3] A. Passant, P. Laublet. "Meaning Of A Tag: A Collaborative Approach to Bridge the Gap Between Tagging and Linked Data". LDOW2008, April 22, 2008.
- [4] Y. Zhao, E. Levina, and J. Zhu. "Community extraction for social networks". arXiv: 1-15, May 18, 2010.
- [5] X. Li, L. Guo, Y. E. Zhao. "Tag-based Social Interest Discovery". Presented at the 2nd Int. World Wide Web Conference Committee (IW3C2). Beijing, China, 2008.

- [6] P. Mika. "*Flink: Semantic Web Technology for the Extraction and Analysis of Social Networks*". Elsevier Science, May 14, 2005.
- [7] Y. Matsuo, J. Mori, M. Hamasaki. "*POLYPHONET: An Advanced Social Network Extraction System from the Web*". Presented at the 2nd Int. World Wide Web Conference Committee (IW3C2). Edinburgh, Scotland, 2006.
- [8] F. Yan, J. Jiang, Y. Lu, Q. Luo, M. Zhang. "*Community Discovery Based on Social Actors' Interests and Social Relationships*". In Proc. 4th Int. Conf. on Semantics, Knowledge and Grid, 2008, pp. 79-86.
- [9] M. K. Smith, C. Welty, and D. McGuinness. "*Owl web ontology language guide*". W3C recommendation, [On-line]. Available: <http://www.w3.org/TR/owl-guide> [May 13, 2011].
- [10] L. Ding, L. Zhou, T. W. Finin, and A. Joshi. "*How the semantic web is being used: An analysis of foaf documents*". HICSS, 2005.
- [11] A. Seaborne and E. Prud'hommeaux. "*Sparql query language for rdf*". W3C recommendation, [On-line]. Available: <http://www.w3c.org/TR/rdf-sparql-query/> [Jan. 1, 2011].
- [12] L. Ding, T. Finin, A. Joshi, R. Pan, R. Cost, Y. Peng, P. Reddivari, V. Doshi, and J. Sachs. "*Swoogle: A search and Metadata engine for the semantic web*". Presented at the Int. Conference on Information and Knowledge Management. Washington, DC, USA, 2004.
- [13] J. Keogh. "*J2ME: The Complete Reference*", Brandon A. Nordin, 2004.
- [14] S. Auer, C. Bizer, G. Kobilarov, J. Lehmann, R. Cyganiak, and Z. Ives. "*DBpedia: A Nucleus for a Web of Open Data*". Presented at the 6th Int. Semantic Web Conf. November 2007.
- [15] J. Mori, T. Tsujishita, Y. Matsuo, and M. Ishizuka. "*Extracting Relations in Social Networks from the Web using Similarity between Collective Contexts*". ISWC 2006, 487-500, 2006.
- [16] A. McCallum, A. Corrada-Emmanuel, and X. Wang. "*Topic and Role Discovery in Social Networks*".
- [17] M. Hamasaki, Y. Matsuo, K. Ishida, Y. Nakamura, T. Nishimura, and H. Takeda. "*Community Focused Social Network Extraction*". Springer Verlag, Berlin Heidelberg, 2006.

Algorithm and Programme for Computation of Forces Acting on Line Supports

Abdulaziz Salem Bahaidara

*Faculty of engineering/Electrical Engg. Departt.
University of Aden
Aden, Republic of Yemen*

abdulaziz_bahaidara@yahoo.com

Abstract

The correct design and selection of line supports is of great importance for successful operation and safety of transmission lines. For this purpose, various forces acting on the line supports must be estimated for normal and abnormal conditions of operation. The author develops algorithm and programme for optimal calculation of these forces, which the line supports should withstand.

The main programme MDFLS and fourteen subroutines are constructed for calculation the forces acting on the line supports. The subroutines (FSUS, FDES, and FCSTA) are for determining the forces from line conductors and (FGWSU, FSWDE, FSWSA) from ground wires at suspension, dead end and strain/angle line supports respectively. The other eight are subsidiary subroutines. The parameters of the conductors (homogenous or non-homogenous) are found by DPMPN and DPMPH. The physical-mechanical properties of the conductor are calculated using PMPL. The specific loadings are determined by RLOLC. The sag-tension calculations are prepared by subroutines CSCT, CSOP and SEQS. Subroutine FSPCB is for calculation of forces due to broken conductor at suspension support in the section. The elaborated programmes are written in FORTRAN 90 and adopted for personal computer.

Keywords: Line Support, Operating Condition, Forces, Tension, Span, Sag.

1. INTRODUCTION

This paper deals with, computation forces acting on line supports, a part of future proposed compound package of programmes related to mechanical design of transmission lines. Line supports of overhead lines ensure the necessary clearances. They should be cheap and stable to loadings, caused from atmospheric conditions and from operating conditions of the phase conductors and ground wires. [1, 9]

The phase conductors and ground wires are unequal loaded when in one or several spans from the section the specific loads are less or greater from these in the remaining spans. The reason of unequaled loading of the conductors is their ice covered. Usually at ice-covered conductors are covered uniformly with ice, but their release from ice may not occur simultaneously for all conductors and ground wires in all spans of the section. The conductor may be released from ice in one or several spans, while in other spans remains ice covered.

The unequaled loading of the conductors' causes: Approach of the conductors situated one above other phases. Approach of the phase conductors near ground wires; release of a conductor from skip terminals at large deflection of insulator strings by axis of electrical line; approach of a conductor near the cross arm of a support at deflection of insulator string.[3,4]

At broken off conductor operating conditions of electrical line are sharply varied. In normal operating condition suspension and strain supports are loaded with forces from the weight of a conductor and from wind pressure in the direction of electrical line, forces are approximately equal to zero. At broken off conductor appreciable forces are raised, which loaded the line

supports. These forces are the biggest for the supports, which confined the span with broken off conductor.

If the conductor is broken off in one span of the section, the insulator strings are deflected and the supports are bended to direction of the spans, at which the entire conductor is preserved. By moving away from the location of the damage, the quantity of the support deformation and the deflection of the insulator strings are reduced. The forces in the conductor at abnormal operating condition are considerably less from its previous normal operating condition; the damages of a conductor are so high. [1, 5]

The overhead electrical lines are computed for abnormal operating condition with broken off conductor due to the following reason: In order to determine the forces, with which the conductors loaded the supports in abnormal operating condition; to determine the sag of a conductor in spans, in which the conductor is healthy. This sag is required, in order to calculate the distances between the conductors and the equipments located under them. [5, 6]

2. LINE CONDUCTOR INDEXES [2, 7]

The physical-mechanical properties of the line conductor are determined. These are: cross-sectional area, weight of the conductor, modulus of elasticity, temperature coefficient of linear expansion, permissible tensile stress, the stress at minimum temperature and the stress at maximum loading. The forces, which are loading the conductors of an overhead line are, their weight, wind pressure, weight of ice and combinations between these forces. Depending up on the given value of operating voltage of the line, the standard clearances are selected and the specific loadings (G_1 - G_7) are calculated.

Critical span and temperature are calculated for finding operating condition for maximum stress in the conductor and maximum sag. The operating condition, at which maximum tension occurs in the conductor, is determined by a comparison of the actual span (given) with critical span. When actual span (l_a) is greater than or equal to critical span (l_{cr}), maximum tension in the conductor occurs at the operating condition of maximum loading and at actual span less than critical span, maximum tension in the conductor occurs at the operating condition of minimum temperature. With criteria, critical temperature (t_{cr}), operating condition is determined at which maximum sag occurs in the conductor in the span. When critical temperature is less than maximum temperature (t_{max}), maximum sag occurs at maximum temperature and at critical, temperature greater than or equal to maximum temperature, maximum sag occurs at ice covered conductor load (G_3) and air temperature -5°C .

3. MAXIMUM LOADING AND TENSION AT ABNORMAL CONDITIONS [1, 5]

At normal operating conditions, suspension and tension supports are loaded with the conductor weight and wind pressure while tension in the direction of electrical line are almost equal and their resultant is zero. When one of the conductors is broken off, the operating conditions of the electrical line will vary sharply and abnormal tension in the direction of the electrical line will load the supports and these tensile forces will gradually increase towards the nearest support to the damaged span, therefore, insulators will be deflected and supports will be bended to the direction of span at which whole conductors are preserved. The deformation of supports is gradually reduces towards the farest support from the location of broken off conductor.

Forces at abnormal condition must be calculated in order to determine loadings on the line supports, when the conductors are broken off. However the new sag must be calculated to determine the clearances between conductors and equipments located under the electrical line. Calculation of abnormal forces can be done in analytical manner by using Shanfer Pharmakovski method [1, 2]. The magnitude of the influenced force (T_{ab}) is calculated depending on critical span.

$$\text{At } l_a \geq l_{cr} \quad T_{ab} = \sigma_{G3} S \quad (3.1)$$

$$\text{At } I_a < I_{cr} \quad T_{ab} = \sigma_{tmin} S \quad (3.2)$$

Where

σ_{tmin} , σ_{G3} - permissible tension in the conductor at minimum temperature and load G_3 (loading due to conductor weight when covered with ice).

S - The cross-sectional area of the conductor.

4. OPERATING CONDITIONS OF OVERHEAD LINES [5, 8]

The line supports are determined in normal and abnormal operating conditions. Normal operating condition is that at which phase and ground wire conductors in all spans of the section are healthy and parameters of an overhead electrical line are within permissible limits. All types of supports are determined for forces conditioned by the following two normal operating conditions:

1. Normal operating condition I, which is described with: phase and ground wire conductors with no ice; maximum wind pressure (perpendicular to the axis of the electrical line); air temperature 15° C.
2. Normal operating condition II, which is described with: ice covered phase and ground wire conductors; 25% of maximum wind pressure; air temperature-5°C. In an abnormal operating condition such as broken off phase conductor or ground wire, wind pressure is assumed to be zero. The location and number of broken off conductors is standardized and depending upon the type of line supports [3,4]
3. Abnormal operating condition, broken off phase conductors provoked maximum bend moment in the elements of the line support.
4. Abnormal operating condition, broken off phase conductors provoked maximum torsion moment in the line support.
5. Abnormal operating condition with broken off ground wires and healthy phase conductors.

In the normal operating condition the following forces act on the suspension line support; vertical-from the weight of the conductors ground wires, insulators, cross arms and support itself; horizontal, perpendicular to the axis of electrical line from influence of wind; horizontal coincided with axis of electrical line-from forces of straining conductors from the two sides of suspension support; in normal operating condition this forces is equal to zero, since the conductors are pulled out for the entire section.

In the abnormal operating condition the following forces act on the suspension line support ; vertical-from the weight of the equipments of electrical line ; horizontal, coincided with axis of electrical line-caused from unbalanced forces in the conductors of individual spans ; suspension insulators with pin type insulators are not determined in abnormal condition, but they should stand loadings by axis of electrical line up to 150 Newton (at this force broken off the dressing is occurred; breakdown the insulator or hook). Horizontal, perpendicular to axis of electrical line force does not exist, because the velocity of the wind at abnormal condition is assumed to be equal zero.

The forces, which act strain supports in normal condition, are equal in magnitude and direction with these, which act on suspension supports. For abnormal condition more heavy computational conditions for strain supports-it is assumed a greater number of broken off conductors. Strain supports are calculated also in stringing condition with forces at side strained conductors.

In the normal condition the following forces act on the conductors, insulators, cross arms, support and others; horizontal, by axis y-from the strain force of conductors $2T \sin (\chi/2)$ is assumed that in this direction the wind acts with maximum force on the conductors and the elements of the support; horizontal, by axis X-in normal condition this force does not act.

In the abnormal condition the following forces act on angle support: vertical, by axis Z-from weights of elements of electrical line ; horizontal, by axis X-from the component of the straining force of healthy conductors- $F_x = T_{ab} \cos(\chi/2)$; horizontal and coincided with axis Y-from the component of straining forces of healthy conductors $F_y = T_{ab} \sin(\chi/2)$.

On dead end supports more high forces act on from straining of the conductors and ground wires. In the normal operating condition vertical forces act on them from weights of conductor elements. Coincided with axis of electrical line, straining forces of conductors and ground wires act on them. The straining of the conductors from the side of distribution outfit is small and its opposed force is neglected. Perpendicular to the electrical line it is assumed that, forces are acted from wind pressure on the conductors and the elements of support. Forces, which loaded support in abnormal condition, are less from forces acting at normal condition. In some cases enclosed points of these forces are such that the support subjected to high torsion moments, which should be taken into consideration during its design.

5. FORCES ACTING ON LINE SUPPORTS [3, 4]

The forces, with which the conductors loaded the line supports of overhead transmission line, are computed at construction of new supports or for check of the loading on the existing support. The forces, which loaded a support are determined by their components along the axis of the three coordinate system X,Y and Z, where-axis X is along the direction of electrical line ; axis Y is perpendicular to the direction of the electrical line, and axis Z is along the axis of the support in the downward direction.

The forces, with which the conductors act on the specified support (say A) at flat terrain, are the following [5]:

$$F_1 \equiv \begin{cases} F_{1X} = T'_s = \sigma'_s S \\ F_{1Y} = \frac{P_{1Y}}{2} \\ F_{1Z} = \frac{P_{1Z}}{2} \end{cases} \quad (5.1)$$

$$F_2 \equiv \begin{cases} F_{2X} = -T''_s = -\sigma''_s S \\ F_{2Y} = \frac{P_{2Y}}{2} \\ F_{2Z} = \frac{P_{2Z}}{2} \end{cases} \quad (5.2)$$

$$F = F_1 + F_2 = \begin{cases} F_X = F_{1X} + F_{2X} = (\sigma'_s - \sigma''_s) S \\ F_Y = F_{1Y} + F_{2Y} \\ F_Z = F_{1Z} + F_{2Z} \end{cases} \quad (5.3)$$

Where

T_o and T_o are the strain forces in the conductor in the spans (adjacent to the specified support) number 1 and number 2 respectively ; $P_{1Y}=GSl_1$ and $P_{2Y}=GSl_2$ -the forces from conductors at influence of wind on no-ice covered ($G=G_4$) or ice covered conductors ($G=G_5$) for spans number 1 and number 2 respectively; $P_{1Z}=GSl_1$ and $P_{2Z}=GSl_2$ -force from the weight of not iced ($G=G_1$) or ice covered conductors ($G=G_3$)for spans number 1 and number 2 respectively.

The forces from the weight and the wind pressure are distributed equally between the two supports, which are restricted the span. Therefore the specified support (say A) is loaded with half of forces from spans number 1 and number 2. The reactions of the forces in the attachment points of the conductor at the support (say A) are equal and opposite acting forces.

At normal operating condition of electrical line with suspension insulators horizontal component of tensile stress in the conductors is same for all spans of section. Therefore $F_x=0$ At conductors with pin type insulators in normal operating condition horizontal component of the tensile stress in

conductor for the spans of the section is different, but the differences are small and can be neglected and therefore $F_x \approx 0$.

In abnormal operating condition of electrical line the component F_{2x} is equal to zero, if the conductor is broken off in the second span. The component $F_{1x} = T_{ab}$.

The suspension and strain line supports are determined for forces (5.3). For dead end line supports, forces from the conductors of one span are equal to zero. The forces, with which the conductors act on dead end line supports, are determined by (5.1).

At inclined terrain, for calculation the result force acting of the conductors in the attachment point, all acting forces are projected on coordinate axis and their projections are summing. It is obtained that

$$F_2 \equiv \begin{cases} F_{2x} = -T'' \cos \alpha_2 \\ F_{2y} = \frac{P_{2y}}{2} - T'' \sin \alpha_2 \cos \varphi \\ F_{2z} = \frac{P_{2z}}{2} + T'' \sin \alpha_2 \cos \varphi \end{cases} \quad (5.4)$$

Where

φ is the angle of inclination of the conductor due to wind pressure ;

α_2 is the angle of the slop of conventional horizontal span.

The angle α_2 can be calculated by

$$\tan \alpha_2 = \tan \psi_2 \sin \varphi \quad (5.5)$$

Where ψ_2 is the inclination of the terrain from the right side of the support.

By similar way the components of the force for span number 1 can calculated:

$$F_1 \equiv \begin{cases} F_{1x} = T' \cos \alpha_1 \\ F_{1y} = \frac{P_{1y}}{2} + T' \sin \alpha_1 \cos \varphi \\ F_{1z} = \frac{P_{1z}}{2} - T' \sin \alpha_1 \sin \varphi \end{cases} \quad (5.6)$$

The result force, which is acted on the support:

$$F = F_1 + F_2 \equiv \begin{cases} F_x = F_{1x} + F_{2x} \\ F_y = F_{1y} + F_{2y} \\ F_z = F_{1z} + F_{2z} \end{cases} \quad (5.7)$$

The reactions of the forces, with which the conductor acts for the support, are equal and opposite the acting forces in the attachment point of the conductor. The acting forces are calculated for equivalent spans of the specified support l_{e1} and l_{e2} [4, 5]. They are large and small equivalent spans if the specified support is located higher and lower than the adjacent supports respectively. Small and large equivalent spans if the specified support is lower from the left side support and higher from the right side support or vice versa. The result force from the conductors on dead end support are determined by (5.7) for $F_2=0$.

At angle support the electrical line changes its direction with angle χ . For calculation forces, acting on angle support coordinate system is introduced with inception in the attachment point at specified angle support. It is assumed, that the direction of the wind is coincided with axis Y. The force, with which wind pressure acts on the conductors in the span with length l , is calculated by

$$P_y = G S l \cos(\chi/2) \quad (5.8)$$

The confront with the direction of the conductors, the component of wind is put with strain force T' or T''

The forces in the conductor in its attachment points to specified support are determined separately for spans number 1 and number 2. For that aim subsidiary coordinate systems are introduced with start point specified support and with axis: axis X_1, X_2 -with direction of the conductors in span number 1; and span number 2 respectively. Axis Y_1 and Y_2 are perpendicular to X_1 and X_2 respectively. For subsidiary coordinate systems forces are calculated, as at supports, located in straight line at flat terrain, and only the force from wind introduces its component on axis Y-equation (5.9).

The forces from conductor from spans number 1 and number 2 are respectively

$$F_1 \equiv \begin{cases} F_{1x} = T'_o \\ F_{1y} = GS \frac{l_1}{2} \cos \frac{\chi}{2} \\ F_{1z} = GS \frac{l_1}{2} \end{cases} ; \quad F_2 \equiv \begin{cases} F_{2x} = -T''_o \\ F_{2y} = GS \frac{l_2}{2} \cos \frac{\chi}{2} \\ F_{2z} = GS \frac{l_2}{2} \end{cases} \quad (5.9)$$

The result force from conductor in the attachment point is found by projection of the forces F_1 and F_2 on the axis of the basic coordinate system X Y Z.

$$F \equiv \begin{cases} F_x = (T'_o - T''_o) \cos \frac{\chi}{2} + GS \frac{l_2 - l_1}{2} \sin \frac{\chi}{2} \cos \frac{\chi}{2} \\ F_y = (T'_o + T''_o) \sin \frac{\chi}{2} + GS \frac{l_1 + l_2}{2} \cos^2 \frac{\chi}{2} \\ F_z = GS \frac{l_1 + l_2}{2} \end{cases} \quad (5.10)$$

The forces, with which the conductors act on angle support in inclined terrain, are calculated, as for angle support in flat terrain. The components of the forces from conductor are calculated by (5.4) and (5.6). The difference is only in the direction of wind pressure, which is at angle $\chi/2$ with respect to axis of the electrical line, and its component is determined by (5.8).

The components of the force F on the basic coordinate system are

$$F \equiv \begin{cases} F_x = (F_{1x} - F_{2x}) \cos \frac{\chi}{2} + (F_{2y} - F_{1y}) \sin \frac{\chi}{2} \\ F_y = (F_{1x} + F_{2x}) \sin \frac{\chi}{2} + (F_{1y} + F_{2y}) \cos \frac{\chi}{2} \\ F_z = F_{1z} + F_{2z} \end{cases} \quad (5.11)$$

6. COMPUTER PROGRAMME

The synthesis algorithm has been written in FORTRAN – 90, and run on a personal computer. Figure 1. shows the flow chart of the programme, which consists of one main programme MDFLS and fourteen subroutines.

The input data : Nominal voltage kv; climatic area – TEP is equal to one for specified standardized or equal to two for special climatic area; length of the span l ; STC1 and STC2 are

codes for the phase conductor and ground wire respectively; λ is the length of insulator string; G_i is the weight of the insulator; χ is the angle of deflection of the trace; ψ_1 and ψ_2 is the inclination of the terrain from the right side and left side of the line support respectively; l_1 and l_2 are the length of the spans adjacent to the specified line support.

The parameters of the line conductors are found by subroutines DPMPH and DPMPN [2]. The subroutine PMPL is used for calculation of physical-mechanical properties of the phase conductors (PF=1) and ground wires (PF=2). The specific loadings are determined by subroutine RLOLC. Subroutine CSCT is for calculation of critical values of span and temperature and CSOP is for determination of operating condition. SEQS is for solution equation of state and it is a subsidiary function to CSCT.

The forces acting from phase conductor on suspension, strain or angle and dead end towers are determined by FCSUS, FCSTA and FCDES respectively. The forces acting from ground wires on suspension, strain or angle and dead end towers are determined by FGWSU, FGWSA and FGWDE. The subroutine FSPCB is used for calculation of the force loading line support at broken off conductors in the section.

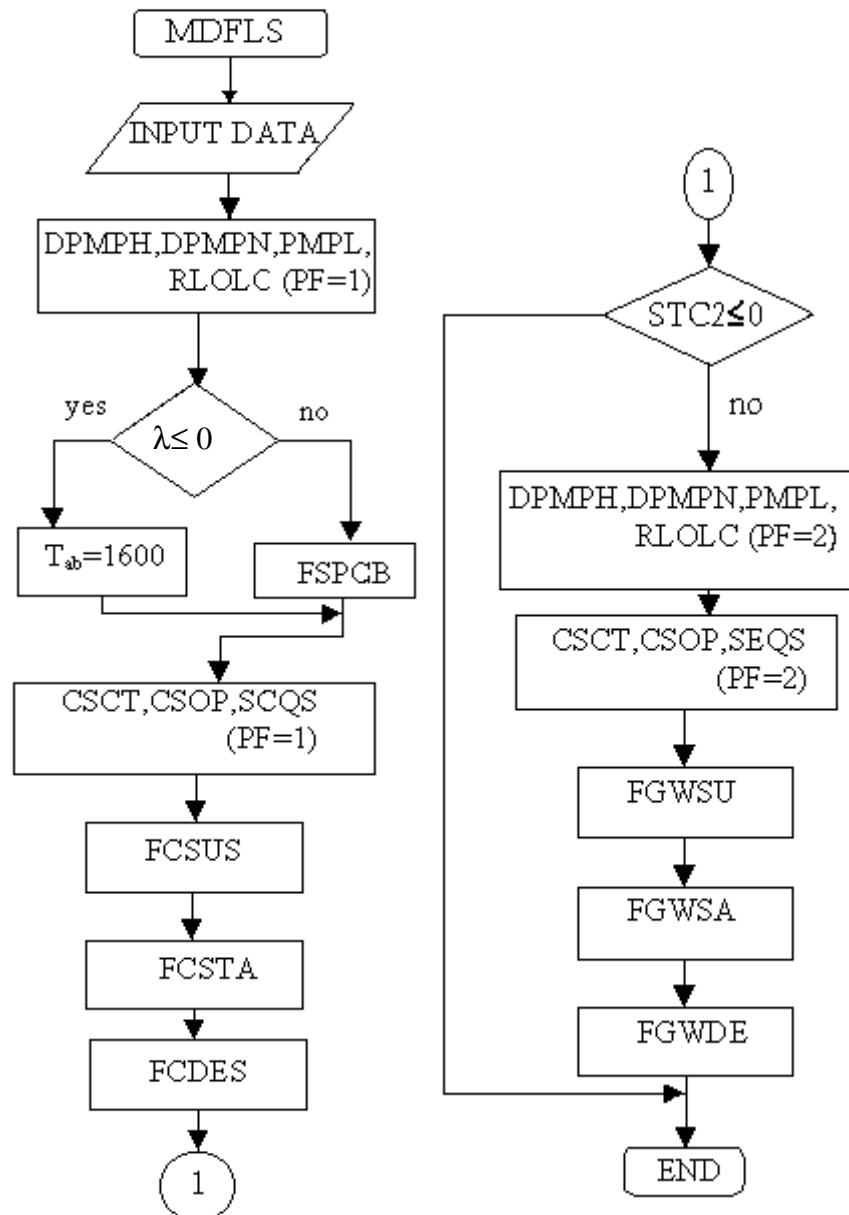


FIGURE 1: Flow chart of programme MDFLS

7. CONCLUSION

For selection and design of the line supports, loadings due to the conductors and wind pressure must be estimated for normal and abnormal conditions of operation. The selected supports should be mechanically strong to withstand these forces.

The elaborated programme enable obtaining the optimum solution of the problem, aiming to increase reliability of transmission lines and the calculated forces to be in consistent with the specified regulations within the permissible limits. Our country began construction of national system high voltage transmission lines 132 kv and in future 220 kv and 400 kv will be erected.

Such programmes are needed and necessary and their use have great benefits. They will give a precise solution, in short time, for one of the problems of mechanical design of an overhead transmission line.

There are some specific areas in our country, which are with high humidity. The future research direction in this field of the existing research paper is to investigate the effect of humidity in the design of line supports for these areas, e.g. the change in the clearances of line supports due to high humidity. This change results to different values of forces, distinguished from standard permissible range, acting on line supports. Therefore, new methodologies should be created and applied for design of line supports and computation of forces acting on them.

8. REFERENCES

- [1] Vadhera S. S. "Power system analysis and stability", Khana Publishers Delhi, India, 1987, pp 142-163.
- [2] Bahaidara A. S. "A new algorithm for mechanical design of overhead conductor". Journal for natural and applied sciences, vol.2 No 3 University of Aden, pp 33-40, 1997.
- [3] Coombs R.D., "Pole and Tower Lines for electric power transmissions ". London Hill Publishing CO.Ltd. , 1963, pp 29-42.
- [4] Cotton H., Barber H. "The Transmission and Distribution of electrical energy", The English Universities Press LTD, St Paul's House Warwick Lane London EC4, Third edition, 1970, pp 205-220.
- [5] Nicolai Genkov. "Mechanical part of an overhead transmission lines". Public House "Technics", Sofia, 1974, pp 211-271.
- [6] Nicolai Genkov. "Guidance of an overhead transmission lines". Public House "Technics", Sofia, 1983, pp 150-183.
- [7] Peter Ivanov. "Mechanical part of an overhead transmission lines". Public House "Technics", Sofia, 1985, pp 37-48.
- [8] Design Manual for High Voltage Transmission Lines, REA Bulletin 160-2, USA, Department of Agriculture, Washington DC.,2005 , pp143-180.
- [9] Singh Y., P.K.Bhatia, O. Sangwan. "A review of studies on machine learning Techniques". International Journal of Computer Science and Security, Vol. 1 Issue 1. , 2007, pp 70-84.

A Micro-Mobility Management Scheme for Handover and Roaming

Debabala Swain

*Dept. of Computer Science
CUTM
Bhubaneswar, India*

debabala.swain@rediffmail.com

Siba Prasada Panigrahi

*Dept of EEE
GITA
Bhubaneswar, India*

siba_panigrahy15@rediffmail.com

Prasanta Kumar Patra

*Dept. of Computer Science
CET
Bhubaneswar, India*

hodcomputer@yahoo.co.in

Abstract

Even though the PMIP provides mobility solutions, there are many issues of user identity, mobility context of users from a home network to the visiting network, the assignment of home address to a user terminal in a visiting network, identification of the user terminal's mobility, and identification of MPA and HA. In this paper, we propose a new mechanism with proxy mobile IPv4, as a mobility solution in networks. In this mechanism during mobile node access authentication, MPA exchanges registration messages with the HA (Home Agent) to set up a suitable routing and tunneling for packets from/to the MN. In this method, the authentication request of the mobile node is passed through the NAS or AP of visiting network, this is then passed to the AAA (Authentication Authorization and Accounting) server, and the authentication server checks the realm and does start authentication procedure at the time of initialing authorizing module of the mobile terminal. It also initiates the mobility extension module, where the AAA server initiates MPA of the access network, which also informs the AAA server of the home network with information on the mobility extensions and request of the mobility parameters of the user terminal. The home AAA server interacts with the HA and collects mobile node parameters, as well as sending back details as a reply request to the visiting AAA server. After the mobility context transfer, the MPA conducts a mobility registration to the HA for that particular mobile node. Later in this paper, we will provide sequence of message exchanges during a mobility session of a user mobile node during handover.

Keywords: Handover, Roaming, Mobility Management

1. INTRODUCTION

The mobility management in the access networks is provided by the mobile IP for the seamless continuity of the services during handover and roaming. The demands for accessing services at high data rates while on the move, anyplace and anytime, resulted in numerous research efforts to integrate heterogeneous wireless and mobile networks. However, when the handover happens, the contention-based medium access mechanism which is mainly used in WLAN is invoked and introduces unbounded transmission delay due to idle time periods and retransmission because of collision during the handover. If this technique is expanded to use in a microcellular network such as connected WLAN micro-cells, contention-based mechanism, therefore, should not be used to handle the MT's handover, especially for vehicular users who change access point every few seconds [1]. IP Mobility management protocols are divided into two kinds of category: host-based and network-based mobility protocol. Issues and challenges in

mobility management identified and discussed in [2]. Recently, a unified IP Multimedia Subsystem (IMS) authentication architecture that extends the scope of IMS by allowing it to offer users different IMS-based services even beyond their own domain has been proposed in [3]. But, all these research activities resulted in various heterogeneous architectures where the interworking was performed at different levels in the network. Also, integration at the UMTS radio access level for seamless session continuity proposed in [4]. But, proposed integration is a technology specific solution. However, in this article, we evaluate micro mobility.

The Proxy Mobile IP (PMIP) [5] solution based on Mobile IP approach; handles mobility management inside access networks. Therefore network entities will require more capability than in the standard Mobile IP. The Foreign Agent is no longer capable to handle the mobility management in this new scenario, so we need to enhance its capabilities with the Mobility Proxy mechanism. This new entity called Mobile Proxy Agent replaces Foreign Agent in the visiting network. It also handles mobility registration with the Home Agent. This change is most significant since the Mobile Node now lies outside the mobility registration procedure. In fact, Mobile Node is not aware of its movement, access networks deceives the host to believe that it is stationary in its Home Network. Since the Mobile Node does not need either movement detection or agent registration, the agent advertisements are no longer necessary.

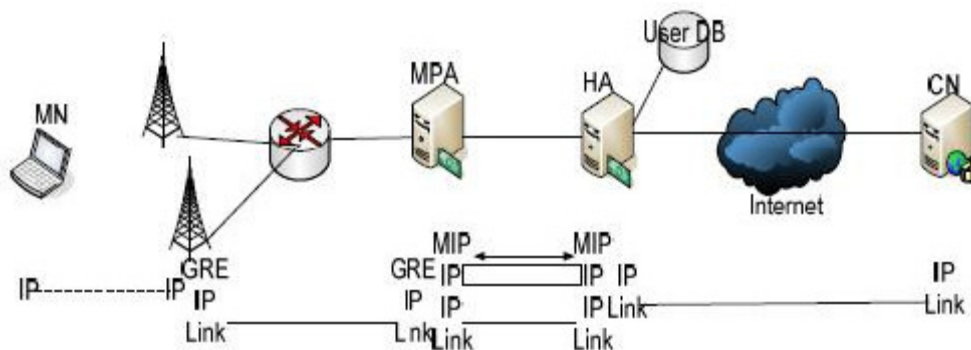


FIGURE 1: Proposed PMIP model

This paper addresses some of the requirements and features to be satisfied for PMIP to provide mobility management:

- Support Unmodified Hosts: As noted above, the protocol supports mobility to nodes that does not have capability of mobility.
- Air link consumption: Mobility-related signaling over the air-link is eliminated. Considering that Network Address Translation (NAT) is ubiquitous in IPv4 networks, a mobile node needs to send keep alive at short intervals to properly maintain NAT states. This can be performed by the MPA in the network which does not consume any air-link bandwidth. The Agent Advertisement is also eliminated in the protocol.
- Support the Heterogeneous Wireless Link Network: One aspect is how to adopt the scheme to an access technology. Since Proxy Mobile IPv4 is based on a heterogeneous mobility protocol, it can be used for any type of access network.
- The other aspect is how to support mobility across different access technologies. As long as the MPA can use the same NAI to identify the MN for various access networks, roaming between them is possible.
- Support the IPv4 and IPv6: As IPv6 increases in popularity, the host will likely be dual stack.

2. PROPOSED SOLUTION FOR PMIP WITH INTEGRATED AAA ARCHITECTURE OF THE 3GPP AND WIRELESS NETWORKS

In this new mechanism, mobility registration of a user terminal is performed by visiting access networks and a home access network. The user terminal does general authentication by visiting

access networks with the help of an EAP (Extensive Authentication Protocol) mechanism. The visiting access networks receive the authentication request from a user terminal through the NAS or AP of the network. The AAA server of visiting network and home networks are modified so that they can communicate with the HA and MPA of their respective networks. New mobility extensions are developed in AAA server to support mobility management, which adds to its present services. These extensions provide mobility context transfer from home access networks, registering the user terminal for mobility at the time of authentication. The visiting network initiates authentication and the mobility extension method whenever it receives a request from the NAS or AP of the access network. During initiation of mobility extensions, the AAA mobility extension process collects data when NAS/AP requests authentication. The AAA mobility process sends mobility user details request to the home network and the AAA server of the terminal, with newly specified attributes of proxy mobile IP. The Home AAA server does receive a request for the mobility user details request as well as the authentication. The home AAA server distinguishes a proxy mobile IP packet from other codes and attributes of the received packet. If the packets need to be a proxy from an intermediate AAA server, then that server adds the proxy attribute to the received packet and sends it to the destination AAA server. If ever the user terminal belongs to the current network, then the AAA server sends a mobility registration request to HA.

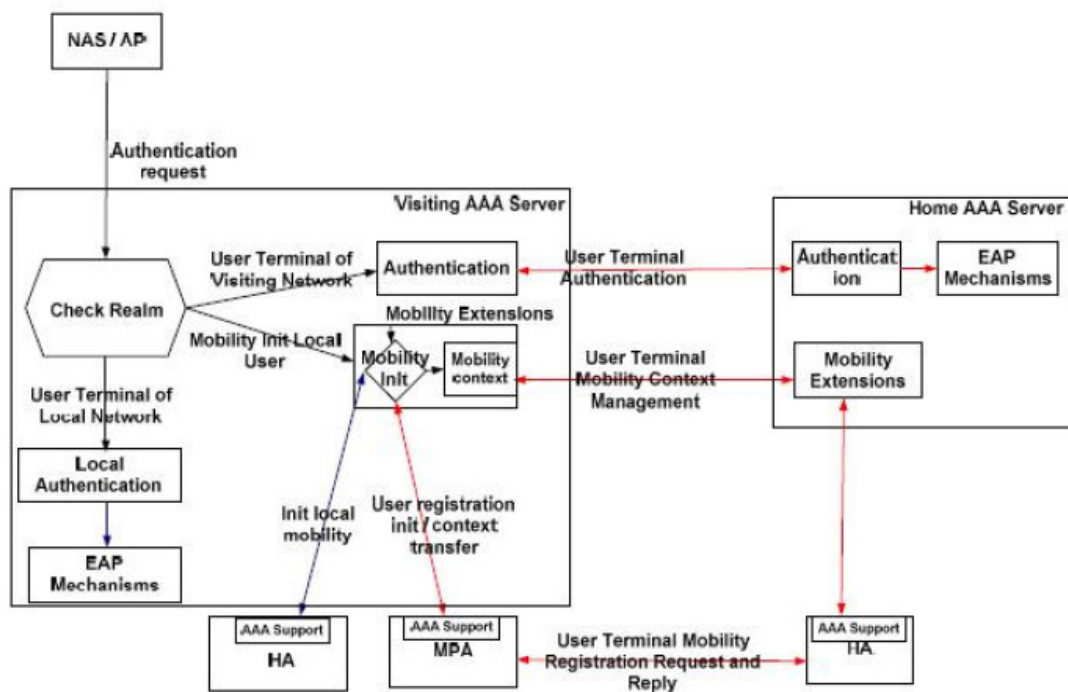


FIGURE 2: Sequence diagram of PMIP Architecture

After receiving the request for mobility user details packet from the visiting AAA server, the home AAA server investigates any information available in the packet and collects user identity from the request packet. After processing the request, the mobility extension method prepares user detail request packet to the HA of the access network. This packet contains details of user id and parameters. The HA receives a request, and with a user ID of request it extract the information of its SID, keys, home address and home agent address from the database of the HA. The HA then sends back a reply to the AAA of home network with the above mentioned data. The AAA server receives a reply and processes the information, and sends back a reply message to the visiting AAA server. The visiting AAA server receives a reply from home server and processes it, storing the data of the user in a temporary database. After processing the reply message, the AAA server sends a mobility registration request to the MPA associated with that particular NAS or AP. This

request contains the details about user ID, SPI, keys, home address and home agent address. When the MPA receives the packet it starts the mobility registration of a user with details from the AAA server.

MPA initiates a mobility registration request of a user terminal with HA using details provided by visiting AAA server. Registration involves the user SPI and the shared key mechanisms with the key available from the AAA server to the MPA. After successful registration of the user with the HA, the MPA will modify the DHCP server configuration with the user terminal's details. These modifications contain details of MAC address and home address of the user in the DHCP server. After successful authentication of the user terminal it initiates a DHCP request for an IP address. The AP/NAS of the visiting network forwards the request to the DHCP server. With the MAC address of the user terminal modified, the DHCP server sends a reply to user's terminal with its home address. The user terminal receives the reply and configures the IP address to the home address. Necessary modification has to be done by the visiting network to accommodate the terminal with the ARP, etc. When the user terminal is in its home domain, the HA registers the terminal and sends the modified DHCP request to the DHCP server and acknowledges the home AAA server of successful registration of a user terminal. The Proxy Mobile IP with the AAA server mobility architecture is shown in Figure 1.

2.1 AAA Mobility Extensions for PMIP Integrated Architecture

In this section we describe the detailed architecture of AAA with mobility extensions to provide mobility management during user mobility in different access networks and technology. In this process, the existing AAA architecture is modified to accommodate proxy mobile IP. In general, authentication information of users is passed through the authenticator, and then this information is passed through the NAS or AP of the access networks. An AAA server authenticates the access networks for the AP or NAS initially, and then processes the user authentication request depending on the realm of the user. In this new method, the mobility management of a user can be initiated during the authentication process. In this process, due to parallel operation of authentication and mobility management, the overall latency of a user during the handover and initial access can be reduced.

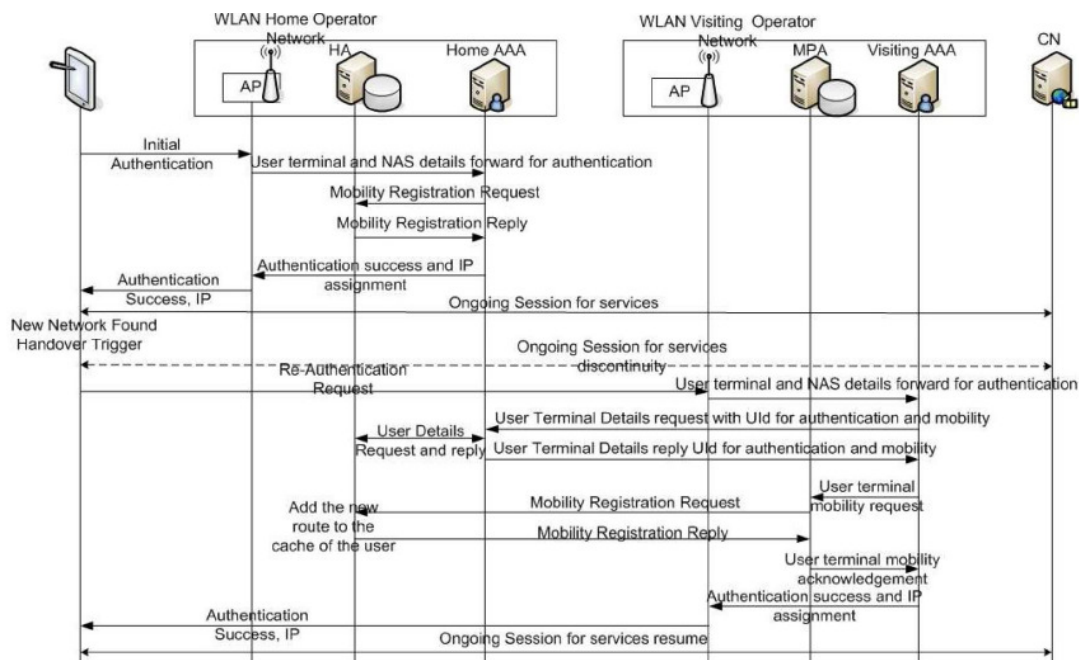


FIGURE 3: AAA mobility extensions sequence Diagram

When there is an authentication request for a user terminal from an NAS or AP, the AAA server initiate authentication module and mobility modules, and processes the user's details by identifying the NAI of the user terminal request. From the NAS or AP request information, such as MAC address of user terminal, NAS details are processed for further procedures. The AAA is modified, with new attributes and codes being added for supporting the PMIP modules. As mentioned previously in the proposed solution section with new extensions, the AAA of the home network can communicate with a visiting network, and can provide mobility context management. With these mobility extensions, the AAA server can communicate with the MPA and HA of the access networks.

On the other side, the visiting AAA server communicates with the home network AAA server, after receiving an authentication request using the mobility extensions, with user information being available from the authentication request from the user's terminal. The visiting server sends a mobility user details request using ID and NAI of the authentication request to the home AAA server. When the home network receives a request packet, the AAA server processes the information of the user from request. It then sends a request to the HA with the new mobility extension, requesting details of the user. After receiving the request packet and processing user details from its internal database, the HA sends back a reply packet with home address, key, SPI and home agent address to the home AAA server. The home AAA server sends back a reply to the visiting AAA server with user details as the reply. After receiving this reply from the home AAA server, the visiting AAA server processes the information of the user and sends a request for mobility registration request with new attributes to the MPA. The MPA receives the user terminal data, sent by the visiting AAA server, and temporarily stores it in a local database. The MPA, with available user information, starts registering with the HA. After registration request and reply message exchange with HA, the MPA sends reply of success or the failure of mobility registration of user to visiting AAA server. Figure 2 describes the AAA mobility architecture.

2.2 PMIP Operation With New Mobility Extensions in MPA and HA

MPA exchanges registration messages with the HA to set up a proper routing and tunneling packets from/to MN. The MN broadcasts messages containing an MN's Network Access Identifier (NAI) to request authentication/authorization, and the AP transfers the request to the local AAA server (visiting AAA). If the MN is away from home, it is clear that the MN is out of the local authentication database.

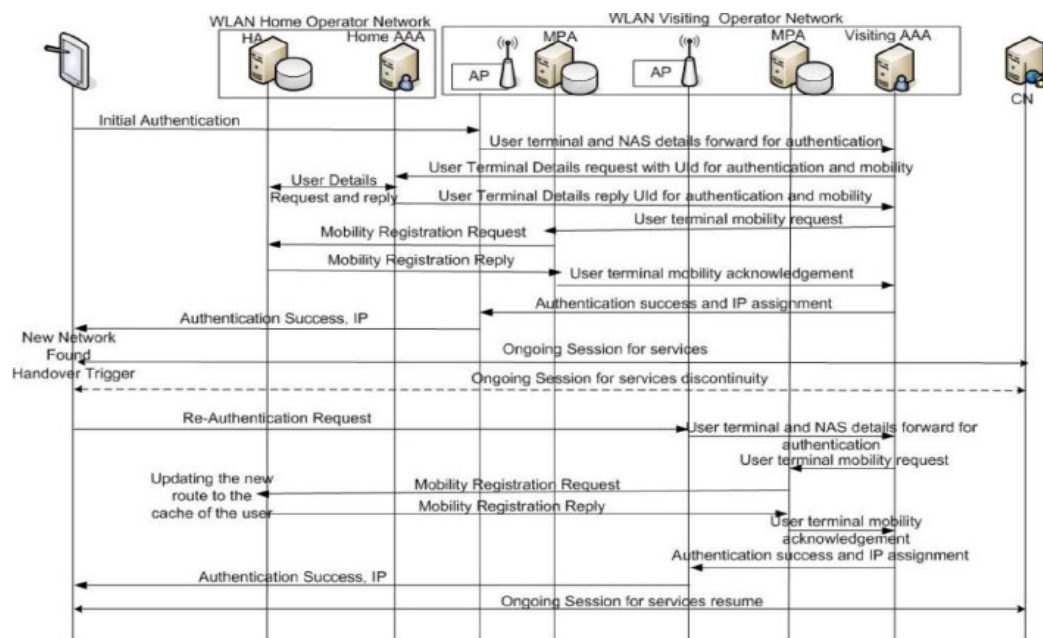


Figure 4

Mobility extensions using MPA and HA

However, the local AAA server can use the NAI to identify the MN's Home Network, and then the authentication/authorization, along with mobility user details, will request a message to be transferred by the visiting AAA to the home AAA Server (AAA_H) in the Home Network.

Along with the authenticating validation, the AAA_H searches for information of the MN stored in the HA, containing MN's HA, NAI, and SPI. If the MN is back to its Home Network, then the local AAA server sends a message to the HA to deregister the MN instead of searching for the data. The MN's information will be transferred to the visiting AAA, which will deliver it to the MPA with the AP's MAC address included. Triggered by the AAA server, the MPA exchanges messages with the HA to demand Mobility Registration and Tunneling.

After successful registration, the MPA sends a message to inform the DHCP server about the MN's arrival. It forces the DHCP server to update the configuration file with the Mobile Node information. Finally, the MPA informs the AAA visiting about the successful registration. The Authentication Accept message is sent to the NAS, granting network access to the MN. After authentication success, the MN sends a Binding DHCPDISCOVER to request the IP address. This message is formatted as described by the DHCP protocol (the CIADDR field is filled with the MN's IP). By searching for information of the Mobile Node, in the configuration, the DHCP server replies with a DHCPOFFER message in which the YIADDR field is filled with the MN's Home Address and the default gateway address, being the MPA's. Next, the MN and DHCP server exchange the DHCPREQUEST and DHCPREPLY to complete this procedure. The MN is then ready to connect to the network with its Home Address.

3 MICRO MOBILITY

In this scenario mobility is performed in same administrative domain and same access technology, we have observed two sub scenarios where the proposed architecture addresses this issue.

3.1 User Terminal Mobility in Home Administrative Domain on Same Access Technology

In this scenario access network has multiple APs, and user terminal moves from one AP to another AP. During initial authentication of user, AAA server does authenticate user and assists HA for mobility registration of user terminal. When user terminal senses other APs of access network and triggers the handover with re-authentication procedure, upon receiving request from new AP, the AAA server sends a mobility registration request to MPA associated with AP. MPA and HA does the mobility registration of the user terminal and sends acknowledgement to AAA server. Upon successfully authentication and registering terminal in HA, it provides access and home IP address of user terminal to AP for providing access to user terminal. The message exchange is shown in Figure 3.

3.2 User Terminal Mobility in Visiting Administrative Domain on Same Access Technology

In this scenario a user terminal moves on same interface from one AP to another in visiting operator network. The user terminal is authenticated and registered in HA with the help of home AAA and visiting AAA servers. When user terminal identifies new AP it triggers the handover and does re-authentication procedures. Upon receiving request from new AP visiting AAA identifies user from previous registration and sends mobility registration request to new MPA with previous details. MPA does register the user terminal with HA and sends acknowledgement to visiting AAA server to complete handover procedure, the whole procedure is shown in message sequence in Figure 4.

3.3 Enhancing the Proposed Solution Using Network Selection Procedure for Seamless Mobility.

To enhance proposed architecture we used network selection procedures combined with this architecture to use context management between the networks. Using this process access networks can create mobility context even before user terminal does initiate access to visiting network. In this process user terminal can communicate with home network using present connected network and negotiate best suitable network to connect during handover. After selecting best suitable network with the assistance of terminal, home network initiate context transfer and creating mobility context with the future visiting network.

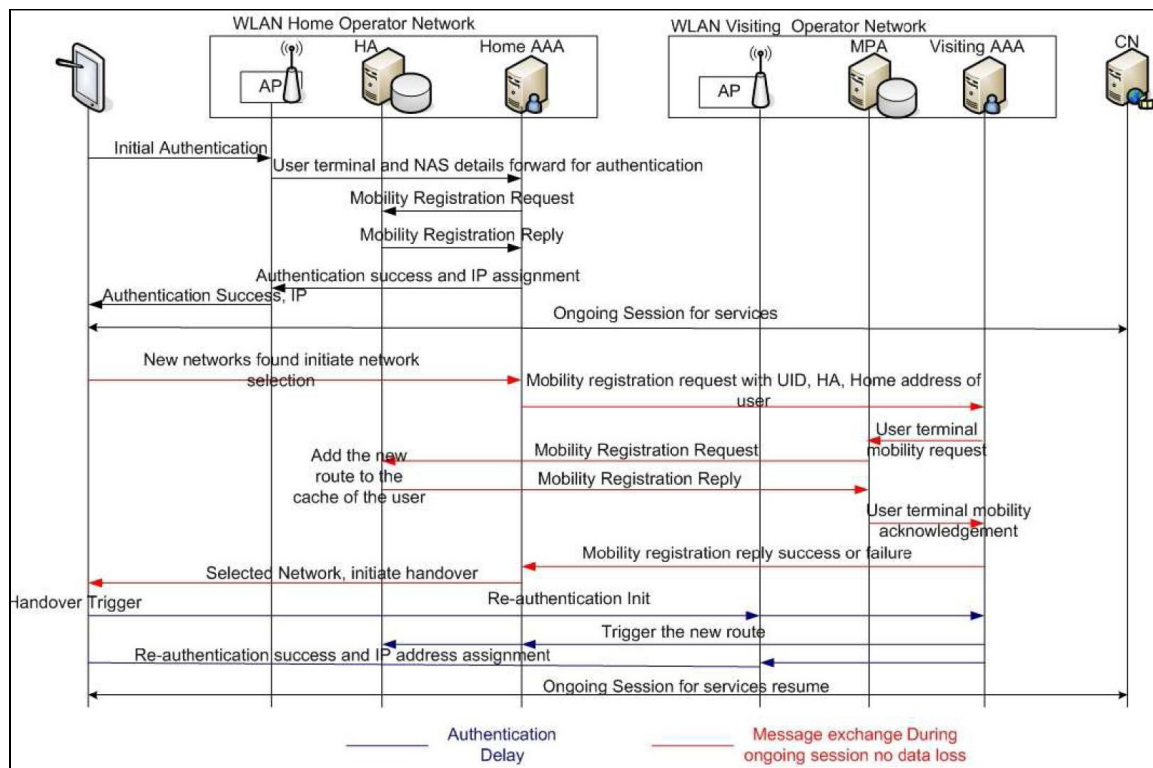


FIGURE 5: Mobility management using Micro mobility model

Using AAA mobility extensions proposed in this architecture AAA of home network sends a mobility registration request to visiting AAA server with UID of the terminal and mobility context details in the request. After receiving request from home AAA server, visiting AAA server collects data and sends a registration request to MPA of visiting network. After receiving request for mobility registration MPA collects user details and initiates registration request to HA of home access network. After successful registration user details of new route are cached in HA and MPA and a tunnel is established between them. When user or home AAA server does the handover triggering, HA does update route upon receiving the RU (route update) request from home AAA server. In this way maintaining multiple tunnels with future visiting networks of user and triggering with the help of home AAA server seamless mobility is achieved.

The whole message exchange sequence diagram is shown in Figure 5. During implementation of this procedure in a test bed we observed zero latency for multi homing handover and for horizontal handover we obtained small latency delay due to re-authentication procedure.

4 NEW PMIP AND AAA MOBILITY EXTENSION DEVELOPMENT AND TEST-BED SETUP

4.1 PMIP and AAA Software Architecture

To implement proposed architecture we developed AAA server and PMIP in house using existing open source software. We have developed software architecture to implement mobility extensions for AAA server. In this architecture AAA server can receive a request from NAS or from another AAA server. From NAS it can receive authentication request and from AAA server it can receive mobility user detail request. Upon receiving mobility registration request, extensions model respond with the reply of user details. Software architecture of AAA as shown in Figure 6, the AAA server can send requests and reply accordingly to incoming requests with the different components. For implementing the PMIP we used dynamics mobile IP architecture and modified to our requirements. We converted FA to an MPA, modified HA and MPA to accept any requests from AAA server and sending reply accordingly. In this architecture MPA can perform registration requests to HA upon request from AAA server and sends acknowledgement as success or failure. New packet formats and codes are added in MPA and HA to implement the proposed architecture.

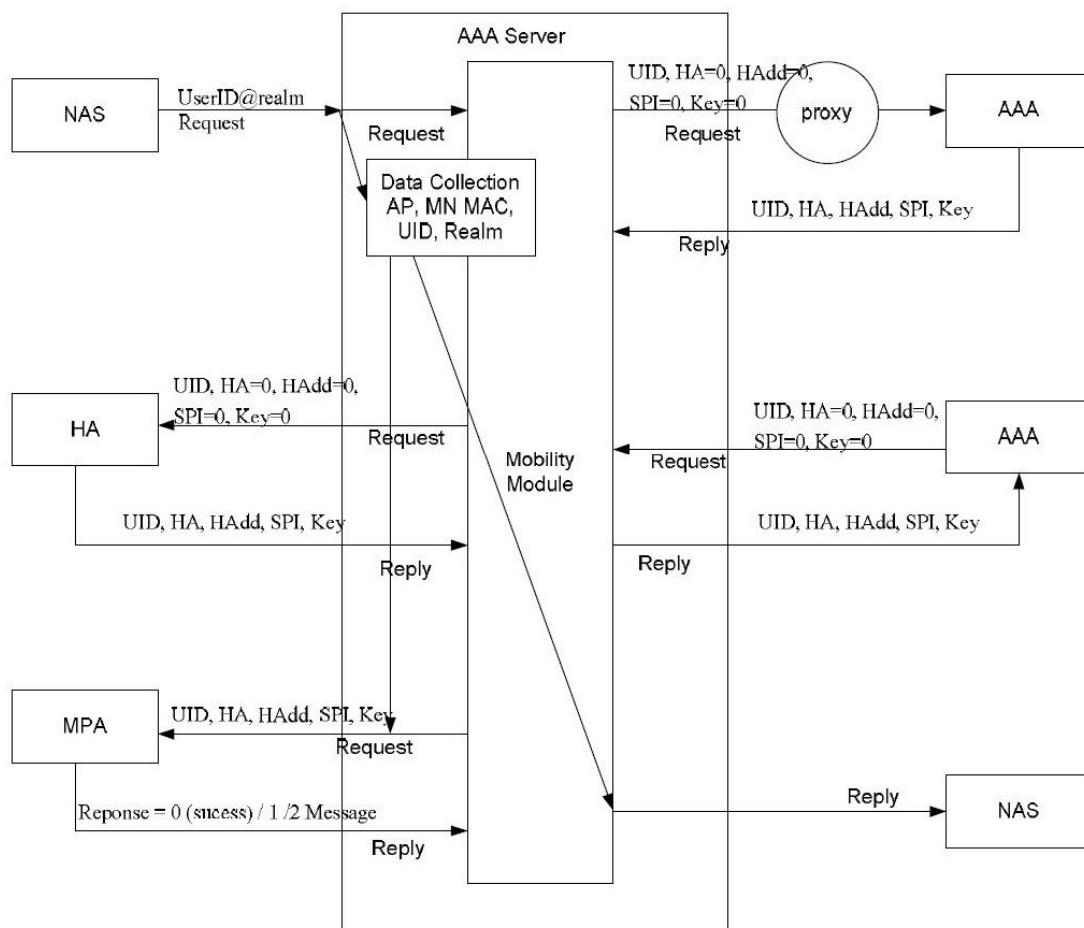


FIGURE 6: Software Architecture for PMIP Architecture

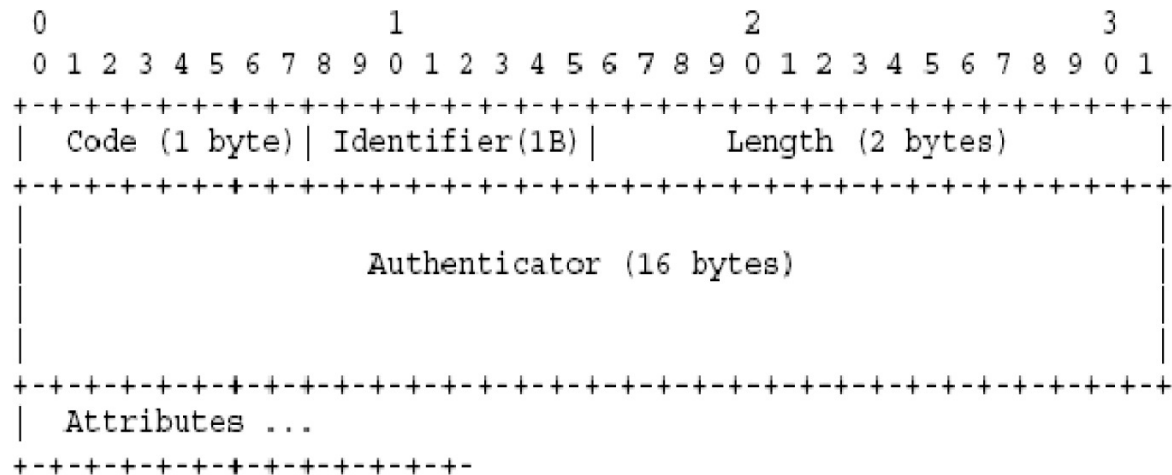
4.2 AAA Mobility Extension and PMIP Packet Formats

We have developed new AAA mobility extensions and new codes and packet formats for developing and demonstrating the capabilities of new mechanisms proposed in this architecture. The AAA server builds Mobility User Detail Request message from Access Request or EAP

Request from the NAS or AP. Remark that intermediate AAA servers just pass through this step, adding Proxy Attribute and forwarding the Request.

4.2.1 AAA Mobility User Detail Request Format:

Note: the codes and the attributes in this document are taken as reference these can be changed according to the IANA consideration; in this case we used available values for developing the prototype, we can change these values if there are any issues.



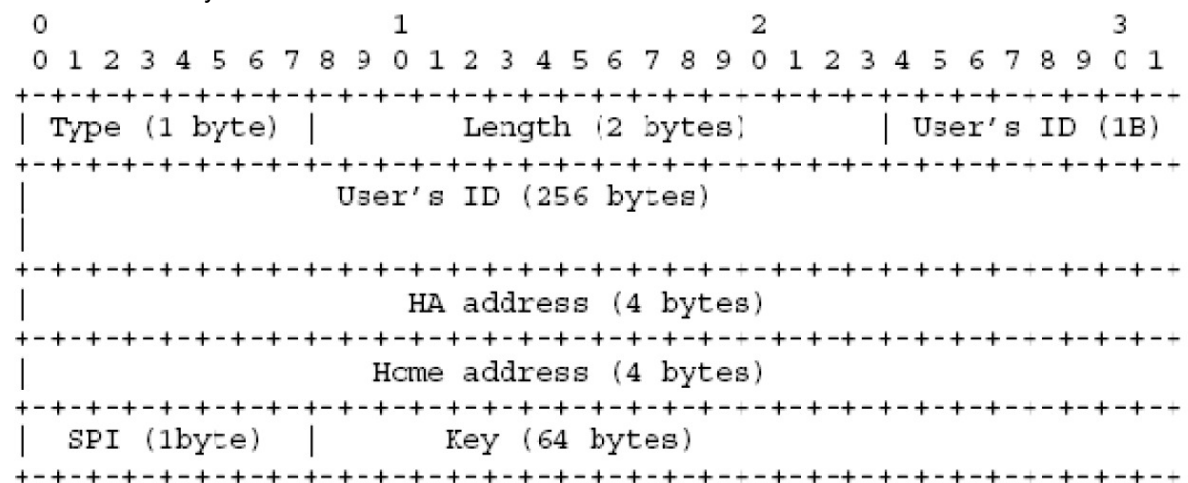
Code: (1 byte) Mobility_User_Detail_Request = 60.

Identifier: (1 byte) number to match the Request/Reply.

Length: (2 bytes) length of the message, including Code, Identifier, Length, Authenticator, Attributes. In the case that there is only mobility attribute, length = 350.

Authenticator: The Authenticator field is 16 bytes. The most significant octet is transmitted first. This value is used to authenticate the reply from the RADIUS server, and is used in the password hiding algorithm.

Attributes: Mobility Attribute:



Type = (1 byte) Mobility_Request_Attribute = 193.

Length (2 bytes) = Length of the message = 332.

User's ID: (256 bytes) extracted from the name of the user (ex: userID@realm).

HA address: (4 bytes) Home Agent's IP address, filled with Zeros.

Home Address: (4 bytes) Mobile Node's Home Address, filled with Zeros.

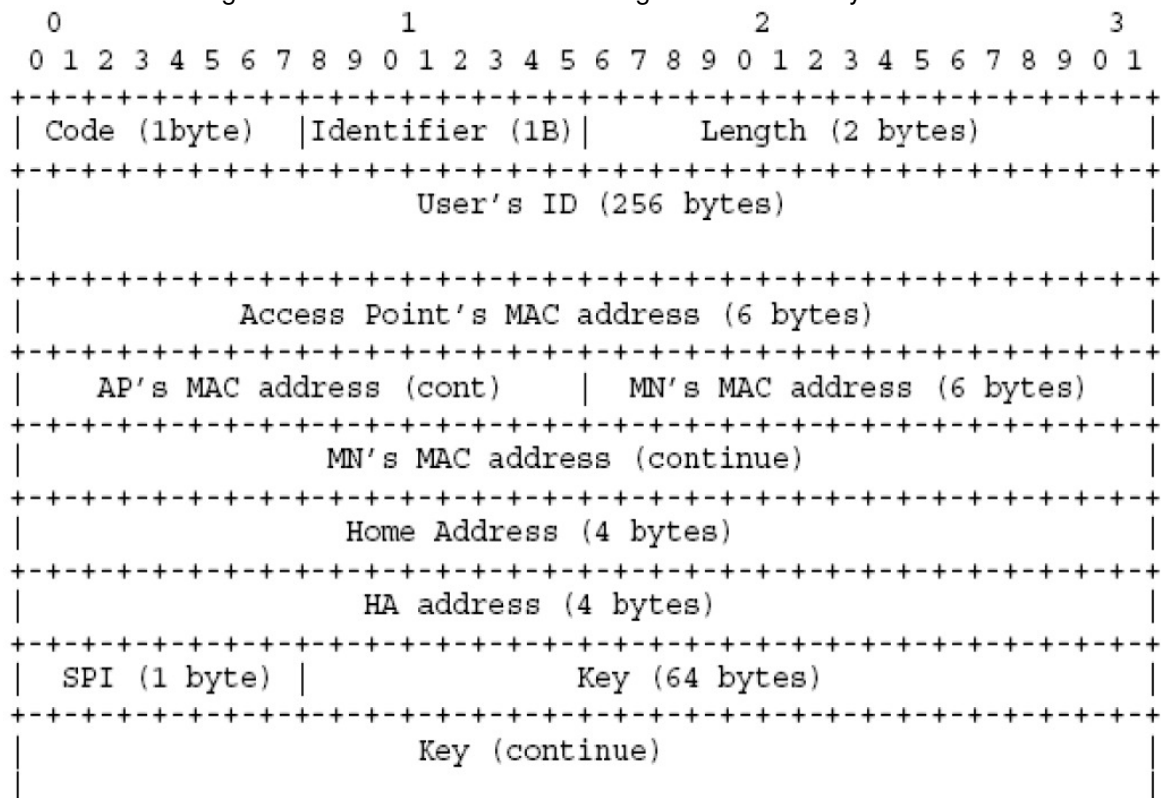
SPI: 1 byte, filled with Zeros.

Key: (64 bytes) public key of the HA, filled with Zeros.
The AAAH will reply with a Mobility Response.

HA/MPA Consultation

If AAA home server receives Mobility user detail request from a visiting server, the AAAH sends message to HA to fill the information required in the Mobility Request Attribute (fields that are filled with Zeros). Remark that the AAAH sends the HA Consultation message only by being triggered by the Mobility user detail Request; the Access Request forces the AAAH to deregister the MN.

H1: Create a message from AAAH to the HA demanding for the necessary information:



Code (1 byte) = HA_Consultation_Request = 63.

Identifier: (1 byte) number to match Request/Response.

Length (2 bytes) = total length of the message = 343

AP and MN's MAC address: These fields are practically used in the message from AAA to MPA. In the message from AAA to HA, these fields are filled with Zeros, and the HA just ignores it. But these fields SHOULD appear in the HA Consultation Message to identify the format of messages AAA-HA and AAA-MPA. It is very useful since the HA and MPA in the same network are usually installed in the same server. This identification simplifies the treatment of message in the HA/MPA server.

Other fields are copied from the Mobility Attribute of the authentication request.

H2: HA looks for the required information in its database, save the AP and MAC address fields. If the information can't be found (this may be due to the modification of the administrator), HA will pass this phase, so that the message will be left Zeros. That allows the AAAH to detect the failure.

H3: HA sends back the reply to the AAA after filling the request's required fields and setting Code = HA_Consultation_Response = 64.

H4: The AAAH replies the visiting AAA with a Mobility user detail Response, which is either an Accept or Reject message. The format of these messages is as same as the request, with different code and attributes.

If the message from HA is not filled with Zeros (successful verification), the AAAH reply to the AAAF with Mobility Accept message which is copied from the Mobility Request whose the Attributes filled by the data retrieved from HA. The Code field for this message is: Code = Mobility_Accept = 61.

If the data from HA is filled with Zeros, the AAAH MUST reply the visiting AAA with a Mobility user detail Reject message, with Code = Mobility user Reject = 62. The Mobility Reject message doesn't contain the Mobility_Attribute, and may include Reply-Message Attribute which contains the error message shown to the user [6]:

[illegible]

Type: 18 for Reply-Message.

Length: length of the attribute, including Type and Length field.

Text: The Text field is one or more octets, and its contents are implementation dependent. It is intended to be human readable, and MUST NOT affect operation of the protocol. If the registration failed, this field is filled with the message extracted from the MPA Mobility Registration Reply.

Mobility Registration

After receiving the Mobility Accept message, the visiting AAA makes MPA handle the Mobility Registration procedure. The MPA exchanges messages with HA and DHCP server, then informs visiting AAA about the result (success or failure). The Mobility registration Reject causes the AAAF to send the Reject message to the NAS and terminate the whole procedure.

MR1: Visiting AAA sends a MPA Mobility Registration Request message to MPA: the format is as same as HA Consultation message:

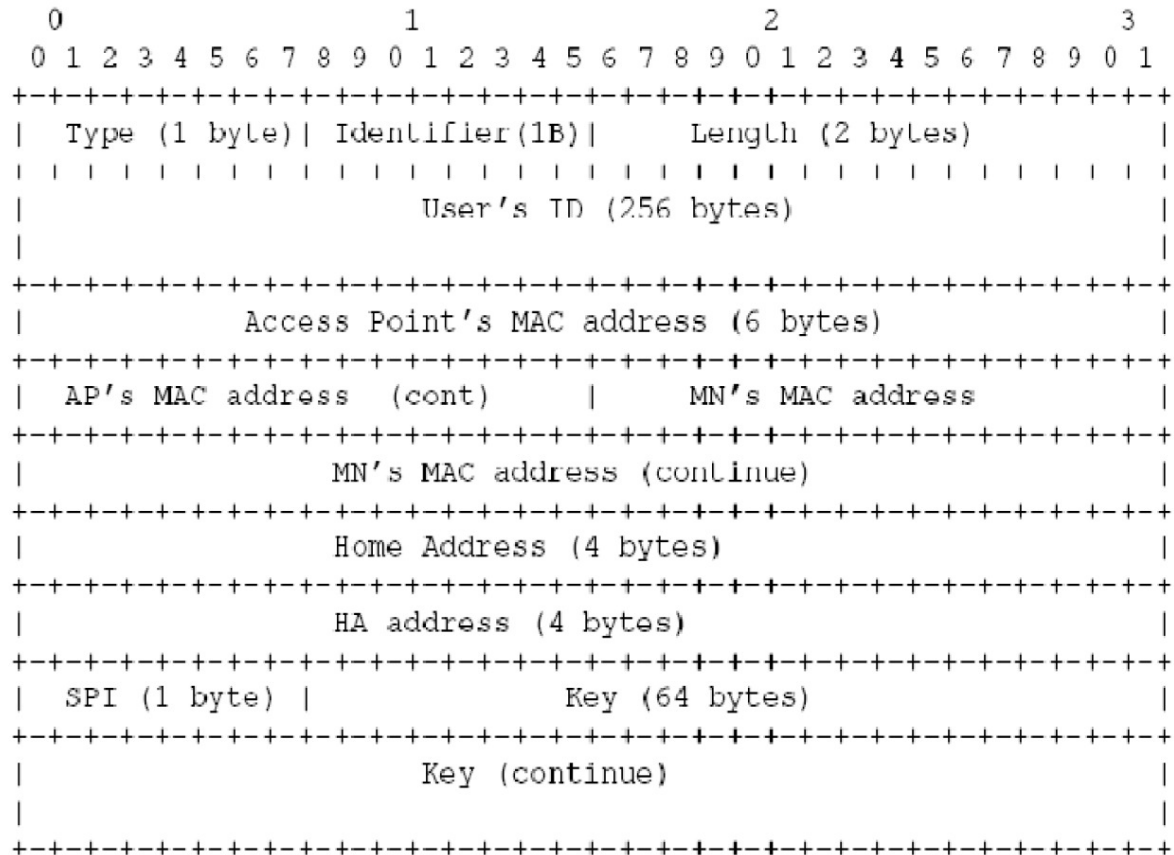
Type (1 byte) = MPA Mobility Registration Request = 65.

Identifier: (1 byte) number to match Request/Response.

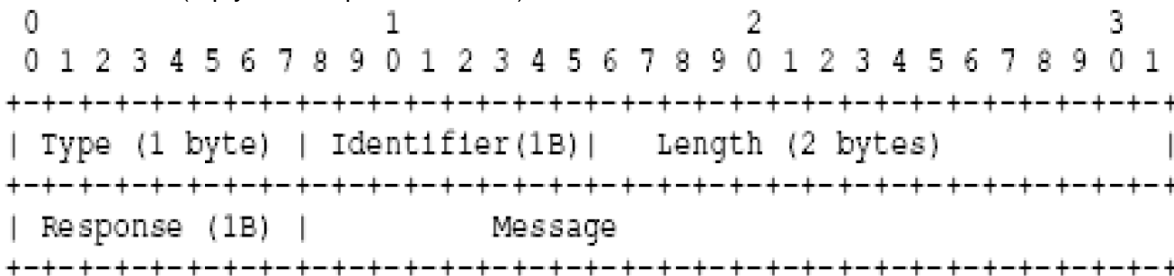
Length (2 bytes) = total length of the message = 343.

Other fields save AP and MN's MAC address are copied from the Mobility Attributes of the Registration Response.

MR6: MPA Mobility Registration Reply to visiting AAA:



The MPA sends back the reply to the AAA after successful communication with the DHCP server, or if it detects any error (registration unsuccessful, DHCP server refusal to register the Mobile Node, or requests cannot reach the destination). In this latter the MPA sends a reject message to the AAA server (reply with response = 1 or 2).



Type = MPA_Mobility_Registration_Reply = 66

Response = 0 if successful, = 1 if unsuccessful with message, = 2 if unsuccessful without message.

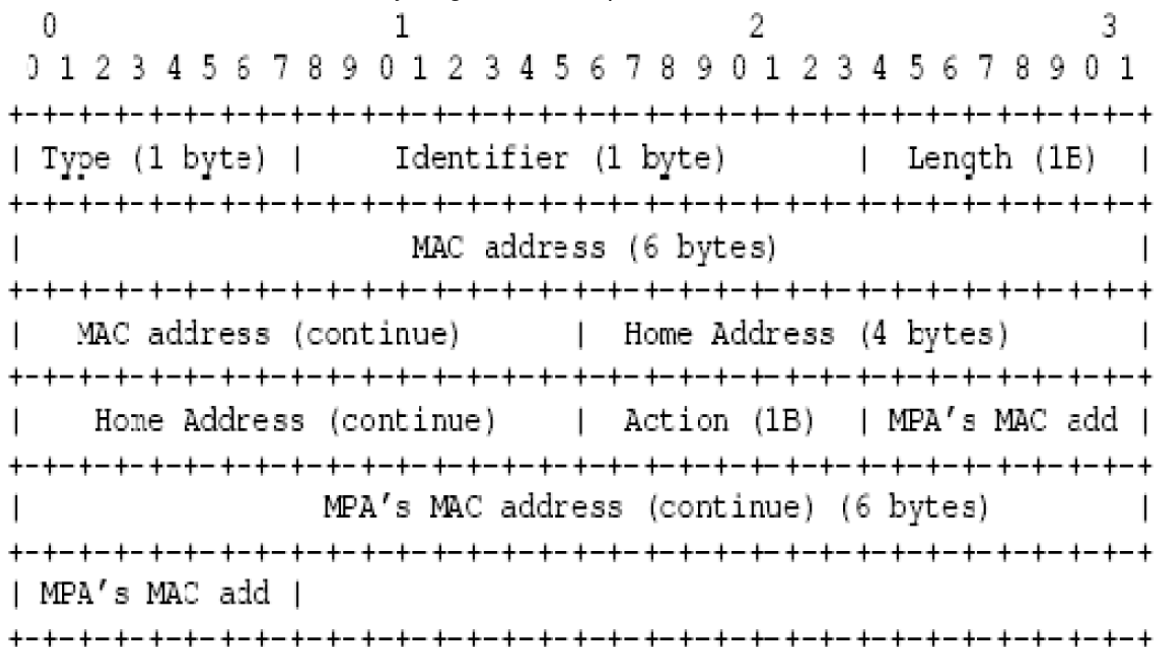
In the unsuccessful case (Response != 0), AAA will send an Access_Reject message to the NAS. Otherwise, if the Response Code = 1, the text in the Message field can be used in the Reply-Message Attribute in the Mobility Registration Reject message.

MR2: Registration

For the convenience of use of Client Mobile (Mobile IPv4) and Proxy Mobile IP simultaneously, the MPA and HA should use the Mobility Registration Request as specified as in RFC3344.

HA reply with Mobility Registration Reply, formatted as specified in RFC3344.

MR4: MPA sends DHCP Mobility Registration Request to DHCP server:



Type = DHCP_Mobility_Registration = 67

Identifier: match Request/Response

Length = 21: length of the message, including the Type and Identifier fields

MAC address: MN's MAC address

Home Address = MN's Home Address.

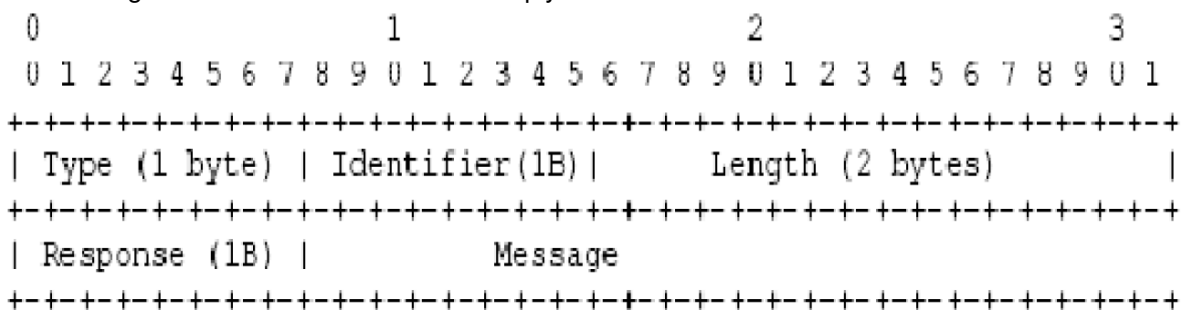
Action: (1 byte) = 0 - binding update: the DHCP server updates its configuration file with the MN's new entry:

MN's MAC address --- MN's IP address --- Default Gateway = MPA's MAC address

If Action = 1 - remove entry: cause the DHCP server to remove the MN's entry in its configuration file. This action is used in the Registration Revocation Procedure. As receiving the message from the MPA, the DHCP server updates its configuration with the information supplied by the MPA. Since then, as soon as the DHCP server receives the (Binding) DHCPDISCOVER message from the MN, it will exchange the messages with the MN granting the MN keep its Home Address; also indicates the MPA as MN's default gateway.

MR5: DHCP Mobility Registration Reply to MPA

The message is formatted as same as the reply from MPA to AAA



Type = DHCP_Mobility_Registration_Reply = 68

Length = length of the message including the Type and Identifier fields

Response Code = 0: accept, = 1 reject with message, = 2 reject without message.

If the response Code is other than 0, the MPA MUST response with the AAA with MPA Mobility Registration Reply whose Response and Message fields copied from DHCP Mobility Registration Reply message.

Message: this message will be used in the response from MPA to AAA.

4.3 Test bed Setup

This section describes testbed setup for implementing solutions proposed in this architecture. As mentioned earlier we have developed mobility extensions for AAA server using Freeradius [7], and PMIP using parts of Dynamics mobile IP [8] with our implementation. The proposed testbed composed of 3GPP, WLAN and WIMAX Networks. We used Infinet's preWIMAX equipment, operating at the frequency of 5.4 GHZ for WIMAX network, WLAN access consists of Linksys WRT54 and Cisco AirNet AP350. The 3GPP network used in this case is EDGE network operated by the French network operator Bouyges Telecom courtesy of MVNO Transatel. The user terminal used in the testbed is DELL Latitude410 using Centrino for wireless with option GT 7.2 ready MAX data card for 3GPP access. Most of our testing for different scenario we have used WIMAX and WLAN due to complexity of EDGE network as we have limited control of the production network provided by MVNO Transatel for us. To validate the solution we used basic testing like vertical handover where the client is equipped with multiple interfaces to validate the solution for multi homing scenarios. As we mentioned earlier horizontal handover is limited for EDGE in our case because of the control of the access network.

The implemented scenario is shown in Figure 7. We have deployed a VPN with cellular network where authentication and data is routed through the cellular network to local testbed. The user terminal is configured with AT commands using PAP for authentication. When user terminal dials for connection, authentication information of user terminal is routed through GGSN to the local authentication in the test bed, the modified AAA server does the authentication and assigns the address using IP pool mechanism, and in parallel mobility context is created for MPA and HA using AAA server.

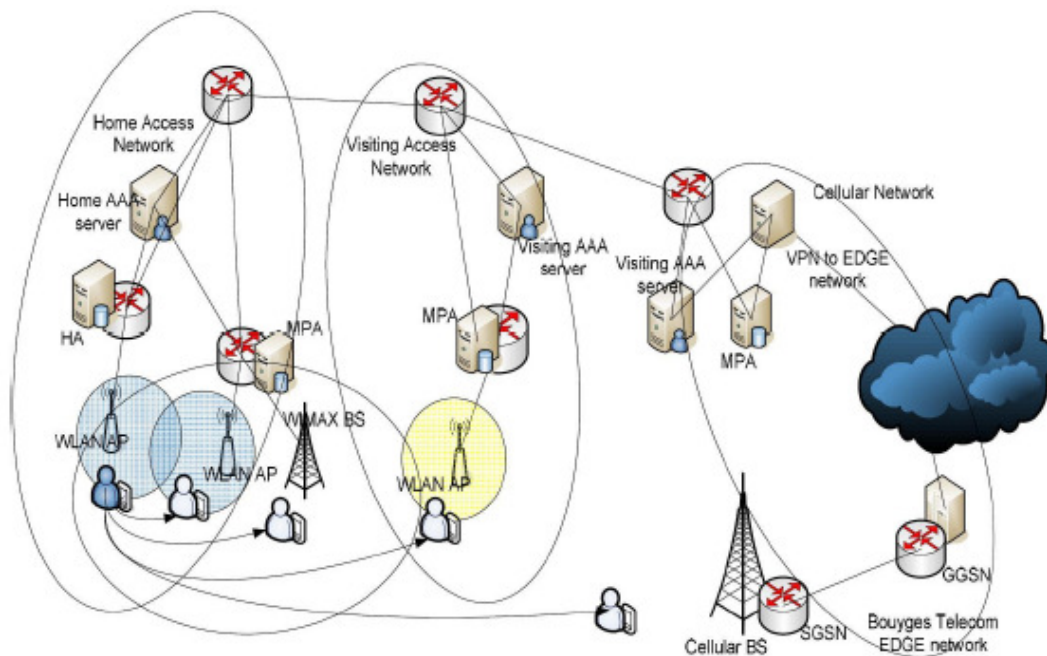


FIGURE 7: Test-Bed set up for proposed model

We have deployed EAP authentication mechanism for authentication in WLAN and WIMAX networks. A user terminal tries to connect access networks using WPA supplicant [9], it is configured with user id with NAI and security mechanisms essential for EAP TLS mechanisms. Once the authentication is initiated in access networks, APs and BS sends authentication request to AAA servers, and AAA initiates authentication and mobility context for user terminal. A GUI is developed on terminal to maintain interfaces and control access management along different access networks.

5 RESULTS

As mentioned in architecture the AAA server does authentication and mobility in parallel when there is a request from the user terminal in test-bed. Using this test-bed we have achieved mobility of user with low latency and seamless mobility in some scenarios. Multi homing, horizontal handover and roaming is performed efficiently using this mechanism. Various scenarios of mobility have been tested using this test-bed. Deployment and extending to the new access networks and operator is very efficient as the modifications are made at network side without any client conscious. The modifications on the network side can be made with additional patches with existing deployments. For testing purposes we have used experimental codes and attribute value pairs these can be extended to the vendor specific or using IANA status can be standardized.

We have observed an overall latency of the user terminal involved during roaming from one network to another on the same technology is around 2.4 sec for WLAN, 3.6 seconds for WIMAX, and 16 seconds for 3G networks, due to re-authentication and mobility management. In 3G networks we have observed high latency due to delay of routing messages from bouyges telecom network to our test bed. For multi homing scenario we observed latency of 18 milliseconds as we have implemented multiple interface scenarios, where a user terminal connects to multiple networks and the management of the mobility is performed by triggering route update message in HA of the user terminal. In the next paragraph we have attached a log of our radius servers in home and visiting networks where the whole procedure is depicted. For more details about logs, ethereal results refer to [10].

5.1 Comparison With Existing Mobility Models

In this section different mobility protocols are compared with the available results and support for access networks with experimental results and simulation results. As we mentioned in last section we have built test bed to perform mobility in different interworking scenarios of mobility using mobility protocols. We take the following result of CMIP, HMIP and PMIP from the test bed and the result of HAWAII and Cellular IP from other sources [11]. The Table 1 shows the different performance results for mobility protocols.

In the test for CMIP and HMIP, we take the result from mobility registration procedure only. Macro-mobility handoff time is counted from moment that MN starts to the end of the handoff; and micro-mobility handoff time is counted from the moment that we switch network connection (changing access point). In fact, using manual switch is little different from real time test in which the MN starts handoff if it moves out of the first access point's cover, since in the later case's handoff time depends largely on network scanning and selecting software used in the MN. We can observe that the CMIP has very high macro-mobility latency, which dues to Agent Discovery phase. We admit that the test bed is so simple as compared to the architecture implemented HAWAII and Cellular IP that the different networks are adjacent, and therefore cannot have a proper comparison among these protocols. The test is purely on latency issue, we don't count on packet loss and robustness. However, the result is persuading enough to prove the advantage of PMIP.

Proxy Mobile IP is advantageous over other mobility protocols over security, since the information is exchanged among the network entities with authenticated mechanism. More precisely, the advantage of PMIP over other protocols comes from the fact that the information exchanged in

registration procedure can be generated for each session, i.e., HA can generate necessary information used for each registration session. Hence, outside AAA authentication, no key is actually stored for mobility registration.

The proposed mechanism for mobility management in this paper is compatible and interoperable with the existing converging networks. We have studied different interworking methods to implement our solution for completing the seamless converging puzzle at the mobility management layer. We interrogated different interworking mechanisms such as Seamless Converged Communications Across Networks (SCCAN), Unlicensed Mobile Access (UMA), Interworking- Wireless LAN (I-WLAN), Media Independent Handover (MIH) IEEE 802.21. The proposed solution can be adapted in these mechanisms to provide seamless services at the mobility layer.

Protocols	Support for Micro mobility	Handover latency Micro mobility	Access Networks Support	Security	Legend
CMIP	--	Non	WLAN/WIMAX	+	++Strong advantage +Advantage -Drawback --Strong drawback *not include network selection and Authentication **include authentication and manual network selection latency ***include re-authentication
HMIP	++	138ms*	WLAN/WIMAX	-	
HAWAII	++	150ms*	WLAN/WIMAX	-	
Cellular IP	+	300ms*	WLAN/WIMAX/ Cellular Mobile Network	+	
PMIP	++	70ms***	WLAN/WIMAX/ Cellular Mobile Network	++	

TABLE 1: Comparison of mobility protocols with PMIP

5.2 Issues of IPv6 Migrations

Due to low IP address space available for ever increasing terminals there is a need of IPv6 in the near future to deliver the services. NETLMM is an IETF working group working in PMIPv6 [12, 13], Specification of PMIPv6 is still in the infancy stage, there are several issues which has to be addressed to obtain the mobility solution. Issues of Mobile IPv6 and PMIPv6 interactions, AAA support for PMIP, MPA discovery in the access networks, handover and route optimizations, Path Management and Failure Detection, Inter access handover support and multi homing scenario handover are still open in the WG. Using AAA mobility extensions and PMIPv6 supporting AAA extensions as proposed in the architecture, issues mentioned above are solved. As part of our future work we are developing dual stack PMIPv4 and PMIPv6 for mobility support in heterogeneous networks.

6 CONCLUSION

Post handover techniques are intended to reduce latency during roaming and handover in heterogeneous networks. As a part of this we have proposed security authentication and mobility management to optimize handover and roaming. Extending existing infrastructure such as AAA in this case is more efficient than proposing new protocols and infrastructure. As a part of it security and mobility extensions are proposed. Using the security mechanisms we estimated the latency obtained in this method is far less than any conventional methods available in the literature. The authentication keying material created dynamically, by this way the theft presentational and security vulnerabilities are reduced. The mechanisms presented are applicable to WLAN, WIMAX and cellular networks and utilizing with RII architecture the solution provides the flexibility to operate in any interworking scenarios of roaming and handover.

Proxy Mobile IP is a development of Mobile IP, where the registration is processed by the network entities. Hence, the Mobile Node does not require a Mobile IP stack to roam over the network without losing its IP address, so this can be applied to unchanged devices. Using this proposed mechanism, authentication and mobility management of users during the access is

performed in parallel; in this way, latency during the authentication and re-authentication is reduced. In this mechanism, using context management the control of users can be maintained according to the access networks. Fast and seamless handover is achieved in various deployment and mobility scenarios using these mechanisms. Extending and upgrading existing networks can be performed efficiently, as no new hardware is added to the existing architectures. Multi homing scenarios, different interworking architectures of WLAN, WIMAX and 3G are addressed using the proposed mechanisms.

7 REFERENCES

- [1] Thanh Hoa Phan, Gaute Lambertsen, Takahiko Yamada, Seamless handover supported by parallel polling and dynamic multicast group in connected WLAN micro-cells system, *Computer Communications, Volume 35, Issue 1, 1 January 2012, Pages 89-99.*
- [2] Ibrahim Al-Surmi, Mohamed Othman, Borhanuddin Mohd Ali, Mobility management for IP-based next generation mobile networks: Review, challenge and perspective, *Journal of Network and Computer Applications, Volume 35, Issue 1, January 2012, Pages 295-315.*
- [3] Salekul Islam, Jean-Charles Grégoire, Multi-domain authentication for IMS services, *Computer Networks, Volume 55, Issue 12, 25 August 2011, Pages 2689-2704.*
- [4] Natasa Vulic, Sonia M. Heemstra de Groot, Ignas G.M.M. Niemegeers, Vertical handovers among different wireless technologies in a UMTS radio access-based integrated architecture, *Computer Networks, Volume 55, Issue 7, 16 May 2011, Pages 1533-1548.*
- [5] Leung K., Dommety G., Yegani P, Chowdhury K, "Mobility Management using Proxy Mobile IPv4," IETF RFC, January 2007.
- [6] Adoba. B, "IANA Considerations for RADIUS," IETF RFC 2869, July 2003.
- [7] Freeradius. [Online]. <http://freeradius.org/>
- [8] Dynamics mobile IP. [Online]. <http://dynamics.sourceforge.net/>
- [9] S. Parkvall, "Long-term 3G Evolution – Radio Access," Ericsson Research Report.
- [10] Detailed results and logs of testbed implementations. [Online]. <http://193.54.225.196/pmip>
- [11] Vollero. L and Cacace. F, "Managing mobility and adaptation in upcoming 802.21 enabled devices," in *4th international workshop on wireless mobile applications and services on WLAN hotspots*, Los Angeles, CA, USA, September 2006.
- [12] Arikko. J and e. al, "Mobility Support in IPv6," IETF RFC 3775, May 2003.
- [13] Network-based Localized Mobility Management. [Online]. <http://www.ietf.org/html.charters/netlmm-charter.html>

Audio Steganography Coding Using the Discrete Wavelet Transforms

Siwar Rekik

*Faculty of Engineering
Université de Bretagne Occidentale
Brest, 29200, France*

Siwar.Rekik@etudiant.univ-brest.fr

Driss Guerchi

*Faculty of Engineering
Canadian University of Dubai
Dubai, 117781, UAE*

Driss@cuad.ac.ae

Habib Hamam

*Faculty of Engineering
University of Moncton
Moncton, E1A 3E9, Canada*

habib.hamam@umoncton.ca

Sid-Ahmed Selouani

*Faculty of Engineering
Université de Moncton
Shippagan, E8S 1P6, Canada*

sid-ahmed.selouani@umcs.ca

Abstract

The performance of audio steganography compression system using discrete wavelet transform (DWT) is investigated. Audio steganography coding is the technology of transforming stego-speech into efficiently encoded version that can be decoded in the receiver side to produce a close representation of the initial signal (non compressed). Experimental results prove the efficiency of the used compression technique since the compressed stego-speech are perceptually intelligible and indistinguishable from the equivalent initial signal, while being able to recover the initial stego-speech with slight degradation in the quality .

Keywords: Speech Compression, Steganography, Information Hiding, Discrete Wavelet Transform (DWT).

1. INTRODUCTION

One of the concerns in the area of information security is the concept of audio steganography coding. Today's reality is still showing that communication between two parties over long distances has always been subject of interception. Providing secure communication has driven researchers to develop several cryptographic and steganographic schemes. While cryptography consists in making the signal look garbled to unauthorized people, steganography consists in secret communication by camouflaging the secret signal in another signal (named the cover signal), to avoid suspicion. Steganography is the art of hiding information in order to covert communication from eavesdroppers. To provide secure channels for communicating entities steganography is the set of techniques striving to hide the presence of secret information from a third party. When compared to encryption techniques, steganography has the advantage of arousing less suspicion. The word steganography is derived from two Greek words: Stego (means cover) and graphy (means writing). The two combined words constitute steganography, which means covert writing is the art of hiding written communications. Steganography dates back to ancient times. Several steganography were used to send message secretly during wars through the territories of enemies. The use of steganography dates back to ancient time where it

was used by romans and ancient Egyptians [1]. Several steganography techniques were used to send messages secretly during wars through the territories of enemies. One technique according to Greek historian Herodotus, was to shave the head of a slave, tattoo the message on the slave's scalp, and send him after his hair grew back. Another technique was to write the secret message underneath the wax of a writing tablet. A third one is to use invisible ink to write secret messages within covert letters [2].

The relative necessities with secure channels for communication and the unlimited amount of bandwidth led us propose an audio steganography codec [3]. Therefore, there is a need to code and compress audio signals to more compact form before being transmitted. Hence researchers were incited to work on this burning field to develop schemes ensuring audio coding to reduce the coded bit rate [4]. In recent years, several applications for audio coding and compression gained ground in domains such as satellite communications, digital broadcasting, teleconferencing systems and voice mail systems.

The main task of high quality audio coding systems is to compress the signal in a way that compressed stego-signal is perceptually indistinguishable from the initial one. The stego-signal is referred to as the signal containing both cover signal and embedded information (secret information). Recently, audio compression techniques using Wavelet Transform (WT) have accommodated more attention, due to their encouraging compression ratio, Signal to noise ratio (SNR), and flexibility in representing speech signals [5]. The main issues related to the development of audio steganography codec using Discrete Wavelet Transform (DWT) are choosing optimal an wavelet transform for stego signals, decomposition level in the DWT and threshold criteria of coefficient truncation which is the basis to provide compression ratio for audio with appropriate peak signal to noise ratio (PSNR).

This paper is organized as follows: section 2, provide a brief overview of the related work on discrete wavelet transform based audio speech compression. After presenting the objectives in Section 3, we describe discrete wavelet transforms including speech decomposition and speech reconstruction in Section 4. Section 5 will describe the audio steganography compression based approach. The general step to compress a stego-speech signal is also included in this section. Then a description of the database, the parameters of our experiments, the evaluation and discussion of the results of our proposed audio steganography compression approach are presented in Section 6. Finally, we conclude and suggest directions for further research in Section 7.

2. RELATED WORK

Speech compression is the technology of removing the redundancy between neighboring samples of a speech signal and/or between the next cycles. Furthermore compression converts human speech into an efficiently encoded illustration that can later be decoded to produce a close approximation of the original signal (in this paper the original signal is referred to as the original stego-signal before encoding). Compression techniques can be classified into two main categories that can be used to reduce the coded bit rate: lossless and lossy. The first techniques take advantage from the statistical redundancy in the audio signal, in these methods the original audio signal can be completely recovered from the encoded signal. In the second method, the original and reconstructed audio signal are not completely identical, this technique separate necessary information and perceptual irrelevant signal than can be removed later.

D. Sinha et al., [6] have presented a new approach for audio compression using discrete wavelet transform. This technique is based on the dynamic dictionary approach with selection of the best adaptive wavelet choice and optimal coefficients quantization procedures. The proposed technique takes advantages from the masking effect persisting in the human hearing through the optimal wavelet transform selection and transform bit allocation measures. A permanent distortion level is used in order to reduce the required quantity of bits representing each frame of audio signal. The used dynamic dictionary significantly decreases statistical redundancies in the

audio source. The experimental results of the proposed method able to accomplish a transparent coding of monophonic compact disk (CD), sampled at 44.1 kHz at bit rates of 64-70 kilobits per second (kb/s). The combined adaptive wavelet selection and dynamic dictionary coding procedures realize approximately transparent coding of monophonic CD quality signals at bit rates of 48-66 kb/s.

P. Srinivasan et al., [7] have proposed a new high quality audio compression approach using an adaptive wavelet packet to achieve perceptual transparent compression of high-quality (44.1KHz) audio signals at about 45 kb/s. The adapted filter bank structure available at the decoder can achieve according to psychoacoustic criteria and computational complexity. The proposed technique takes advantage from the availability of a computational power in order to realize real time coding/decoding. The bit allocation method is an adapted zero-tree scheme taking input from the psychoacoustic model. The quantity performance measurement of the proposed technique named sub-band perceptual rate, is adapted by the filter bank structure to approach the perceptual entropy (PE) as closely as possible. This technique is able to accomplish a good quality of possible reconstruction considering the size of the bit stream existing at the decoder side, amenable to progressive transmission. Thus this technique presents a new scheme to approve the results in wavelet packets and perceptual coding in order to make a well matched algorithm to high-quality audio dedicated for internet and storage applications.

The wavelet analysis process is to implement a wavelet prototype function, known as an analyzing wavelet or mother wavelet. Coefficients in a linear combination of the wavelet function can be used in order to represent the development of the original signal in terms of a wavelet, data operations can be performed with the appropriate wavelet coefficients [8]. Choose the best wavelets adapted to represent your data, also truncate the coefficients below a threshold; your data is sparsely signified. Because of this sparse coding the wavelets is considered as an exceptional technique in the field of data compression. A general overview of the discrete wavelet transform is given in this section.

G. Amara et al., [9] have presented a general overview of wavelets that cut up information into different frequencies in order to perform a study of these different component with resolution corresponding to its scale. They introduced wavelets to the concerned industrial person outside the digital signal processing domain. A detailed history description of wavelets have been presented starting with the Fourier method, a comparison between these two methods was investigated. The main goal of this investigation was to state the properties and the special aspects of wavelets, and finally to list some interesting applications such as image compression, musical tones, and de-noising noisy data.

G. Tzanetakis et al., [10] have given a brief description of their study that consist on analyzing the temporal and spectral properties of non stationary signals such as audio using the Discrete Wavelet Transform. They also give a detailed description of some applications using Discrete Wavelet Transform and the difficulties of extracting data from non-speech audio. A detailed automatic classification of different types of audio using Discrete Wavelet Transform is described also a comparison with other traditional feature extractor proposed in the literature was given.

M. L. Hilton et al., [11] Have proposed an adaptive data selecting scheme for the threshold for wavelet contraction based noise removal. The proposed method involves a statistical test of theory based on a two dimensional cumulative sum of wavelet coefficients, that takes into consideration the coefficients magnitude and their positions.

G. Kronquist et al., [12], have presented a thresholding method on the discrete wavelet coefficients since the background noise has to be removed from the speech signal.

A soft thresholding have been used and particularly adopted to speech signal in order to reduce the coefficients. The training sequence is used to determine the noise levels which are adaptively

changed. Their proposed technique of thresholding for denoising speech signal improve that the signals does not change the characteristics of background noise, only its amplitude is decreased.

3. OBJECTIVES

Our objective is to develop a high performance compression speech steganography system. The design of such system mainly consists in the optimization of the following attributes:

- The compression ratio, used to quantify the reduction in speech-representation size produced by a compression algorithm. It is defined as the ratio of the size of the compressed signal to that of the initial signal.
- The impact of the compression process on the initial stego-speech (stego-signal) quality. We intend to produce a compressed stego-signal that is perceptually indistinguishable from the initial signal.
- Lossless compression, our aim is to allow the reconstruction of the initial stego-speech from the compressed signal after going through the compression-decompression process.
- The accuracy with which the compressed signal can be recovered at the receiver. Efficient techniques are to be developed to minimize the impact of compression on the stego-signal.

4. SPEECH DISCRETE WAVELET TRANSFORMS

The wavelet transform transforms the signal from the time domain to the wavelet domain. This new domain contains more complicated basis functions called wavelets, mother wavelets or analyzing wavelets [13]. The fundamental idea behind wavelets is to analyze the behavior of the signal with respect to scale. Any signal can then be represented by translated and scaled versions of the mother wavelet. Wavelet analysis is capable of enlightening aspects of data that other signal analysis techniques are unable to perform, aspects like trends, discontinuities in higher derivatives, breakdown points and self-similarity.

The basic idea of DWT for one-dimensional signals is shortly described. The wavelet analysis enables splitting a signal in two parts, usually the high frequencies and the low frequencies part. This process is called decomposition. The edge components of the signal are largely limited to the high frequencies part. The signal goes through series of high pass filters to analyze the high frequencies, and goes through series of low pass filters to analyze the low frequencies. Filters of different cutoff frequencies are used to analyze the signal at different resolutions [14,15].

The DWT involves choosing scales and positions based on powers of two, so called dyadic scales and positions. The mother wavelet is rescaled by powers of two and transformed by integers. Specifically, a function $f(t) \in L^2(R)$ (defines space of square integrable functions) can be represented as:

$$f(t) = \sum_{j=1}^L \sum_{k=-\infty}^{\infty} d(j,k) \psi(2^{-j}t - k) + \sum_{k=-\infty}^{\infty} a(L,k) \phi(2^{-L}t - k) \quad (1)$$

The function $\psi(t)$ is known as the mother wavelet, while $\phi(t)$ is known as the scaling function. The set of function $\{\sqrt{2^{-L}} \phi(2^{-L}t - k), \sqrt{2^{-j}} \psi(2^{-j}t - k) | j \leq L, j, k, L \in Z\}$, Where Z is the set of integers is an orthonormal basis for $L^2(R)$. The numbers $a(L,k)$ are known as the approximation coefficients at scale L , while $d(j,k)$ are identified as the detail coefficients at scale j . The approximation and detail coefficients can be expressed consecutively as:

$$a(L,k) = \frac{1}{\sqrt{2^L}} \int_{-\infty}^{\infty} f(t) \phi(2^{-L}t - k) dt \quad (2)$$

$$d(j, k) = \frac{1}{\sqrt{2^j}} \int_{-\infty}^{\infty} f(t) \psi(2^{-j}t - k) dt \quad (3)$$

To better understand the above coefficients let's consider a projection $f_l(t)$ of the function $f(t)$ that provides the best approximation (in the sense of minimum error energy) to $f(t)$ at a scale l . This projection can be constructed from the coefficients $a(L, k)$, using the equation:

$$f_l(t) = \sum_{k=-\infty}^{\infty} a(l, k) \phi(2^{-l}t - k) \quad (4)$$

As the scale L decreases, the approximation becomes finer, converging to $f(t)$ as $l \rightarrow 0$. The difference between the approximation at scale $l+1$ and that at l , $f_{l+1}(t) - f_l(t)$, is totally defined by the coefficients $d(j, k)$ using the equation of decomposition and can mathematically be expressed as follows:

$$f_{l+1}(t) - f_l(t) = \sum_{k=-\infty}^{\infty} d(l, k) \psi(2^{-l}t - k) \quad (5)$$

Using these relations, given $a(L, k)$ and $\{d(j, k) \mid j \leq L\}$, are useful for building the approximation at any scale. Hence, the wavelet transform breaks the signal up into a coarse approximation $f_L(t)$ (given $a(L, k)$) and a number of layers of detail $\{f_{j+1} - f_j(t) \mid j < L\}$ (given by $\{d(j, k) \mid j \leq L\}$). As one layer of details is added, the approximation at the next higher scale is achieved.

4.1 Signal decomposition

Starting with a discrete input stego-speech signal, the primary steps of the DWT algorithm consists in decomposing the signal into sets of coefficients. These are the approximation coefficients cA_1 (low frequency information, Figure 1) and the detail coefficients cD_1 (high frequency information). In order to obtain the coefficient vectors, the signal s goes through the low-pass filter Lo_D (mathematically stated, a convolution operation is performed) and through the high-pass filter Hi_D for details. A down sampling by a factor of 2 or a dyadic decimation is then applied to obtain the approximation coefficients [16]. The filtering operation process of the DWT is shown in Figure 1.

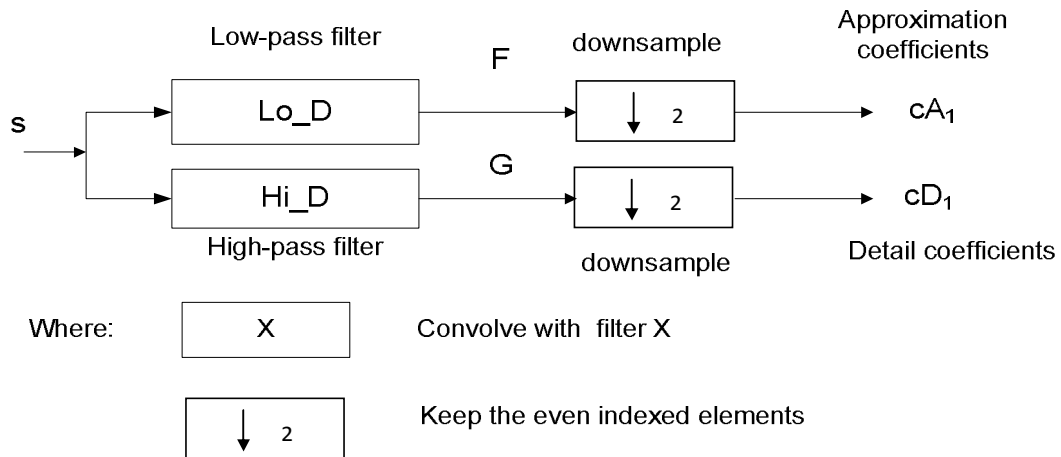


FIGURE 1: Filtering Operation of the DWT

Mathematically the two-channel filtering of the discrete signal can be represented by:

$$cA_1 = \sum_k c_k s_{2l-k} \quad (6), \quad cD_1 = \sum_k g_k s_{2l-k} \quad (7)$$

These equations implement a convolution with a down sampling by a factor 2, then transfer the forward discrete wavelet transform. If the length of the initial stego-signal s is equal to n , and if the length of all filter is equivalent to $2N$, then the equivalent lengths of the coefficients cA_1 and cD_1 are calculated by:

$$\text{floor}\left(\frac{n-1}{2}\right) + N \quad (8)$$

This shows that the total length of the wavelet coefficients vector is always slightly greater than the length of the initial signal due to the filtering process used. Wavelet decomposition tree can be constructed by following an iterative decomposition process with successive approximations [17]. Thus, the input stego-signal is broken down in several subordinate resolution components. Figure 2 shows the decomposition in approximation and details of signal s in 3 levels.

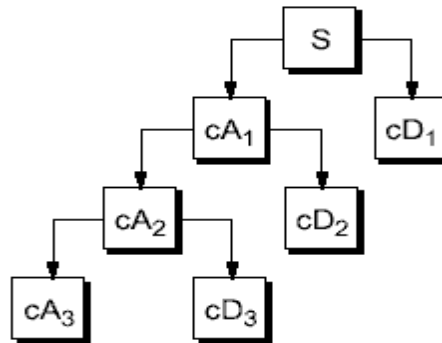


FIGURE2: Decomposition of DWT coefficients

4.2 Signal Reconstruction

The initial signal can be reconstructed using the Inverse Discrete Wavelet Transform (IDWT), following the above procedure of Figure 2 in the reverse order. As pointed out is shown in Figure 3, the synthesis starts with the approximation and detail coefficients cA_j and cD_j , and then reconstructs cA_{j-1} by up sampling and filtering with the reconstruction filters [18, 19].

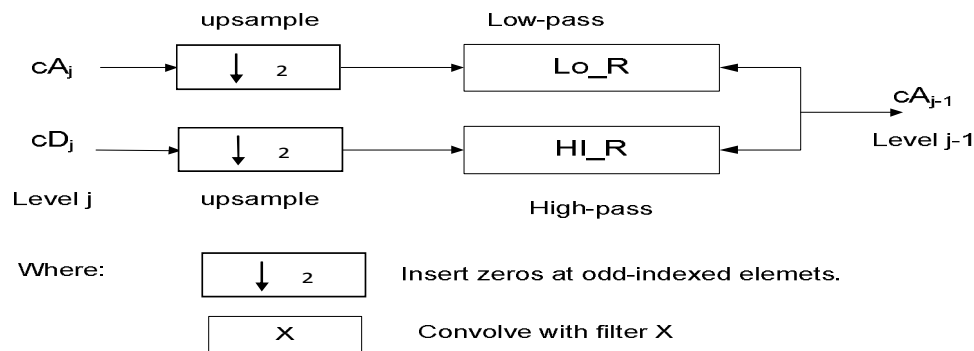


FIGURE3: Wavelets Reconstruction

The effect of aliasing created in the wavelet decomposition stage is revoked with the effect of the reconstruction filters. This process forms a system known as quadrature mirror filters (QMF) composed with the reconstruction filters (Lo_R and Hi_R) and with the low and high pass decomposition filters. For a multilevel analysis, approximations at finer resolutions and a synthesized initial signal can be produced during the reconstruction procedure.

5. AUDIO STEGANOGRAPHY COMPRESSION BASED APPROACH

The idea behind stego-signal compression using wavelets is principally related to the relative scarceness of the wavelet domain representation for the signal. Wavelets concentrate speech information (energy and perception) into a few neighboring coefficients [20]. Therefore; several coefficients will either be zero or have insignificant magnitudes, this effect resulting from taking the wavelet transform of a signal [21]. Data compression is then achieved by treating small valued coefficients as insignificant data and thus removing them the process of compressing a speech signal using wavelets involves a number of different stages, each of which are discussed below. Figure 4 shows the block diagram of the different steps involved in the compression of the stego-speech signal by using discrete wavelet transform, using Matlab version 9. In designing a wavelet based stego-speech coder, the major issues covered in this section are:

1. Hiding an audio speech signal in a cover signal
2. Setting up an audio steganography database using a different hiding technique.
3. Choosing optimal wavelets for stego-speech,
4. Selecting decomposition level in wavelet transforms,
5. Choosing Threshold criteria for the truncation of coefficients,
6. Efficiently representing zero valued coefficients,
7. Quantizing and digitally encoding the coefficients,
8. Signal reconstruction

The performance of the wavelet compression method in coding stego-speech signals and the quality of the reconstructed signals is also evaluated.

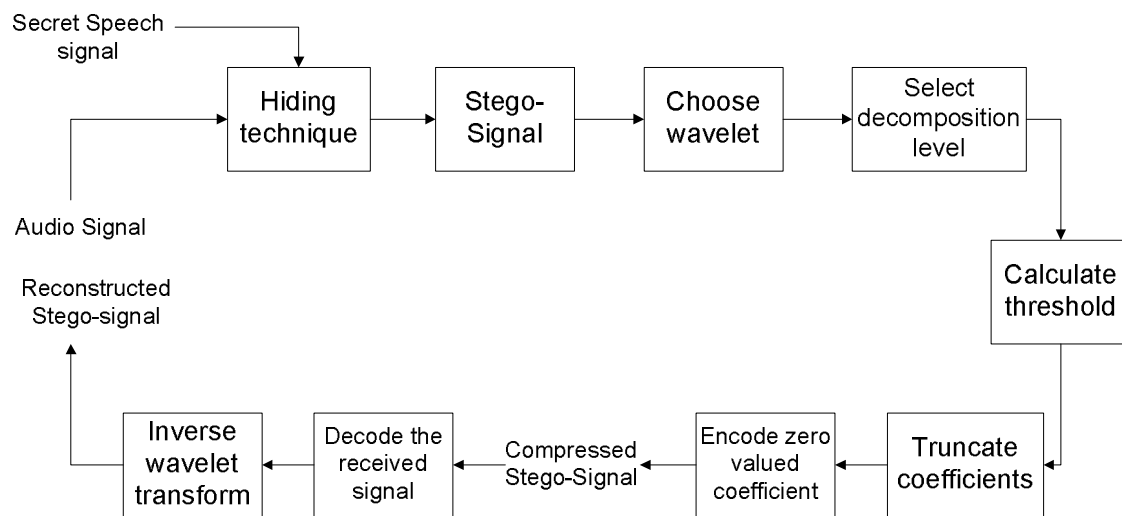


FIGURE 4: Block diagram of the based stego-speech encoder/decoder

5.1. Audio Steganography Database

Steganography provides secrecy by making secret information invisible to opponents [22]. Steganography hide the data by embedding it in another data medium called cover. In this paper we intend to apply our compression techniques on speech by generating speech-in-speech files. In order to generate our stego-speech database, we use three different steganographic techniques. The first one was our speech steganography technique using discrete wavelet and fast fourier transform developed in [23]. The two other methods are Steganos[24] and StegHide [25]. These tools were chosen on the basis of being popular methods and also with readily available software.

5.2 Choice Of The Mother-Wavelet

The choice of the appropriate mother-wavelet is of great importance for designing high quality speech coders. The choice of the optimal wavelet function is based on several criteria. Since the main objective is to maximize the signal to noise ratio (SNR). In general the amount of energy a wavelet basis function can concentrate into the level 1 approximation is one of the criteria that can be used to select the optimum wavelet. By giving a better SNR ratio, daubechies wavelets provide a good compression property for wavelet coefficients.

5.3 Wavelet Decomposition

For a given stego-signal the wavelet starts by decomposing a signal at different level that can reach up to $L = 2K$ levels, where K is the length of the discrete signal. Thus we can perform the transform at any of these levels. The type of signal being analyzed usually affects the choice of the decomposition level. In order to represent the accurately signal components the selection of the appropriate number of approximation and details coefficients is extremely important in the compression procedure. For the processing of speech signals decomposition up to scale 5 is sufficient, with no further advantage gained in processing beyond scale 5 [26]. In the paper, comparisons were made with level 4 and 6 decomposition after performing levels 5 decomposition.

5.4 Threshold Calculation

After applying DWT the obtained coefficients on the frame concentrate energy in few neighbors. Thus we can truncate all coefficients with "low" energy and preserve those holding the high energy value. Two different techniques can be used for calculating thresholds. The first, recognized as Global Thresholding consist of taking the wavelet expansion of the signal and preserving the largest absolute value coefficients. In this method we can set a global threshold manually, thus just a single parameter needs to be selected. The coefficient values below this value should be set to zero, to achieve compression. The second technique known as By Level Thresholding consists of applying visually determined level dependent thresholds to each decomposition level in the wavelet transform [27].

The following figure5 shows the setting of global threshold for a typical stego-speech signal. In this figure, the X-axis represents the coefficient values. The black (dark) vertical line moves to right or left, thereby changing the threshold. The intersection of this line with green line indicates the percentage of zero coefficients below this threshold. Its intersection with the red line indicates the percentage of signal energy retained after truncating these coefficients to zero.

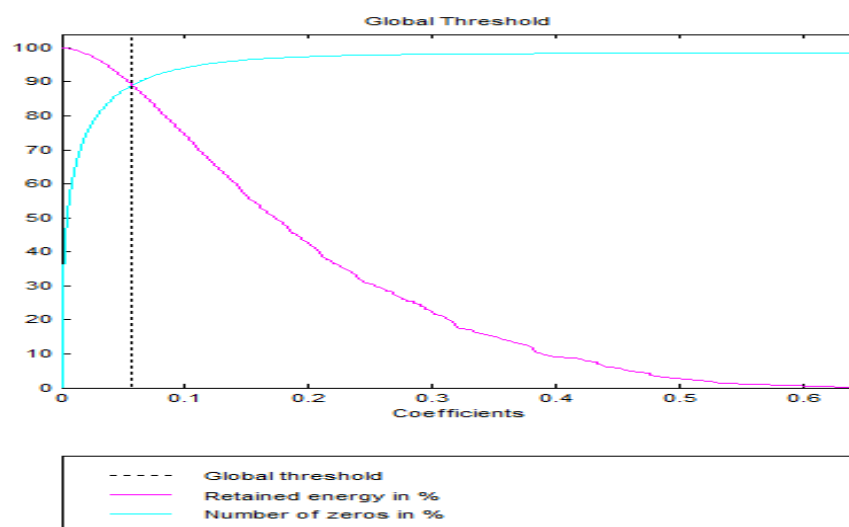


FIGURE 5: Setting of global threshold for a typical stego-speech signal

5.5 Encoding Coefficients

Signal compression is achieved by first truncating small-valued coefficients and then encoding them. Storing the coefficients along with their corresponding positions in the wavelet transform vector, in order to represent the high-magnitude coefficients [28]. For a stego-speech signal of frame size F , taking the DWT generates a frame of size T , slightly larger than F . If only the largest L coefficients are retained, then the compression ratio C is given by:

$$C = \frac{F}{2L} \quad (9)$$

Another approach to compression is to encode consecutive zero valued coefficients [29], with two bytes. One byte to present a series of zeros in the wavelet transforms vector and the second byte representing the number of consecutive zeros. The transform vector has to be compressed, after zeroing wavelet coefficients with negligible values based on either calculating threshold values or simply selecting a truncation percentage.

In this proposed audio steganography coding, consecutive zero valued coefficients are encoded with two bytes. One byte is used to identify a starting string of zeros and the second byte keeps track of the number of successive zeros. Due to the scarcity of the wavelet representation of the stego-speech signal, this encoding technique leads to a higher compression ratio than storing the non-zero coefficients along with their respective positions in the wavelet transform vector, as suggested in the literature review [30].

6. EVALUATION

6.1 Experimental Setup

To evaluate the performance of the proposed audio steganography coding, we conducted several computer simulations using NOIZEUS database [31,32,33]. This corpus contains thirty sentences from the IEEE sentence database, recorded in a sound-proof booth using Tucker Davis Technologies (TDT) recording equipment. The sentences are produced by three male and female speakers. The thirty sentences: 15 male and 15 female include all phonemes in the American English language. The sentences were originally sampled at 25 kHz and down-sampled to 8 kHz. The length of the speech file varies between 0.02 ms to 0.03 ms. In the comparative evaluation, we conducted three sets of tests, before starting the compression procedure. In the first set of simulations, we embedded each of the 15 male speech files in the remaining 14 male speech files using DWT-FFT technique [23]. In the second set of tests, we hide the same gender speech files using StegHide software [24]. In the third set of tests, we hide the same gender speech files using Steganos software [25]. Every set is iterated with female speech files. Each set is iterated for 2 different wavelet families (Haar, Daubechies). Db4, Db6, Db8, Db10, Haar. The selection of these appropriate mother-wavelets is based on the amount of energy a wavelet basis function can concentrate into the level 1-approximation coefficients.

All the stego-speech signals were decomposed to scale 5 and Global Thresholding was applied. The entire signal was decomposed at once without framing. A summary of the performance is given below for the different used wavelets.

6.2 Evaluation Outcomes

One of the performance measures of any stego-speech coding system is the comparison between the original (stego-speech) and the compressed signals. In this work, we used subjective and objective performance measures. In the subjective measures, we conducted several informal listening comparative tests. In these simulations, we played in a random order the original signal and the compressed signal to several listeners. Each listener had to identify the better quality speech file among the original and the compressed signals. The majority of listeners couldn't distinguish between the two speech files.

As an objective measure, a number of quantitative parameters is used to assess the performance of the wavelet based stego-speech coder, in terms of both reconstructed signal quality after decoding and compression scores. The following parameters are compared (Signal to Noise Ratio (SNR), Normalized Root Mean Square Error (NRMSE), and Retained Signal Energy).

The results obtained for the above quantities are calculated using the following formulas:

- Signal to Noise Ratio

$$SNR = 10 \log_{10} \left(\frac{\sigma_x^2}{\sigma_e^2} \right) \quad (10)$$

σ_x^2 is the mean square of the speech signal and σ_e^2 is the mean square difference between the original and reconstructed signals.

- Peak Signal to Noise Ratio

$$PSNR = 10 \log_{10} \frac{NX^2}{\|x-r\|^2} \quad (11)$$

N is the length of the reconstructed signal, X is the maximum absolute square value of the signal x and $\|x-r\|^2$ is the energy of the difference between the original and reconstructed signals.

- Normalized Root Mean Square Error

$$NRSME = \sqrt{\frac{(x(n)-r(n))^2}{(x(n)-\mu_x(n))^2}} \quad (12)$$

$x(n)$ is the speech signal, $r(n)$ is the reconstructed signal, and $\mu_x(n)$ is the mean of the speech signal.

- Retained Signal Energy

$$RSE = \frac{100 * \|x(n)\|^2}{\|r(n)\|^2} \quad (13)$$

$\|x(n)\|$ is the norm of the original signal and $\|r(n)\|$ is the norm of the reconstructed signal. For one-dimensional orthogonal wavelets the retained energy is equal to the L2-norm recovery performance.

- Compression Ratio

$$C = \frac{\text{Length}(x(n))}{\text{Length}(cWC)} \quad (14)$$

cWC is the length of the compressed wavelet transform vector. The original stego-speech signal which was used to obtain the performance measure.

In table 1, we present the average of the used quantitative parameters for each of the three different sets of tests for level 4 decomposition. In table 2, we present the average of the same sets of tests for level 5 decomposition. For level 6 decomposition the result is presenting is table 3.

Level 4	Male speaker					Female speaker				
Wavelet	C	SNR	PSNR	NRMSE	RSE (%)	C	SNR	PSNR	NRMSE	RSE (%)
Db4	2.95	18.86	83.65	0.86	95.88	2.82	18.76	86.64	0.57	94.98
Db6	2.21	18.63	84.53	0.59	96.87	2.61	18.73	79.43	0.58	97.98
Db8	3.09	18.58	79.68	0.68	97.72	3.01	17.58	76.54	0.75	96.87
Db10	3.19	17.91	74.83	0.59	96.75	3.09	17.61	74.63	0.77	96.78
Haar	3.18	17.55	73.24	0.89	94.75	3.05	18.45	83.24	0.83	96.84

TABLE 1: A male and female Stego-speech decomposed at level 4.

Level 5	Male speaker					Female speaker				
Wavelet	C	SNR	PSNR	NRMSE	RSE (%)	C	SNR	PSNR	NRMSE	RSE (%)
Db4	3.15	19.86	87.65	0.57	96.88	3.08	19.76	87.65	0.67	95.88
Db6	3.21	19.93	89.45	0.37	98.98	3.11	19.83	89.45	0.39	96.98
Db8	3.19	19.68	86.64	0.58	97.92	3.01	19.58	86.64	0.58	96.87
Db10	3.09	19.61	84.73	0.47	96.69	3.09	19.51	84.73	0.47	96.78
Haar	3.15	19.75	83.24	0.78	97.85	3.05	19.65	83.24	0.77	96.84

TABLE 2: A male and female Stego-speech decomposed at level 5.

Level 6	Male speaker					Female speaker				
Wavelet	C	SNR	PSNR	NRMSE	RSE (%)	C	SNR	PSNR	NRMSE	RSE (%)
Db4	2.45	17.86	82.65	0.93	94.88	2.92	17.76	85.64	0.97	93.98
Db6	2.01	17.63	83.53	0.69	95.87	2.51	17.73	78.43	0.78	96.98
Db8	2.09	17.58	78.68	0.78	96.72	2.91	17.68	75.54	0.85	95.87
Db10	2.19	16.91	73.83	0.79	95.75	3.09	17.11	73.63	0.97	96.38
Haar	2.88	17.55	72.24	0.99	93.75	2.45	18.15	82.24	0.73	96.14

TABLE 3: A male and female Stego-speech decomposed at level 6.

It is observed that no advantage is gained in going beyond scale 5 and usually processing at a lower scale leads to a better compression ratio. Therefore, for processing speech signals choosing the right decomposition level in the DWT is important. Male voices have relatively more approximate coefficients than female voices for all levels decomposition. Based on the energy retained in the first $N/2$ coefficients criterion, Daubechies 6 preserves perceptual information better than all the other wavelets tested. The Db6 wavelet also provides the highest SNR, PSNR, compression ratio, and lowest NRMSE, as shown in table 2.

Figure 6 show the original stego-signal in red color and the compressed stego-signal in black color using Db6 wavelet and 5 level decomposition.

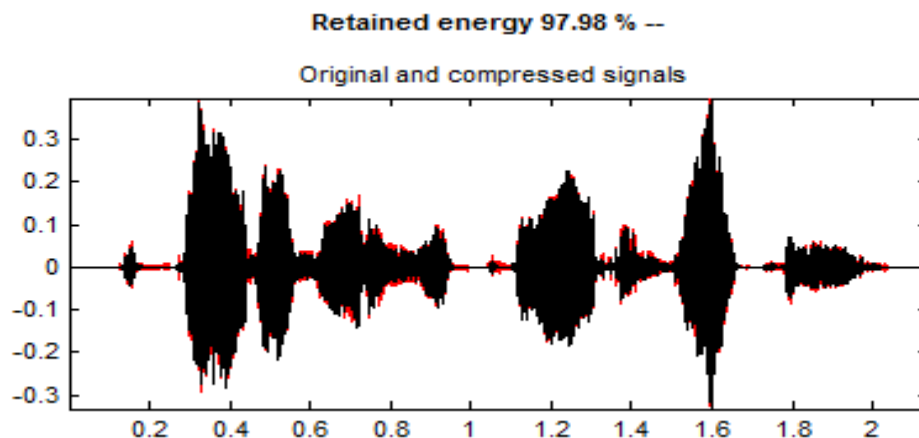


FIGURE 6: Original and compressed stego-signal

The performance of the stego-audio codec is evaluated by taking into consideration diverse parameters such as steganography system, decomposition levels, optimal wavelets and threshold value for wavelet coefficients in order to obtain low bit rate signal. In the simulation results show we can observed that the optimum number of wavelet decomposition level is 5 by using the Daubechies 6 wavelet. More specifically, the results demonstrates that the Daubechies wavelets best suits the compression of stego-speech signals due to their high SNR values of 19.93 dB and low NRMSE value of 0.39 compared with the other family wavelets. It is well recognized that the SNR cannot faithfully indicate speech quality. For evaluation of performance of wavelets for speech enhancement one more criteria used is subjective test. As subjective measures we have conducted informal listening tests. In these simulations, the evaluators have listened randomly to both the original stego-speech and the compressed signal and give their

opinion for which one has the better quality. Most of the listeners couldn't distinguish between original stego-speech a compressed speech.

7. CONCLUSIONS

This work has proven through informal tests that our audio steganography compression technique is robust. The proposed coding method produces a compressed stego-speech files that are indistinguishable from their equivalent stego- speech files. Therefore this method does not depend on the type of steganographic technique. The results show that the use of wavelet transform achieves high compression ratios with acceptable SNR. The proposed wavelet based steganography compression system reaches an SNR of 19.93 dB at a compression ratio of 3.21 by using the Daubechies 6 wavelet. Performance was measured by using the Haar and Daubechies wavelet families. These parameters values are very significant in design efficient wavelet based stego-speech compression software for mobile applications and multimedia. Furthermore the compression ratios can be easily varied when using the wavelets technique, while most other compression method has a fixed compression ratio.

In future work, we will extend this work to applications involving Voice over IP (VoIP) audio steganography coding and to using other speech coding technique such as excited linear predictive coding (CELP) for speech.

8. REFERENCES

- [1] Petitcolas, Fabian A.P.; Katzenbeisser, Stefan. "Information Hiding Techniques for Steganography and Digital Watermarking". Artech House Publishers. ISBN 1-58053-035-4. (2000).
- [2] Johnson, N.F. Jajodia, S. "Exploring steganography: Seeing the unseen," IEEE Computer 31 (2), pp.26–34, 1998.
- [3] S. I. Gel'fand and M. S. Pinsker, "Coding for channel with random parameters," Prob. of Control and Inform. Theory, vol. 9, no. 1, pp. 19–31, 1980.
- [4] N. F. Johnson and S. Katzenbeisser. "Information hiding - a survey", Artech House, Norwood, MA, 2000.
- [5] Oppenheim, Alan V.; Schaffer, Ronald W.; Buck, John A. (1999). Discrete-time signal processing. Upper Saddle River, N.J.: Prentice Hall. pp. 468–471. ISBN 0-13-754920-2.
- [6] D. Sinha and A. H. Tewfik, "Low bit rate transparent audio compression using adapted wavelets," IEEE Transactions on Signal Processing, vol. 41, no. 12, pp. 3463–3479, 1993.
- [7] P. Srinivasan and L. H. Jamieson, "High Quality Audio Compression using an Adaptive Wavelet Packet decomposition and Psychoacoustic Modelling," *IEEE Transactions on Signal Processing*, Vol. 46, No. 4, April 1998, pp. 1085-1093.
- [8] 1/C Chris Eubanks, "Haar Wavelets, Image Compression, and Multi-Resolution Analysis", Initial Report for Capstone Paper, SM422 April 4, 2007.
- [9] G.Amara "An introduction to Wavelets", IEEE Computational Science and Engineering, 1995, vol. 2, num. 2.
- [10] G.Tzanetakis, G. Essl, P. Cook," Audio Analysis using the Discrete Wavelet Transform", conference on Signal Processing, 2001.
- [11] M.L. Hilton, R.T, Ogden, "Data analytic wavelet threshold selection in 2-D signal denoising", Signal Processing, IEEE Transactions on, Issue 2, pages 496-500, August 2002.

- [12] G. Kronquist and H. Storm, "Target Detection with Local Discriminant Bases and Wavelets," Proc. of SPIE, v. 3710, pp 675-683, 1999.
- [13] M. Misiti, Y. Misiti, G. Oppenheim and J-M Poggi, "Wavelet Toolbox™ 4 User's Guide", The Math Works Inc., 2000.
- [14] B. Lin, B. Nguyen and E.T. Olsen, "Orthogonal Wavelets and Signal Processing", Signal Processing Methods for Audio, Images and Telecommunications, P.M. Clarkson and H. Stark, ed., Academic Press, London, 1995, pp. 1-70.
- [15] S. Mallat, "A Wavelet Tour of Signal Processing", Academic Press, San Diego, Calif., 1998.
- [16] J.I. Agbinya, "Discrete Wavelet Transform Techniques in Speech Processing", IEEE Tencon Digital Signal Processing Applications Proceedings, IEEE, New York, NY, 1996, pp 514-519.
- [17] H. Shahina and T. Takara, "Performance Comparison of Daubechies Wavelet Family for Bangla Vowel Synthesis", JOURNAL OF COMPUTING, VOLUME 3, ISSUE 9, SEPTEMBER 2011, ISSN 2151-9617.
- [18] Y. Nievergelt, "Wavelets made easy", Birkhäuser, Boston, 1999.
- [19] J. Ooi and V. Viswanathan, "Applications of Wavelets to Speech Processing", Modern Methods of Speech Processing, R.P. Ramachandran and R. Mammone, ed., Kluwer Academic Publishers, Boston, 1995, pp. 449-464.
- [20] Cai, T. and Silverman, B. W. "Incorporating information on neighboring coefficients into wavelet estimation", (1999).
- [21] Coifman, R.R. and Donoho, D.L. (1995). Translation invariant denoising. In A. Antoniadis and G. Oppenheim (eds), Wavelets and Statistics, Lecture Notes in Statistics 103. New York: Springer-Verlag, pp. 125-150.
- [22] M.M. Amin, M. Salleh, S. Ibrahim, et al., "Information Hiding Using Steganography", 4th National Conference On Telecommunication Technology Proceedings (NCTT2003), Shah Alam, Malaysia, pp. 21-25, January 14-15, 2003.
- [23] R. Siwar, G. Driss, S. Sid-Ahmed, H. Habib "Speech Steganography using Wavelet and Fourier Transforms" EURASIP Journal on Audio, Speech, and Music Processing, Accepted.
- [24] Steganos, <http://www.steganos.com>.
- [25] <http://steghide.sourceforge.net/>
- [26] J.I. Agbinya, "Discrete Wavelet Transform Techniques in Speech Processing", IEEE Tencon Digital Signal Processing Applications Proceedings, IEEE, New York, NY, 1996, pp 514-519.
- [27] A. Jayaraman, P. Indumathy, "A New Threshold Calculation Approach in the Performance Enhancement of Spread Spectrum System Using Double Density Discrete Wavelet Filter" Communications in Computer and Information Science, 2010, Volume 101, Part 3, 654-659, DOI: 10.1007/978-3-642-15766-0_115.

- [28] E.B. Fgee, W.J. Phillips, W. Robertson, .Comparing Audio Compression using Wavelets with other Audio Compression Schemes,. IEEE Canadian Conference on Electrical and Computer Engineering, IEEE, Edmonton, Canada, 1999, pp. 698-701.
- [29] W. Kinsner and A. Langi, "Speech and Image Signal Compression with Wavelets",. IEEE Wescanex Conference Proceedings, IEEE, New York, NY, 1993, pp. 368-375.
- [30] B. Lin, B. Nguyen and E.T. Olsen, "Orthogonal Wavelets and Signal Processing",.Signal Processing Methods for Audio, Images and Telecommunications, P.M.Clarkson and H.Stark, ed., Academic Press, London, 1995, pp. 1-70.
- [31] Hu, Y. and Loizou, P. "Subjective evaluation and comparison of speech enhancement algorithms," Speech Communication, 2007, 49, 588-601.
- [32] Hu, Y. and Loizou, P. "Evaluation of objective quality measures for speech enhancement," IEEE Transactions on Speech and Audio Processing, 2008, 16(1), 229-238.
- [33] Ma, J., Hu, Y. and Loizou, P. "Objective measures for predicting speech intelligibility in noisy conditions based on new band-importance functions", Journal of the Acoustical Society of America, 2009,125(5), 3387-3405

New Proposed Classic Cluster Layer Architecture for Mobile Adhoc Network (cclam)

Kuldeep Sharma

Research Scholar

Anna University Coimbatore, INDIA-560066

sharma.kuldeep3@gmail.com

Nikhil Khandelwal

Student

BITS PILANI, INDIA

nikhil.khandelwal08@gmail.com

Sanjeev Kumar Singh

Assistant Professor, GLBITM,

Greater Noida, INDIA

sanjeevpbh@gmail.com

Abstract

Organization, scalability and routing have been identified as key problems hindering viability and commercial success of mobile ad hoc networks. Clustering of mobile nodes among separate domains has been proposed as an efficient approach to address those issues. In this work, we introduce an efficient distributed clustering layer algorithm that uses location metrics for cluster formation and we divided cluster in layers to secure our ordinary nodes. Our proposed solution mainly addresses cluster stability and manageability issues. Also, unlike existing active clustering methods, our algorithm relieves the network from the unnecessary burden of control messages broadcasting, especially for relatively static network topologies. The efficiency, scalability and competence of our algorithm against alternative approaches have been demonstrated through algorithm.

Keywords: Secure Architecture Design, Updated Database, Master Node

1. INTRODUCTION

Wireless communication and the lack of centralized administration pose numerous challenges in mobile wireless ad-hoc networks (MANETs) [6]. Node mobility results in frequent failure and activation of links, causing a routing algorithm reaction to topology changes and hence increasing network control traffic [2]. Ensuring effective routing and QoS support while considering the relevant bandwidth and power constraints remains a great challenge. Given that MANETs may comprise a large number of MNs, a hierarchical structure will scale better [5].

Hence, one promising approach to address routing problems in MANET environments is to build hierarchies among the nodes, such that the network topology can be abstracted. This process is commonly referred to as *clustering* and the substructures that are collapsed in higher levels are called *clusters* [12]. The concept of clustering in MANETs is not new; many algorithms that consider different metrics and focus on diverse objectives have been proposed [12]. However, most existing algorithms fail to guarantee stable cluster formations. More importantly, they are based on periodic broadcasting of control messages resulting in increased consumption of network traffic and mobile hosts (MH) energy. In this article, we introduce a distributed algorithm for efficient and scalable clustering of MANETs that corrects the two aforementioned weaknesses. The main contributions of the algorithm are: fast completion of clustering procedure, where both location and battery power metrics are taken into account; derived clusters are sufficiently stable, while cluster scale is effectively controlled so as not to grow beyond certain limits; minimization of control traffic volume, especially in relatively static MANET environments. The remainder of the paper is organized as follows: Section II provides an overview of clustering

concepts and algorithms. Section II New Network Model and algorithm. IV Characteristics of Cluster and MN Finally, Section V concludes the paper and draws directions for future work.

II. CLUSTERING

In clustering old procedure, a representative of each subdomain (cluster) is 'elected' as a *cluster head* (CH) and a node which serves as intermediate for inter-cluster communication is called *gateway*. Remaining members are called *ordinary nodes*. The boundaries of a cluster are defined by the transmission area of its CH. With an underlying cluster structure, non-ordinary nodes play the role of dominant forwarding nodes, as shown in Figure 1.1.

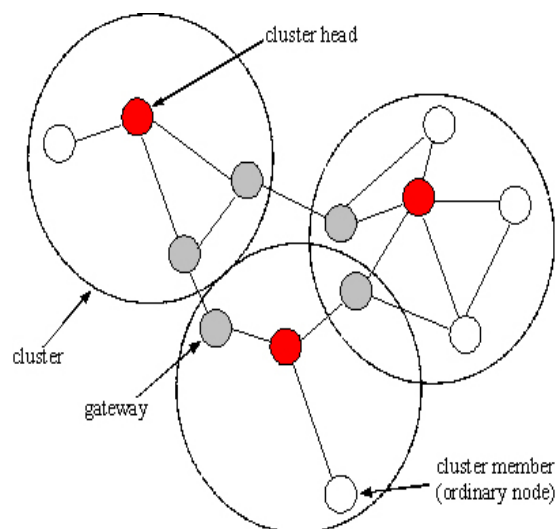


FIGURE 1: Cluster heads, gateways and ordinary nodes in mobile ad hoc network clustering.

Cluster architectures do not necessarily include a CH in every cluster. CHs hold routing and topology information, relaxing ordinary MHs from such requirement; however, they present network bottleneck points. In clusters without CHs, every MH has to store and exchange more topology information, yet, that eliminates the bottleneck of CHs. Yi et al. identified two approaches for cluster formation, *active clustering* and *passive clustering* [10]. In active clustering, MHs cooperate to elect CHs by periodically exchanging information, regardless of data transmission. On the other hand, passive clustering suspends clustering procedure until data traffic commences [11]. It exploits on-going traffic to propagate "cluster-related information" (e.g., the state of a node in a cluster, the IP address of the node) and collects neighbor information through promiscuous packet receptions.

Passive clustering eliminates major control overhead of active clustering, still, it implies larger setup latency which might be important for time critical applications; this latency is experienced whenever data traffic exchange commences. On the other hand, in active clustering scheme, the MANET is flooded by control messages, even while data traffic is not exchanged thereby consuming valuable bandwidth and battery power resources.

Recently multipoint relays (MPRs) have been proposed to reduce the number of gateways in active clustering. MPR hosts are selected to forward broadcast messages during the flooding process [7]. This technique substantially reduces the message overhead as compared to a typical flooding mechanism, where every node retransmits a message when it receives its first copy. Using MPRs, the Optimized Link State Routing (OLSR) protocol can provide optimal routes, and at the same time minimize the volume of signaling traffic in the network [1]. An efficient clustering method should be able to partition a MANET quickly with little control overhead. Due to the dynamic nature of MANETs, optimal cluster formations are not easy to build. To this end, two

distributed clustering algorithms have been proposed: Lowest ID algorithm (LID) [10] and Highest Degree algorithm (HD) [10]. Both of them belong to active clustering scheme.

In LID algorithm, each node is assigned a unique ID. Periodically, nodes broadcast the list of nodes located within their transmission range (including themselves) through a 'Hello' control message. The lowest-ID node in a neighborhood is then elected as the CH; nodes which can 'hear' two or more CHs become gateways, while remaining MHs are considered as ordinary nodes. In HD algorithm, the highest degree node in a neighborhood, i.e. the node with the largest number of neighbors is elected as CH. Figure 2 compares LID vs. HD algorithm approaches.

LID method is a quick clustering method, as it only takes two 'Hello' message periods to decide upon cluster structure and also provides a more stable cluster formation than HD. In contrast, HD needs three 'Hello' message periods to establish a clustered architecture [3]. In HD method, losing contact of a single node (due to MH movement), may cause failure of the current CH to be re-elected. On the other hand, HD method can get fewer clusters than LID, which is more advantageous in large-scale network environments.

In current clustering schemes, stability and cluster size are very important parameters; however, reducing the number of clusters does not necessarily result in more efficient architectures. A CH may end up dominating so many MHs that its computational, bandwidth and battery resources will rapidly exhaust. Therefore, effective control of cluster size is another crucial factor.

Summarizing, both LID and HD algorithms use exclusively location information to form clusters and elect CHs. In a more recent approach, Li et al proposed Vote-based Clustering (VC) algorithm, where CH elections are based not purely on location but also on the battery power level of MHs [3]. In particular, MHs with high degree (large number of neighbors) and sufficient battery power are elected as CHs. However, simulations have shown that the combination of position and power information in clustering procedure results in frequent CH changes, i.e. overall cluster structure instability [3]. In a MANET that uses cluster-based services, network performance metrics such as throughput, delay and effective management are tightly coupled with the frequency of cluster reorganization. Therefore, stable cluster formation is essential for better management and QoS support. In addition, LID, HD and VC algorithms share a common design characteristic which derives from their active clustering origin. Cluster formation is based on the periodic broadcast of 'Hello' signaling messages. In cases where MHs are relatively static (e.g. in collaborative computing, on-the-fly conferencing, etc), periodic 'storms' of control messages only occur to confirm that cluster structure established in previous period should remain unchanged. These unnecessary message broadcasts not only consume network bandwidth, but valuable battery power as well.

III. New Network Model

In clustering my procedure, a representative of each subdomain (cluster) is 'elected' as a *Master Node (MN)* and a node which serves as intermediate for inter-cluster communication is called *gateway*. Remaining members are called *ordinary nodes*. The boundaries of a cluster are defined by the transmission area of its CH. With an underlying cluster structure, non-ordinary nodes play the role of dominant forwarding nodes, as shown in Figure 1.2.

In this Clustering procedure I have divided Cluster into three Core Cluster Layers such as (1) Core Cluster (2) Core Cluster Layer 1 (3) Core Cluster Layer 2.

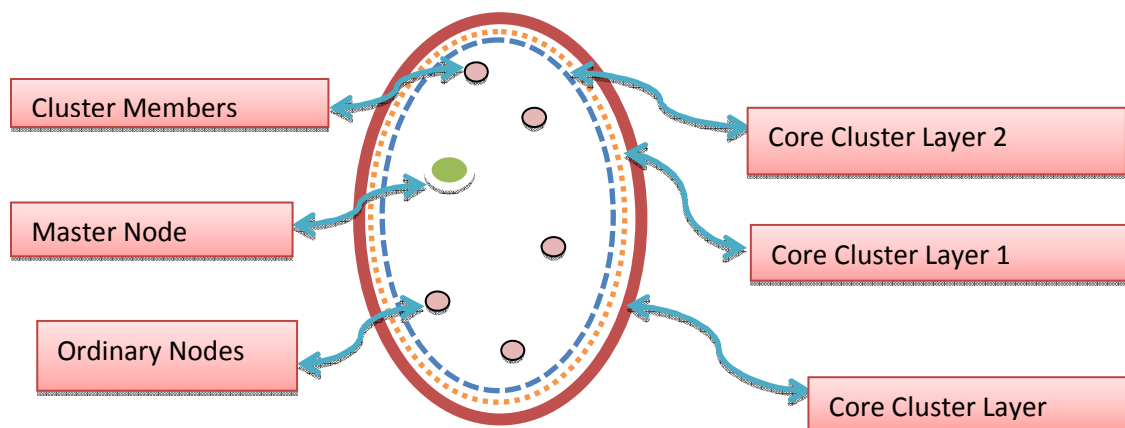


FIGURE 2: Cluster Layers , Master Node and ordinary nodes in mobile ad hoc network clustering.

MANET can be divided into several overlapped clusters. And Cluster can be divided into three layers. A cluster comprises of a subset of nodes that communicate via their assigned MN. The network is modeled as an undirected graph $G(V, E)$ where V denotes the set of all MHs (vertices) in the MANET and E denotes the set of links or edges (i, j) where $i, j \in V$.

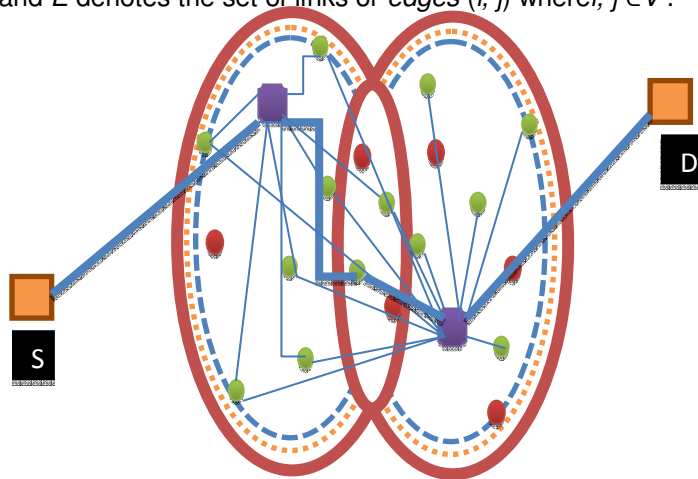


FIGURE 3: Working Model Of New Cluster Layer Manet

In this architecture I decided to assign one MASTER NODE (MN). Which will contain several tables such as:-

- I. Node_Table :- Contain unique ID of Nodes.(NUI)

Node Number	NUI
1	1X00N1
2	1X00N2
3	1X00N3
4	1X00N4
5	1X00N5
6	1X00N6

TABLE 1

II. Node_Table1 :- Contain information of free nodes and busy nodes.



FREE NODE 	BUSY NODE 
1	5
8	11
4	6
7	2
9	10
3	12

TABLE 2

III. Ms_Node_Table :- Contain unique IDs of every Master Node with their Cluster information.(MNUI)

IV.

Cluster	MNUI
CI1	Ms000X0120MN00001x1
CI2	Ms000X0120MN00001x2
CI3	Ms000X0120MN00001x3
CI4	Ms000X0120MN00001x4

TABLE 3

- V. TNUI_Node_Table :- Contain time being assigned IDs for every Nodes which will change every short period of time by Master Node.

Node NUI	Node TNUI
1X00N1	TN000XOU00N0X1
1X00N2	TN000XOU00N0X2
1X00N3	TN000XOU00N0X3
1X00N4	TN000XOU00N0X4

TABLE 4

- VI. TMNUI_Node_Table :- Contain time being assigned IDs for every Master Node which will be changed by Master Node every short of time and share with every Nodes.

MNUI	TMNUI
Ms000X0120MN00001x1	Ms000X01T20MN0001x1
Ms000X0120MN00001x2	Ms000X01T20MN0001x2
Ms000X0120MN00001x3	Ms000X01T20MN0001x3
Ms000X0120MN00001x4	Ms000X01T20MN0001x4

TABLE 5

- VII. CI_Node_Table :- Contain information of all Nodes available at Clusters range include common Cluster nodes. Common Nodes will contain by both cluster table. This table will contain by Master Nodes and all Nodes.

CL1	CL2	CL3	CL4	CL5
Nodes Available in Cluster 1	Nodes Available in Cluster 2	Nodes Available in Cluster 3	Nodes Available in Cluster 4	Nodes Available in Cluster 5

TABLE 6

VIII.Defaulter_Node_Table :- Contain defaulter nodes information. When Ordinary Nodes will go out of range again and again that time that Node will consider as defaulter Node and that Node ID will destroy permanently so that if any attacker will try to use those IDs MANET can easily identify and stop attackers.

Cluster	TNUI
1	TNOOXOU00N0X1
5	TNOOXOU00N0X3
8	TNOOXOU00N0X4

TABLE 7

IX. Routing_Table:- Contain information of entire routing tables by which route our packets are moving.

R o u t e	Source Node TNUI& Destination Node TNUI	Used TMNUI	U s e d T N U I	Gat ewa y TNU I	Use d Rout e TNU I
1	x,y,z,...	x,y,z,...	x, y, z,	x,y,z ,...	x,y,z ,...
2	x,y,z,...	x,y,z,...	x, y, z,	x,y,z ,...	x,y,z ,...

TABLE 8

Cluster Characteristics

- X. All Clusters are having limited range and depending on Master Nodes range.
- XI. Clusters can collapse with each other.
- XII. Collapsed area will call common Cluster.
- XIII. Cluster will maintain three separate layer to secure Master Node position.
- XIV. Those three layer will called as (1) Core Layer (2) Core Cluster Layer 1(3) Core Cluster Layer 2.

Master Node Characteristics

1. All Master Nodes will be dynamic.
2. Every Cluster should have one Master node.
3. All Master nodes should maintain all database tables.
4. Only Master Nodes can change Time Being assigned Unique Id for Nodes and Master Nodes.
5. After changing of TNUI of every nodes and own every master nodes will share all changed new updated database.
6. After changing of TMNUI Master Nodes will share the update with every nodes and every master nodes of each cluster.
7. After every updation Master Nodes will verify with all shared Nodes and Master Nodes.
8. If any Nodes cross cluster layer 2 instant one message will go to Master nodes available on that Cluster.
9. Master Node will send one MSG to that Nodes and inform him that he is going out of range.
10. If that Node will not listen and continuing to go out of Cluster Layer 1 then again Master Node will send him warning that not to move out of rang otherwise your will become defaulter Node.
11. After crossing of Core Cluster Layer MN will send a request to all MN that any node has entered in your area.
12. If that Node entered in other Cluster area then that's Node responsibility to update himself with new Clusters MN.
13. If all MN will reply that no updating that time that node will become defaulter and that will go to Defaulter_Node_Table.

Conclusion and Future Work

As I proposed in this paper about new architecture of MANET and Cluster layers and their (MN & Clusters) characteristics. By using of Cluster layer architecture we can save our MANER from all attackers and upcoming malicious drafts. This solution gives us an opportunity to identify attacker's type and nodes position. By using of this architecture we can identify how many nodes are free and busy in our cluster and by suing of nodes position we can identify which node node going out of range and which one is new node in our cluster.

After acceptance of this proposed design pattern. I am going to explain new proposed algorithm with their real time simulation for this design and going to explain how this new design is better than existing model by comparing all drawbacks of existing model of MANET. In this paper I have added 5 new table and future the number of tables can be increase as per the requirement.

In my next work is to simulate and test this model with all existing attackers and secure MANET.

REFREANCES

- [1] T. Clausen, P. Jacquet, "Optimized Link State Routing Protocol", Internet Draft, draft-ietf-manet-olsr-11.txt, July 2003.
- [2] X. Hong, K. Xu, M. Gerla, "Scalable Routing Protocols for Mobile Ad Hoc Networks", IEEE Network, 16(4), pp. 11-21, July-Aug 2002.
- [3] F. Li, S. Z., X. Wang, X. Xue, H. Shen, "Vote-Based Clustering Algorithm in Mobile Ad Hoc Networks", Proc. of International Conference on Networking Technologies for Broadband and Mobile Networks (ICOIN'2004), LNCS Vol. 3090, pp. 13 – 23, 2004.
- [4] D. Gavalas, G. Pantziou, C. Konstantopoulos, B. Mamalis, "An Efficient and Scalable Clustering Algorithm of Wireless Ad Hoc Networks", Proc. of the 1st International Workshop on Distributed Algorithms and Applications for Wireless and Mobile Systems (DAAWMS'2005), in press.

- [5] C. R. Li, M. Gerla, "Adaptive Clustering for Mobile Wireless Networks", IEEE Journal of Selected Areas in Communications, 15(7), pp. 1265-1275, 1997.
- [6] C. Perkins, "Ad Hoc Networking", Addison-Wesley, 2001.
- [7] A. Qayyum, L. Viennot A. Laouiti, "Multipoint relaying: Anefficient technique for flooding in mobile wireless networks", Proc. of the 35th Annual Hawaii International Conference on System Sciences (HICSS'2001), 2001.
- [8] S. Sivavakeesar, G. Pavlou, A. Liotta, "Stable Clustering Through Mobility Prediction for Large-Scale Multihop Ad Hoc Networks", Proc. of the IEEE Wireless Communications and Networking Conference (WCNC'2004), IEEE, March 2004.
- [9] Y. Yi, M. Gerla, T. Kwon, "Efficient Flooding in Ad hoc Networks: a Comparative Performance Study", Proceedings of the IEEE International Conference on Communications (ICC'2003), 2003.
- [10] Y. Yi, M. Gerla, T. Kwon, "Passive Clustering (PC) in Ad Hoc Networks", Internet Draft, draft-ietf-yi-manet-pac-00.txt, 2001.
- [11] J. Yu, P. Chong, "A Survey of Clustering Schemes for Mobile AdHoc Networks", IEEE Communications Surveys, 7(1), pp. 32-48, March 2005.

Quality and Distortion Evaluation of Audio Signal by Spectrum

Er. Niranjan Singh

*M-Tech (Computer science and engineering)
RGPV
Bhopal, 462003, India*

enggniranjan@gmail.com

Dr. Bhupendra Verma

*Director (PG courses) (Computer science and engineering)
RGPV
Bhopal, 462021, India*

bk_verma3@rediffmail.com

Abstract

Information hiding in digital audio can be used for such diverse applications as proof of ownership, authentication, integrity, secret communication, broadcast monitoring and event annotation. To achieve secure and undetectable communication, stegano-objects, and documents containing a secret message, should be indistinguishable from cover-objects, and show that documents not containing any secret message. In this respect, Steganalysis is the set of techniques that aim to distinguish between cover-objects and stegano-objects [1]. A cover audio object can be converted into a stegano-audio object via steganographic methods. In this paper we present statistical method to detect the presence of hidden messages in audio signals. The basic idea is that, the distribution of various statistical distance measures, calculated on cover audio signals and on stegano-audio signals vis-à-vis their de-noised versions, are statistically different. A distortion metric based on Signal spectrum was designed specifically to detect modifications and additions to audio media. We used the Signal spectrum to measure the distortion. The distortion measurement was obtained at various wavelet decomposition levels from which we derived high-order statistics as features for a classifier to determine the presence of hidden information in an audio signal. This paper looking at evidence in a criminal case probably has no reason to alter any evidence files. However, it is part of an ongoing terrorist surveillance might well want to disrupt the hidden information, even if it cannot be recovered.

Keywords: Component Steganalysis, Watermarking, Audio Quality Measures, Distortion Metric

1. INTRODUCTION

Information hiding in digital audio can be used for such diverse applications as proof of ownership, authentication, integrity, secret communication, broadcast monitoring and event annotation. There are two well-known special cases of information hiding – digital watermarking and steganography. In digital watermarking, the embedded signal depends on a secret key as the threat model includes a malicious adversary who will try to remove or invalidate the watermark. Thus the methods are denominated as “active Steganalysis” since the adversary can actively manipulate the object to alter, invalidate, and obfuscate etc. the watermark. Note that in a digital watermarking application, we always assume that the adversary knows that the content is watermarked and also knows the exact technique that is being used for watermarking. The rapid proliferation of Voice over Internet Protocol (VoIP) and other Peer-to-Peer (P2P) audio services provide vast opportunities for covert communications. By slightly altering the binary sequence of the audio samples with existing steganography tools [2], covert communication channels may be relatively easy to establish. Moreover, the inherent redundancy in the audio signal and its transient and unpredictable characteristics imply a high hidden capacity. This is further aided by the fact that the human ear is insensitive to small distortions in the audio signal.

Steganalysis itself can be implemented in either a passive warden or active warden style [3]. A passive warden simply examines the message and tries to determine if it potentially contains a hidden message. If it appears that it does, then the document is stopped; otherwise it will go through. An active warden, on the other hand, can alter messages deliberately, even though there may not see any trace of a hidden message [4], in order to foil any secret communication that can nevertheless be occurring. It should be noted that although there has been quite some effort in the Steganalysis of digital images Steganalysis of digital audio is relatively unexplored. The steganalyzer can be constructed as a “distortion meter” between the test signal and the estimated original signal, \hat{x} , using again de-noising.

For this purpose, one can use various “audio signal quality measures [5]” to monitor the extent of steganographic distortion. Here, we implicitly assume that the distance between a smooth signal and its de-noised version is less than the distance between a noisy signal and its de-noised version [6, 7]. The implicit assumption is that any embedding effort will render the signal less predictable and smooth. The perturbations, due to the presence of embedding, translate to the feature space, where the “audio quality features” plot in different parts of the feature space between the marked and non-marked signals. An alternate way to sense the presence of “marking” would be to monitor the change in the predictability of a signal, temporally and/or across scales.

2. PROPOSED TECHNIQUE

It has been observed that filtering an audio signal with no Watermark message causes changes in the quality metrics differently than that of an embedded audio signal [8, 9, 10, 11]. A generic watermarking scheme is shown in Figure 1 (a). The inputs consist of the watermark information, the audio input data and the watermark embedding keys to ensure security. A generic detection process is presented in Figure 1 (b). Depending on the method the original data and watermark may be used in recovery process and also depending on the method the output of recovery may be the watermark itself or some confidence measure [12], which says how likely it is for the given watermark at the input to be present in the data under processing.

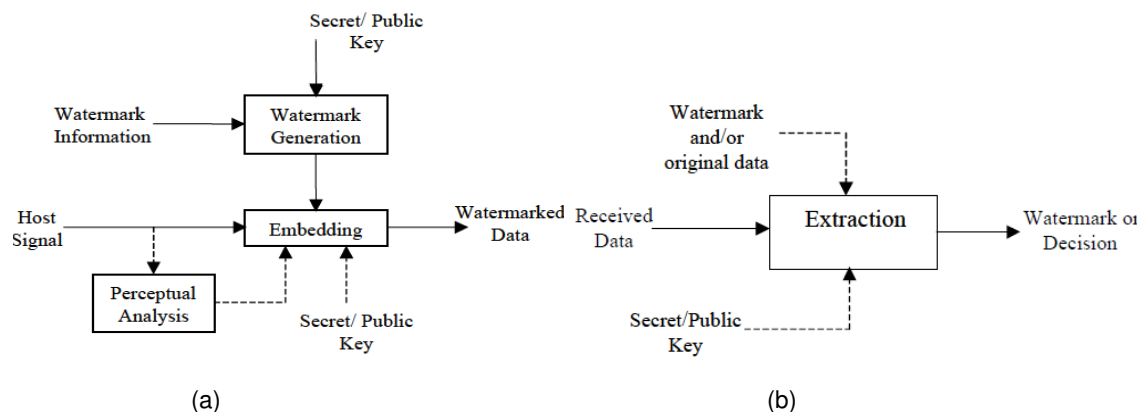


FIGURE 1: Generic watermarking scheme, (a) embedding, (b) recovery

1. Audibility

In order to evaluate the audibility performance of proposed method we have used a perceptual audio quality measure based on psychoacoustic sound representation (PAQM) which have high correlation with subjective measure mean opinion score (MOS) [13]. The ITU has standardized the PAQM as an objective audio quality measure system. In subjective measures the subjects are presented with original and distorted objects (in our case watermarked objects) and give scores for each audio object

2. Robustness

In the robustness experiments, the watermarked object are subjected to a variety of potential signal distortions and watermark detect statistics are computed. The Audio Stir mark [14] Benchmark has been used to simulate the signal attacks. The Benchmark has about 50 distinct distortion tools. The distortion descriptions and the parameters used are presented in Table 1. Some of the attacks such as noise addition, brumm addition and extra-stereo attacks are applied with different strengths

Attack Name	Description / Parameter
Add Brumm	Adds buzz or sinus tone to the sound / 100 to 10100
Add Dyn Noise	Add dynamic white noise to the samples / 20%
AddFFT Noise	Add white noise to the samples in the FFT room /3000
Add Noise	Adds white noise to the samples. The value "0" adds nothing and "32768" the absolute distorted maximum / 100 to 1100
Add Sinus	Adds a sinus signal to the sound file. With it, you can insert a disturb signal in the frequency band where the watermark is located / at 900Hz
Amplify	Changes the loudness of the audio file / 50 (divide the magnitude by 2)
Bass Boost	Increases the bass of the sound file.
Compressor	This works like a compressor. You can increase or decrease the loudness of quietly passages / 2.1
Copy Sample	Is like Flipp Sample but this evaluation process copies the samples between the samples / parameters are the same as Flipp-Sample
Cut Samples	Removes Remove Number (7) of samples ever Remove period (100)
Echo.	Adds an echo to the sound file
Exchange	Swaps two sequent samples for all samples
Extra Stereo	Increases the stereo part of the file / 30,50,70
FFT_HL Pass	Is like the RC-High- and RC-Low-Pass, but now in FFT room / 200 and 9000 Hz.
FFT_Invert.	Inverts all samples (real and imaginary part) in the FFT room
FFT_Real Reverse	Reverses only the real part from the FFT.
FFT_Stat1	Statistical evaluation in FFT room.
FFT_Test I	will do some tests in FFT domain.
Flipp Sample	Swaps samples inside the sound file periodically / number of flipped sample is 2000
Invert	Inverts all samples in the audio file.
LSBZero	Sets all least significant bit's (LSB) to "0" (zero).
Normalize	Normalize the amplify to the maximum value.
Nothing	This process does nothing with the audio file. The watermark should be retrieved. If not, the watermarking algorithm can be a snake oil!
Pitch Scale	Makes a pitch scale
RC-High Pass	Simulates a high pass filter build with a resistance (R) and a capacitor (C).
RC-Low Pass	Simulates a low pass filter like RC-High-Pass.

Re-sampling	Changes the sample rate of the sound file / half the sampling rate
Smooth	This smoothes the samples.
Smooth2	Is like Smooth, but the neighbor samples are voted a little bit different.
Stat1	Statistical distortion 1
Stat2	Statistical distortion 2
Voice Remove	Is the opposite to Extra-Stereo. This removes the mono part of the file (mostly where the voice is). If the file does not have a stereo part (expl. only mono) then everything will be removed.
Zero Cross	This is like a limiter. If the sample value is less the given value (threshold), all samples are set to zero / 1000
Zero Length	If a sample value is exactly "0" (zero) then it inserts more samples with the value "0" (zero) / 10 samples are included
Zero Remove	This removes all samples where the value is "0" (zero).

TABLE 1: Attacks applied by Audio Stir mark Benchmark tool

3. Comparison Tests

We have conducted some more experiments in order to compare the proposed approach with a DCT based audio watermarking technique [15], which is one of the leading non-oblivious watermarking techniques proposed in the literature. In this technique, the watermark is embedded by modifying the largest coefficients of DCT (excluding DC term). Their conjecture is that, these components are heuristically perceptually more significant than others. In the decoding phase, they use the original cover data, extract it from the received object, and compare the residual with the original watermark and make a decision

4. Regression Analysis Classifier

In the design of a regression classifier, we regress the distance measure scores to, respectively, -1 and 1, depending upon whether the audio did not or did contain a hidden message. In the test phase, the incoming audio signal is de-noised and the selected quality metrics are calculated, then the distance measure is obtained by using the predicted regression coefficients [16]. If the output exceeds the threshold 0, then the decision is that the audio contains message, otherwise the decision is that the audio does not contain any message

5. Algorithm

The proposed feature calculation algorithm proceeds along the following steps:

- Step 1. For a given audio file $x(n)$, apply wavelet de-noising to get its de-noised version $\tilde{x}(n)$.
- Step 2. Partition the signal $x(n)$ and $\tilde{x}(n)$ with pre-defined segment length M . Calculate the wavelet coefficients \hat{C}_m^p and C_m^p at different levels p for segment m .
- Step 3. For each wavelet decomposition level p , calculate the distortion measure H_m^p .
- Step 4. Set up the feature vector V^p by calculating the moments of D^p for each wavelet decomposition level p .
- Step 5. Set up the high-dimensional feature V .
- Step 6. Generate signal spectrums of $x(n)$ H_m^p .

3. EXPERIMENTAL RESULT

In the experiments, the signal, sampled at 16 kHz, is segmented into 25 ms frames, which are weighted with a hamming window. There exists 50% overlap between segments. The tests are run for three sets of data, namely, speech, pure instrumental audio and song records. There is overall 156 speech records, 112 music excerpts and 86 instrumental records used. The speech segments have durations of three to four seconds, and recorded in acoustically shielded medium. In the audio repertoire, three different instrumental sources and three different song records are used.

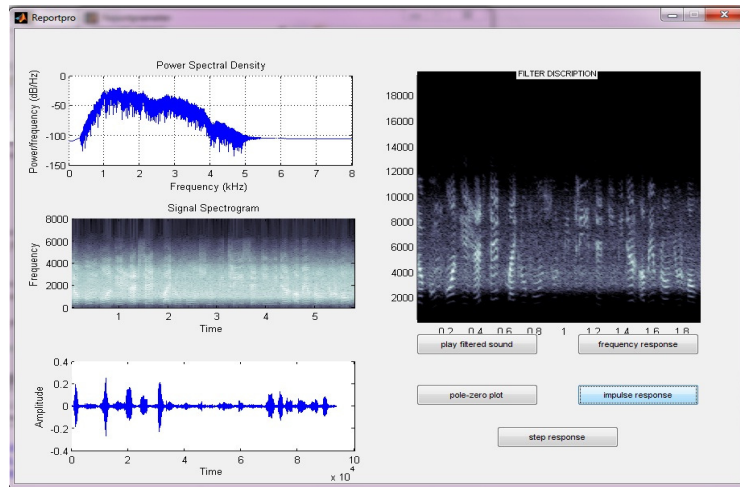


FIGURE 2: A complete report plot of original and plain audio file

The audio records (songs and instrumentals) are separated into 10-second long segments and processed as individual objects. That is for speed up the experiments because there are lots of experiments to do. We have conducted the experiments with different watermarking rates (8, 16 and 32 bits per second) on the three types of data types, which are speech, pure instrumental, and music. The attacks are applied one at a time, in other words the combined attacks are not considered.

In Figure 3, the impacts of some attacks on original wave sound are presented. In the figure 3 the attacks can be deduced from the figure that the attacks generate visible distortions and the distortions on the wave shapes can easily be observed.

We are take a plain audio file and check it signal spectrogram, frequency response, pole-zero, impulse response and step response. We also plot graph between Time and amplitude. We are not get any mixed sound or distraction.

First we have taken original audio file without any hidden message. And apply different method to check hidden file. This section will show some examples of audio file that can hide the message. But we detect the presence of steganography programs, detect suspect carrier files, and disrupt stegano-graphically hidden messages.

The detection of steganography file on a suspect computer is important to the subsequent forensic analysis. As the research shows, many steganography detection algorithm work best when there are clues as to the type of steganography that was employed in the first place. Finding steganography file on a computer would give rise to the suspicion that there are actually steganography files with hidden messages on the suspect computer.

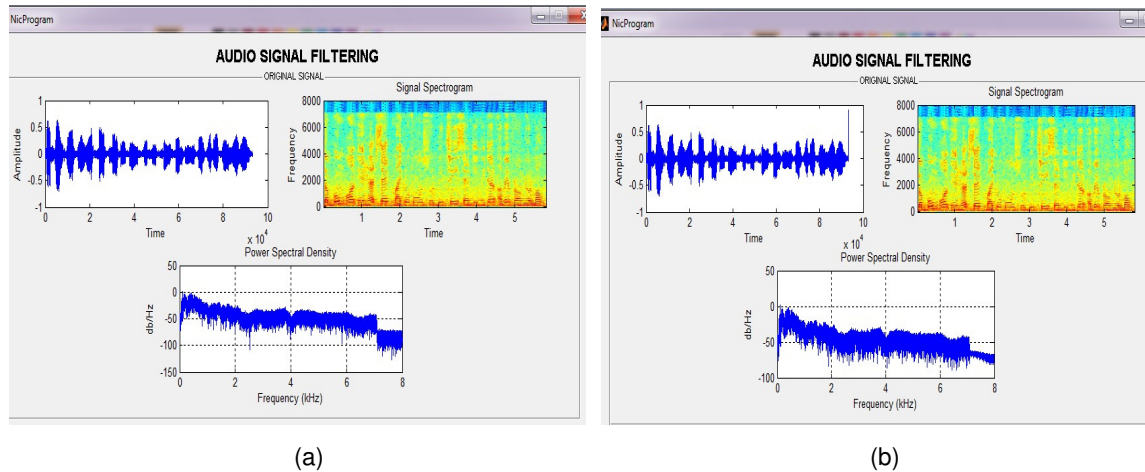


FIGURE 3: The original record and attacked versions, (a) original, (b) Add Noise attack

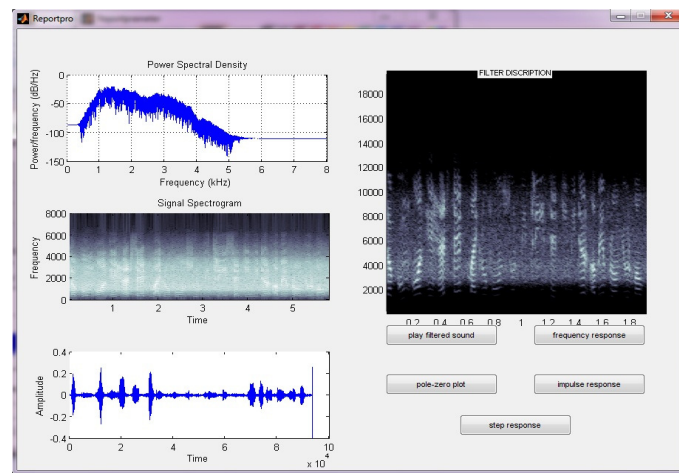


FIGURE 4: A complete report plot of audio file with hidden message

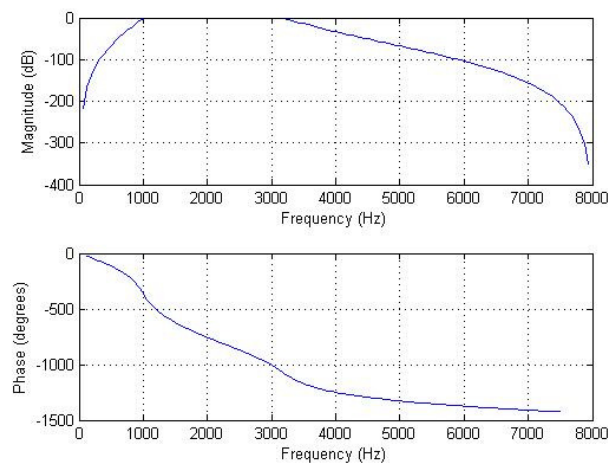


FIGURE 5: A frequency response graph plot of original and plain audio file

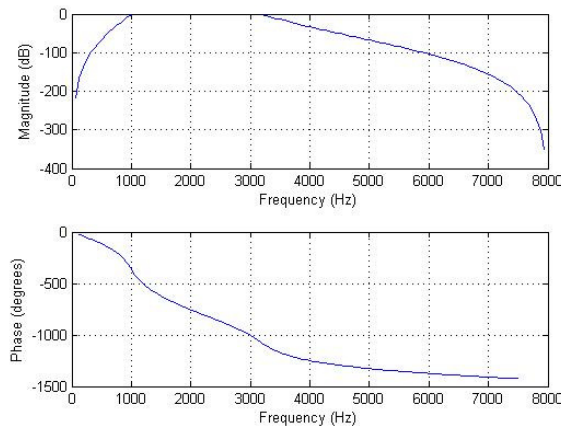


FIGURE 6: A graph plot of Frequency Response of audio file with hidden message

This paper has been tested on 10 audio file. Our steganography algorithm was able to detect the presence of hidden messages with 65 percent accuracy with a false-positive rate less than 0.001 percent.

4. CONCLUSION

A distortion metric based on Signal spectrum was designed specifically to detect modifications and additions to audio media. We used the Signal spectrum to measure the distortion. The distortion measurement was obtained at various wavelet decomposition levels from which we derived high-order statistics as features for a classifier to determine the presence of hidden information in an audio signal.

In this study, an audio Steganalysis technique is proposed and tested. The objective audio quality measures, giving clues to the presence of hidden messages, are searched thoroughly. The distortion measurement was obtained at various wavelet decomposition levels from which we derived high-order statistics as features for a classifier to determine the presence of hidden information in an audio signal.

In this paper, an audio Steganalysis technique is proposed and tested. The audio Steganalysis algorithms exploit the variations in the characteristic features of the audio signal as a result of message embedding. Audio Steganalysis algorithms that detect the discontinuities in phase (as a result of phase coding), variations in the amplitude (as a result of Echo hiding) and the changes in the perceptual and non-perceptual audio quality metrics as a result of message embedding have been proposed. In summary, each carrier media has its own special attributes and reacts differently when a message is embedded in it. Therefore, the Steganalysis algorithms have also been developed in a manner specific to the target stegano file and the algorithms developed for one cover media are generally not effective for a different media.

5. REFERENCES

- [1] Er. Niranjana Singh and Dr. Bhupendra Verma, "Steganalysis of Audio Signals, Audio Quality and Distortion Measures" *ICCET 2010 - International Conference on Computer Engineering and Technology* CET6011.0.607 ISBN No 978-81-920748-1-8.
- [2] Johnson, N.F., S. Jajodia, "Steganalysis of images created using current steganography software", in David Aucsmith (Ed.): *Information Hiding, LNCS 1525*, pp. 32-47. Springer-Verlag Berlin Heidelberg, 1998.
- [3] Westfeld, A. Pfitzmann, "Attacks on steganographic systems", in *Information Hiding, LNCS 1768*, pp. 61-66, Springer-Verlag Heidelberg, 1999.

- [4] Bender, W., D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding", *IBM Systems Journal*, vol. 35, no: 3&4, pp. 313-336, 1996.
- [5] Kitawaki, N., H. Nagabuchi, and K. Itoh, "Objective quality evaluation for low-bit-rate speech coding systems," *IEEE J. Select. Areas Commun.*, vol. 6, pp. 242-248, Feb. 1988.
- [6] Coifman, R. R., and D. L. Donoho, "Translation-invariant denoising," in *Wavelets and Statistics A. Antoniadis and G. Oppenheim, Eds, Springer-Verlag lecture notes*, San Diego, 1995.
- [7] Yang, W, M. Dixon, and R. Yantorno, "A modified bark spectral distortion measure which uses noise masking threshold," *IEEE Speech Coding Workshop*, pp. 55-56, Pocono Manor, 1997.
- [8] Voloshynovskiy, S., S. Pereira, V. Iqbal, and T. Pun, "Attack modeling: towards a second generation watermarking benchmark", *Signal Processing*, vol. 81, pp. 1177-1214, 2001.
- [9] Swanson, M. D., Bin Zhu, Ahmed H. Tewfik, and Laurence Boney, "Robust Audio Watermarking Using Perceptual Masking", *Signal Processing* 66, pp. 337-355, 1998.
- [10] Bassia, P. and I. Pitas, "Robust Audio Watermarking in the Time Domain", in *9th European Signal Processing Conference (EUSIPCO'98), Island of Rhodes, Greece*, 8–11 Sept. 1998.
- [11] Chen, B. and G. W. Wornell, "Quantization Index Modulation: a Class of Probably Good Methods for Digital Watermarking and Information Embedding", *IEEE Trans. on Information Theory*, Vol. 47, No. 4, pp. 1423-1443, May 2001.
- [12] Wang, S., A. Sekey, and A. Gersho, "An objective measure for predicting subjective quality of speech coders", *IEEE J. Select. Areas Commun.*, vol. 10, pp. 819-829, June 1992.
- [13] Beerends, J. G. and J. A. Stemerdink, "A Perceptual Audio Quality Measure Based on a Psychoacoustics Sound Representation," *J. Audio Eng. Soc.*, Vol. 40, pp.63- 978, Dec. 1992.
- [14] StirMark, <http://amslmb.cs.unimagdeburg.de/smfa/main.asp>, 2004.
- [15] Cox, I., J. Kilian, F. T. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia", *IEEE Trans. on Image Process.*, Vol. 6, No. 12, pp. 1673-1687, Dec 1997.
- [16] Voran, S., "Objective estimation of perceived speech quality, part I: development of the measuring normalizing block technique", *IEEE Transactions on Speech and Audio Processing*, in Press, 1999.

INSTRUCTIONS TO CONTRIBUTORS

The *International Journal of Computer Science and Security (IJCSS)* is a refereed online journal which is a forum for publication of current research in computer science and computer security technologies. It considers any material dealing primarily with the technological aspects of computer science and computer security. The journal is targeted to be read by academics, scholars, advanced students, practitioners, and those seeking an update on current experience and future prospects in relation to all aspects computer science in general but specific to computer security themes. Subjects covered include: access control, computer security, cryptography, communications and data security, databases, electronic commerce, multimedia, bioinformatics, signal processing and image processing etc.

To build its International reputation, we are disseminating the publication information through Google Books, Google Scholar, Directory of Open Access Journals (DOAJ), Open J Gate, ScientificCommons, Docstoc and many more. Our International Editors are working on establishing ISI listing and a good impact factor for IJCSS.

The initial efforts helped to shape the editorial policy and to sharpen the focus of the journal. Starting with volume 6, 2012, IJCSS appears in more focused issues. Besides normal publications, IJCSS intend to organized special issues on more focused topics. Each special issue will have a designated editor (editors) – either member of the editorial board or another recognized specialist in the respective field.

We are open to contributions, proposals for any topic as well as for editors and reviewers. We understand that it is through the effort of volunteers that CSC Journals continues to grow and flourish.

IJCSS LIST OF TOPICS

The realm of International Journal of Computer Science and Security (IJCSS) extends, but not limited, to the following:

- Authentication and authorization models
- Computer Engineering
- Computer Networks
- Cryptography
- Databases
- Image processing
- Operating systems
- Programming languages
- Signal processing
- Theory
- Communications and data security
- Bioinformatics
- Computer graphics
- Computer security
- Data mining
- Electronic commerce
- Object Orientation
- Parallel and distributed processing
- Robotics
- Software engineering

CALL FOR PAPERS

Volume: 6 - Issue: 3 - June 2012

i. Paper Submission: March 31, 2012 **ii. Author Notification:** May 15, 2012

iii. Issue Publication: June 2012

CONTACT INFORMATION

Computer Science Journals Sdn Bhd

B-5-8 Plaza Mont Kiara, Mont Kiara
50480, Kuala Lumpur, MALAYSIA

Phone: 006 03 6207 1607
006 03 2782 6991

Fax: 006 03 6207 1697

Email: cscpress@cscjournals.org

CSC PUBLISHERS © 2011
COMPUTER SCIENCE JOURNALS SDN BHD
M-3-19, PLAZA DAMAS
SRI HARTAMAS
50480, KUALA LUMPUR
MALAYSIA

PHONE: 006 03 6207 1607
006 03 2782 6991

FAX: 006 03 6207 1697
EMAIL: cscpress@cscjournals.org