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

Global Journal of Computer Science and Technology

DISCOVERING THOUGHTS AND INVENTING FUTURE

Technology 12 Reforming Ideas

December 2011

Pinnacles

- Websites Make Sense
- Detection of QRS Complexes
- Sliding Mode Stabilization
- Object Oriented Software

The Volume 11
Issue 20
Version 1.0

ENG

Global Journal of Computer Science and Technology

Global Journal of Computer Science and Technology

Volume 11 Issue 20 (Ver. 1.0)

Open Association of Research Society

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

Global Journals Inc.

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

Sponsors:Global Association of Research

Open Scientific Standards

Publisher's Headquarters office

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

Offset Typesetting

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

Packaging & Continental Dispatching

Global Journals, India

Find a correspondence nodal officer near you

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

eContacts

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

Pricing (Including by Air Parcel Charges):

For Authors:
22 USD (B/W) & 50 USD (Color)
Yearly Subscription (Personal & Institutional):
200 USD (B/W) & 250 USD (Color)

Editorial Board Members (HON.)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Contents of the Volume

Global Journal of Computer Science and Technology
Volume 11 Issue 20 Version 1.0 December 2011
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Does a Citation-Index for Websites Make Sense?

By Martin Ebner, Aldi Alimucaj
Graz University of Technology

Abstract - The usefulness of external references to websites is a crucial factor of web-monitoring. It is of high general interest whether your website is visited by the estimated target group or not. This publication measures the value of references of websites by bringing the idea of citation-index to web-analytic tools. The approach presented is considering the number and quality of actions a visitor of a specific website does and the time s/he spent on this website as well as the previous website the user is coming from. The combination of these three parameters are expressed by formulas and afterwards visualized by different tools. Finally this approach is tested and discussed on an existing project. It can be concluded that this concept is indeed useful to get a deeper insight whether external websites addressing the intended target group or not.

Keywords : *citation-index, ranking websites, web analytics, L3T, piwik.*

GJCST Classification : *H.3.1, H.3.5*

Strictly as per the compliance and regulations of:

Does a Citation-Index for Websites Make Sense?

Martin Ebner [α], Aldi Alimucaj [Ω]

Abstract - The usefulness of external references to websites is a crucial factor of web-monitoring. It is of high general interest whether your website is visited by the estimated target group or not. This publication measures the value of references of websites by bringing the idea of citation-index to web-analytic tools. The approach presented is considering the number and quality of actions a visitor of a specific website does and the time s/he spent on this website as well as the previous website the user is coming from. The combination of these three parameters are expressed by formulas and afterwards visualized by different tools. Finally this approach is tested and discussed on an existing project. It can be concluded that this concept is indeed useful to get a deeper insight whether external websites addressing the intended target group or not.

Keywords : citation-index, ranking websites, web analytics, L3T, piwik.

I. Introduction

Ranking information is one of the most important issues on the web, bearing in mind that there is no good or bad information. By considering this and by knowing some conventional methods such as the *impact factor* for ranking scientific journals, following research question centered our interest: *does a citation-index for websites make sense*? The citation-index works similarly to existing ones but with a special focus on your publication. In other words it does not compare the ranking of your publication to other publications directly it relatively rank how often publications got cited by others. Assigned the same principle for websites a better understanding of referencing websites sharing same interests will occur and deepen the cooperation between websites in order to reach a win-win situation. Unlike the impact factor our citation-index is conceived for the web, so when we speak about other sites we mean websites like ours, which quotes us and adds the link as a reference. This link as we will explain later on is the key for measuring the criteria we set up for the index. Beside the theoretical part we took advantage of the online book called L3T (German textbook about Technology Enhanced Learning) (http://l3t.eu/) to gather the necessary information for making a founded reasoning about the advantages this new index offers.

Author α : Associate Professor at the Institute of Information Systems Computer Media and head of the department Social Learning at Graz University of Technology. E-mail : martin.ebner@tugraz.at

Author Ω : bachelor degree in Computer Science and Economics and is currently finishing his master degree at the University of Technology in Graz. Telephone: 00436802305474

E-mail : aldi.alimucaj@student.tugraz.at

II. Theory

a) Impact Factor

Publishing in scientific journals is very important for the career of a scientist. Choosing the right journal may be crucial for that. Of course there are many journals and they for sure differ in quality which is hard to evaluate. But easy enough, to be found just by doing some bibliographic research and counting the number of citations of articles published in a specific journal. One tool for estimating the relative prestige of journals in a given field is called Journal Citation Reports. JCR is an electronic resource which determines the frequency of citation in total, average as well as the impact factor. The impact factor of a journal is among the criteria considered when candidates are evaluated for promotion [Day, Gastel 2011 p. 30].

Definition

"The impact factor is a measure of the frequency with which the "average article" in a journal has been cited in a particular year or period. The annual JCR *impact factor is a ratio between citations and recent citable items published. Thus, the impact factor of a journal is calculated by dividing the number of current year citations to the source items published in that journal during the previous two years (see Figure 1). "*

A= *total cites in 1992*

B= *1992 cites to articles published in 1990-91 (this is a subset of A)*

C= *number of articles published in 1990-91*

D= *B/C = 1992 impact factor*

Figure 1 : Calculation for journal impact factor (Source: thomsonreuters.com, July 2011)

However this index has its limitations as well, for example it reflects just the impact factor of the whole journal not of individual articles. It is not interdisciplinary and cannot measure journals of different fields. It is obvious that some journals get a higher rating by counting replies to articles that cite the article in question but not counting them as papers. Editors can increase the impact factors of their journals by publishing good polemical articles early in the year [Hartely 2008, p137].

b) Our approach

First the general rules must be set up and combined them together into an equation to form a ranking system. Many of the web analytics systems listed below such as *google* analytics, *piwik* or *open web analytics* are offering all the data which can be tracked from the user (called "raw data") but preview them in no relationship with each other. This was the purpose of our study, to build a system, gather data, analyze them and give conclusions about the possibility of its application. First the web analytics framework is introduced which helps us gathering the necessary data together with a brief introduction to web analytics itself.

c) WEB ANALYTICS

The Web Analytics Association (http://www.webanalyticsassociation.org) has proposed a standard definition for web analytics:

"Web analytics is the objective tracking, collection, measurement, reporting, and analysis of quantitative Internet data to optimize websites and web marketing initiatives." [Kaushik, 2007 p. 6]

Following this definition, collecting data is just one of many functions web analytics can and has to fulfill. The data that are being collected and measured are called clickstream information. Clickstream is foundational data that helps to measure and analyze all kinds of site behavior: visits, visitors, dwell time on site, page views, bounce rate, sources, and more. On base of these data we can analyze the following aspects:

- Brand buzz and opinion tracking
- Customer satisfaction
- Net promoter indices
- Open-ended voice-of-customer analysis
- Visitor engagement
- Stickiness
- Blog-pulse

There are many business models that use web analytics for their selling and/or promoting purposes. Whether it is an online shop, a blog or some highly specialized financial software that runs on the browser.

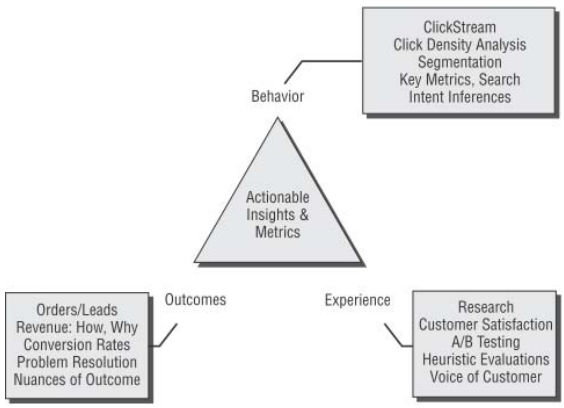


Figure 2 : The trinity diagram. Source: [Kaushik, 2007, p. 18.]

Figure 2 shows the trinity framework; a new way of perceiving web analytics for most efficient data outcome. The goal of behavior analysis is to infer the intent of the website visitors basing on all what we know about them, which is basically clickstream data. The outcome is the result measured in company's predefined objectives, for example if it is an e-commerce website, how many viewers did actually buy the product. But for detailed information analysis and understanding customers' behavior we need profiled web analytics.

i. *Web Analytics Frameworks*

Web analytics tools date back in the early 90s. Since then they have been improving from simple requests counting to highly accurate JavaScript clients, from log files to databases and from text outputs to impressive reporting methods. Besides commercial tools (see Table 1) there are some well implemented open source competitors as well.

COMMERCIAL TOOLS FOR WEB ANALYTICS	
ClickTracks	ClickTracks provides an innovative line of products and hosted services in the field of web site traffic analysis. ClickTracks focuses on presenting meaningful information about user behavior visually in context.
Coremetrics	Coremetrics Web Analytics platform captures and stores all customer and visitor clickstream activity to build LIVE (Lifetime Individual Visitor Experience) profiles that serve as basis for all successful e-business initiatives.
Google Analytics	Google Analytics offers free web analytics services with integrated analysis of Ad-Words and other keyword-based search advertising. Google Analytics bases on Urchin, which Google purchased in 2005.
NedStat	NedStat is a provider of software solutions and services for monitoring websites and reporting on website-visits.
Omniture	SiteCatalyst is a hosted application that offers a comprehensive view of activity on a company's website that includes historical (data warehouse) and real-time analysis as well as reporting. SAS Web Analytics applies SAS Customer Intelligence software to online channels for a complete view on the customer´s interaction.

Visual Sciences	Real-Time Analysis Platform (RTAP) and Suite of applications for to collect, process, analyze and visualize user data for decision making; including Internet sites and services.
WebTrends	WebTrends offers both an on demand service as well as software solutions for measuring campaign performance, search engine marketing, web site conversion and customer retention.

Table 1: Commercial Web Analytics Frameworks. [Source: digitalenterprise.org, July 2011]

Two of the most popular open source web analytics tools are Piwik (http://piwik.org/) and Open Web Analytics (http://www.openwebanalytics.com/). They are both licensed under GPL (*www.gnu.org/copyleft/**gpl**.htm*) and offer nearly the same features and use the same technologies. We implemented our plugin for Piwik which is the framework we are going to discuss in details.

a) Piwik

Piwik is a downloadable, open source (GPL licensed) web analytics software program. As an alternative to services like Google Analytics, Piwik allows you to host your statistics services on your own server, have full ownership and control over the data collected from your visitors. A plugin offers a user interface which is very manageable and easy to use.

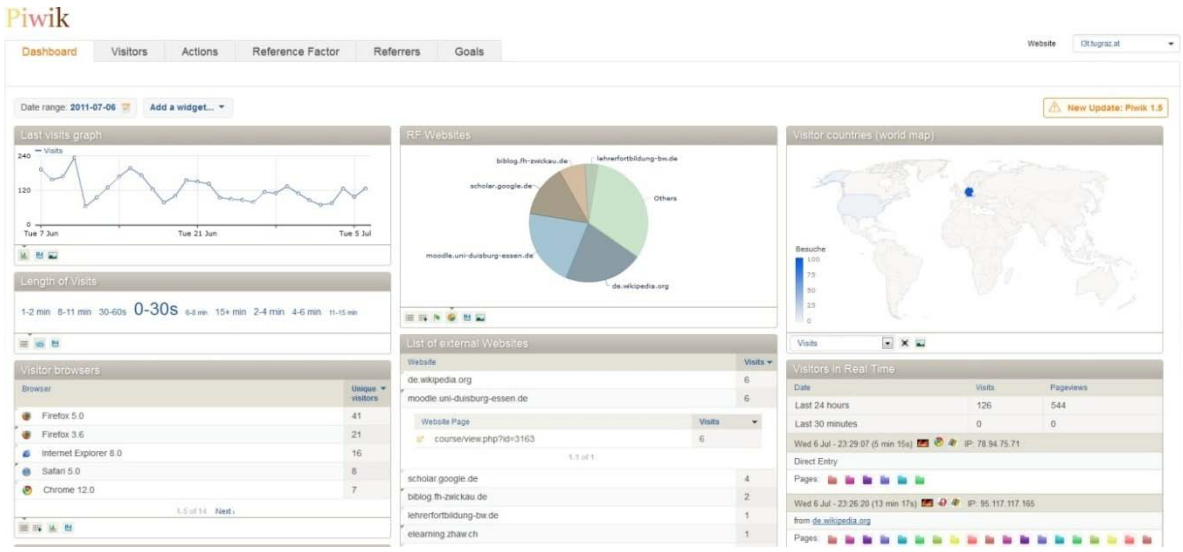


Figure 1 : Piwik user interface. [Source: l3t.tugraz.at Piwik]

Piwik is currently on stable version 1.5 and offers many features such as:

- Real time reports
- Detailed view of your visitors, pages they have visited, goals triggered
- Customizable dashboard
- Dashboard for all websites
- Analytics for ecommerce
- Ecommerce – abandoned carts reporting
- Ecommerce – product and categories reporting
- World map of your visitors
- Automatic tracking of file downloads
- Automatic tracking of clicks on external websites
- Analytics campaign tracking
- More than 800 search engines tracked
- Scheduled email reports (PDF and HTML reports)

[Source: piwik.org, July 2011]

b) Extending Piwik

Besides the user interface Piwik offers a lot of plugins out of the box which cover most of the customer wishes. One of the tasks of this work was to implement our own metrics and incorporate them into Piwik through its plugin interface. First thing to do was to understand Piwik's architecture, how could it be extended and what possibilities does it offer.

c) Technical Implementation

Piwik gathers all its information from a JavaScript client called the Tracker Code which is anchored into the websites that need to be observed. When a user opens the site it sends the initial information to the server containing browser specification, OS platform, language, forwarding link and so on. After that, the client continues polling information about user activities such as click actions or time spent doing something. On the server side Piwik

has a well-developed MVC (Model–view–controller) architecture based on Zend Framework (a PHP optimizing package). The plugins are on the other hand based on the MVC architecture themselves and can be seen as application within the application. From the database we accessed most of the data needed for our new metrics so we didn't need to collect new data from the client.

d) Defining the Metrics

The Tracker Code supplies the forwarding external website´s name which linked the user to the website of our interest. The main idea is to find out those external websites that forward the most fitting target group regarding to the website analyzed. In other words, which external website should we set our focus on and is worth invested more time on? There are different parameters how to measure that: First to find out is how many users are coming from a specific website to ours, second how many actions does the user do on our website and third how long did the user stay on our website. The goal of this research work is to combine these three parameters into one formula and visualize the usefulness of references pointing to our website.

In general Piwik offers the raw data to build a more complex analysis. The first formula to be applied was intended to show the average values of incoming connections for a given time frame. Since we are working on the incoming references from other website we called it "Reference Factor" (RF). The average reference factor formula is shown in Formula 1

$$RFA(w) = \frac{\emptyset V_w}{\emptyset V_a} * \frac{\emptyset A_w}{\emptyset A_a} * 10^6$$

Formula 1 : Reference Factor Average

Furthermore a second formula called the "Multiplicative Reference Factor" (RFM) is needed, because we first define the ratio of the website data with the system and then multiply the data in order to set them in relation with each other.

$$RFA(w) = \frac{V_w}{V_a} * \frac{A_w}{A_a} * 10^2$$

Formula 2 : Reference Factor Multiplicative

The given shortcuts are explained in Table 2.

RFA	Reference Factor Average
RFM	Reference Factor Multiplicative
V	Visit Time
A	Actions
B_w	Visits website
B_a	Visits system
Ø	Average
V_w	Visit Time website
V_a	Visit Time system
A_w	Actions website
A_a	Actions system
W	Website

Table 2 : Formula abbreviations

The average RF is build up with the average values of the reference website (rw) and those from the system. To build an average value it is important to create a rank, which is based on quality instead of quantity. For example we know that website1 is at the first place and has for example 447 visits over 6 months with 2045 actions and 94789 seconds visit time. But measured in average values website2 with 39 visits and 474 actions 42108 visit time has much more interested users who are willing to spend more time on our website. This tells us that website1 users could be misled or were just lurking but website2 users where certain of the content and found just what they were looking for. The RFM is a measurement scale involving visit time and actions, brought together to build a benchmark. A hugh number of users coming from a website is leasing to a high RF-factor of that site, so all popular sites are always at the top. That's why we have to consider both diagrams for an accurate overview. Both formulas were multiplied with factors of 10 to improve their conspicuity.

e) Reporting mechanism

RF Websites

Website	Visits	Actions	Visit Time	RF Multipl	RF Avarage
de.wikipedia.org	460	1913	75795	108	52
www.facebook.com	447	2045	94789	144	74
scholar.google.de	431	1440	69138	74	41
www.weiterbildungsblog.de	339	1459	71861	78	70
twitter.com	287	1035	41093	32	40
www.futurezone.at	194	876	38044	25	68
konzeptblog.joachim-wedekind.de	192	477	19879	7	20
www.medienpaedagogik-praxis.de	188	956	44313	31	92
blog.studiumdigitale.uni-frankfurt.de	178	653	30549	15	48
www.tu-chemnitz.de	155	853	27806	18	76

1-10 of 444 Next ›

Figure 2 : Piwik RF Widget

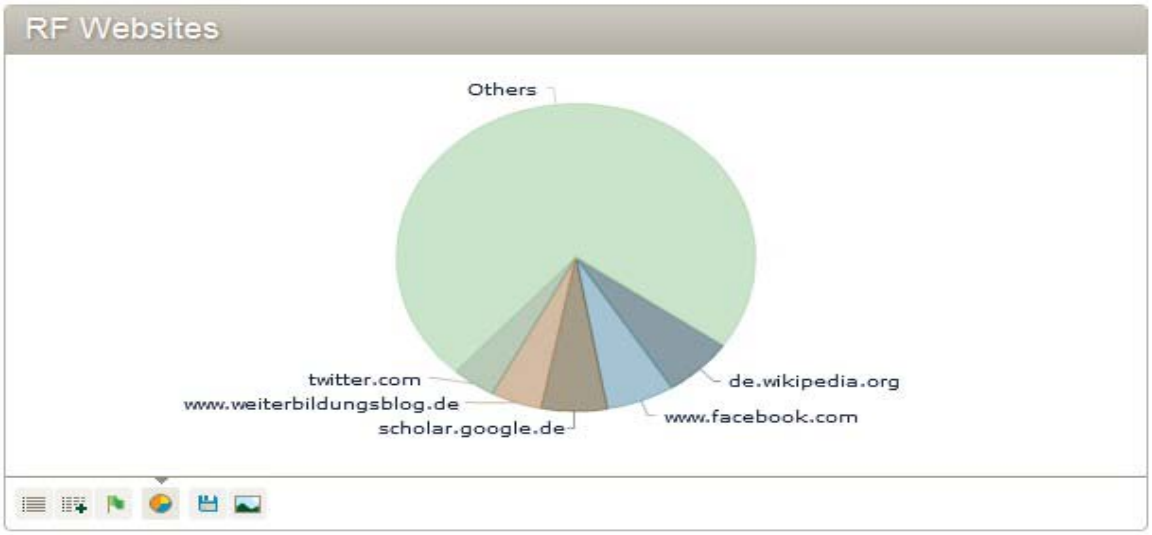


Figure 3 : Widget, Pie Chart View

Figure 3 shows the implemented widget. It builds a table of reference websites and their corresponding number of visits in the first column, the actions, visit time, RFM and RFA. The table can be browsed and sorted. You can even "unfold" one site and take a look at the link where your tracker is placed. You can even build pie charts or vertical bar graphs within the widget. These graphs were satisfactory for one dimensional values. But the RF-s where compound of many values, so it had to be multi-dimensional. To fulfill that we chose a powerful tool (such as MS Excel) to build the graphs out of three dimensions: actions, visit time and visits. The yearly graph looks like figure 5 and 6

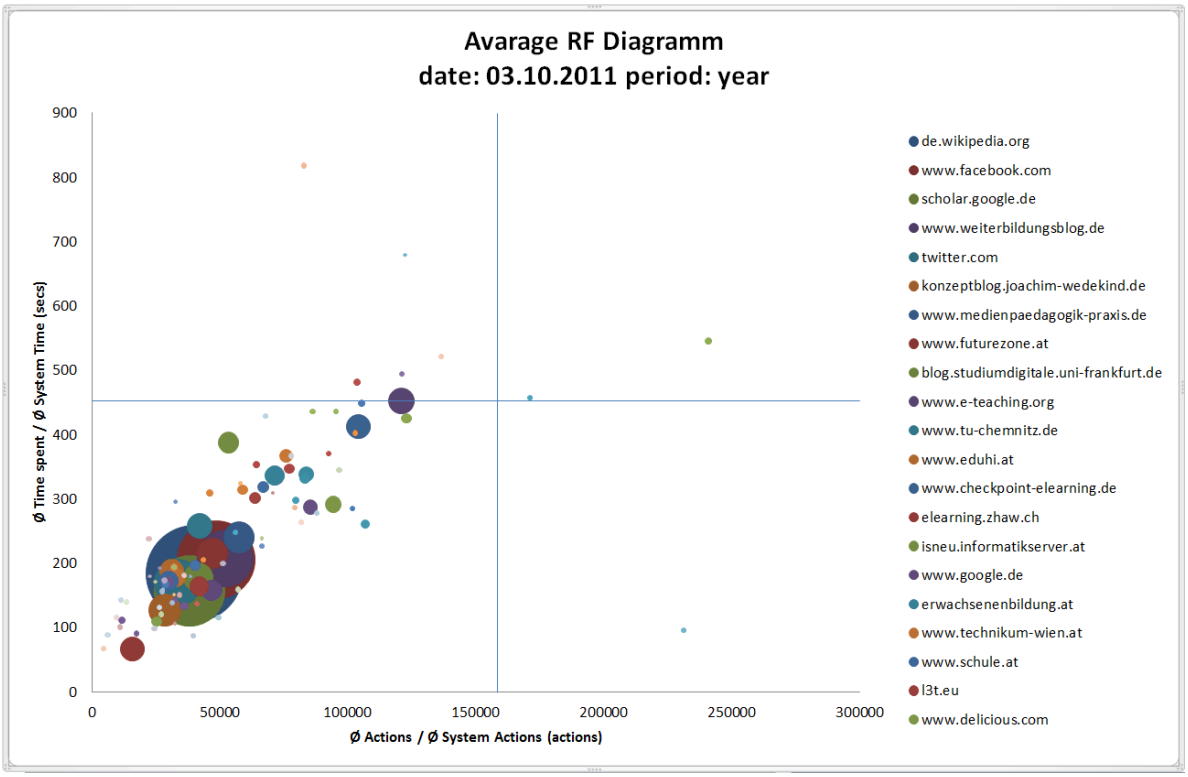


Figure 4 : RFA period: year 2011

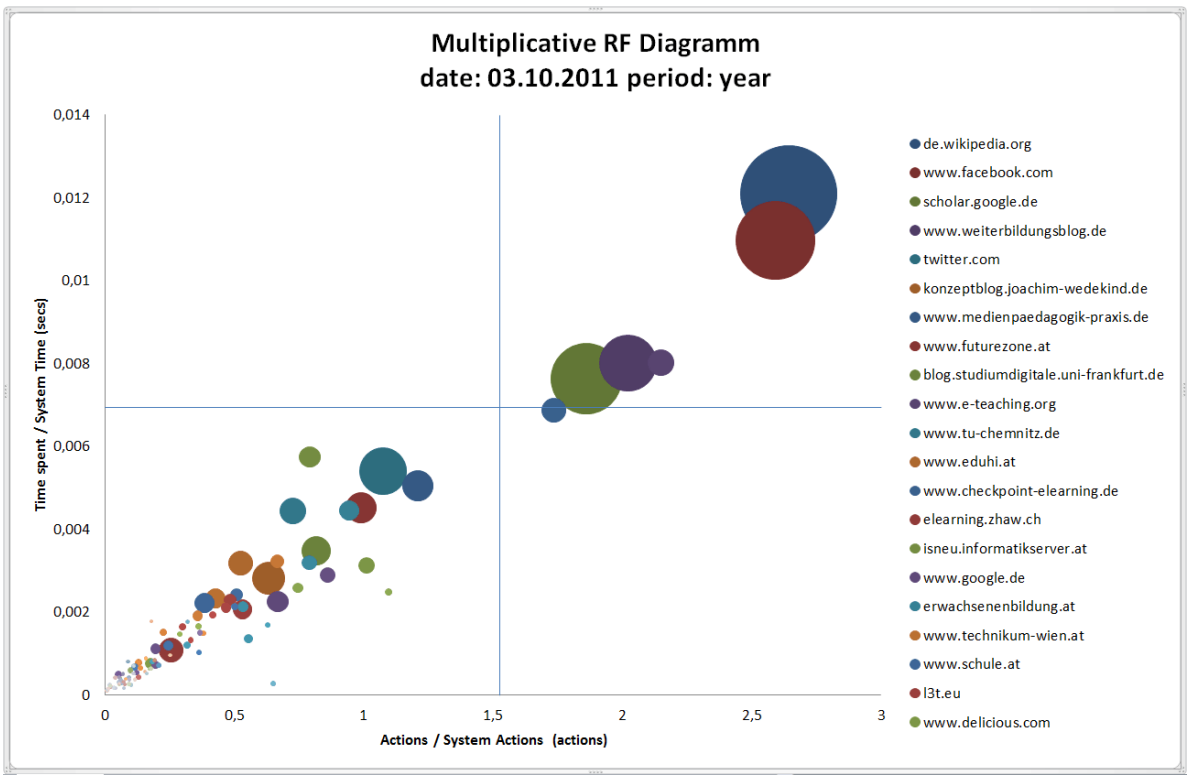


Figure 5 : RFM period: year 2011

Microsoft Excel didn't offer the possibility to build these three dimensional graphs out of the box where the third one is the number of visits represented by the size of the circle. So the only possibility was to write a VBA Macro (Visual Basic for Applications) to build the graph and make the changes we needed. Some items are underrepresented with a smaller circle size as it can be shown so we set a default representation value for all items smaller than three units. The size of the circle is also adapted to the graphs possibilities like i.e. some site with more the 1000 visits cannot have a circle of size 1000 because it would be too big to be rendered. So the biggest value is divided by the scale of max circle size and the rest is adapted to that value. The Macro is tested in MS Excel 2011 and MS Excel 2010 for Mac and Windows.

III. Proof of Concept

Having finished the technical implementation we tested the whole concept and prove its capabilities. The project L3T (http://l3t.eu), which is a German text book on technology enhanced teaching and learning, was chosen for that purpose. The project website of L3T already had piwik installed providing enough data for a good analysis and conclusions. In piwik 1.1 the possibility is given to choose between fixed time periods which are daily, weekly, monthly, or the whole year. Of course, the more data you have to process the more accurate becomes the result. So we started with the annual period which rendered us the table as to be seen in figure 3. On base of this table we can get all the information needed to work out a conclusion. If the same information is needed for example for a presentation then the content could be exported and rendered in MS Excel with the supplied macro. The data used for this table is the same as for the simple ranking. The application of the reference factors offers us two new types of ranking which could be similar but don't have to be the same with the simple ranking.

IV. Discussion

As mentioned before, the tables give an accurate data but lack on fast visual interpretation potential; so for the final discussion the excel graphs will be used. Taking a look at the monthly periods we see that those are more dynamic and could reveal information that is smoothened by larger time periods.

February 2011 was the first monthly information gathering period to start. It can be shown that popular websites like *facebook* very soon attracted a large number of users. But it didn't take long for other sites to contribute to the popularity of the project. In fact for the rest of other monthly reports other profiled websites such as those from universities or Wikipedia were running on top of the RFM list. This is because users who were linked through those websites where more interested in the topic which resulted in longer visit times and more actions within the website. Browsing and long time reading means that the user found what s/he was searching and looking for. In March 2011 for example many other websites were represented as big contributors by reaching the right-top side of the RFM graph having larger circles. Although they generated about the same amount of visits during the time, the quality (actions, visit time) were not always predictable. Wikipedia accords to the yearly period graph at first place in raw data measurement and RFM because it generated a lot of traffic. And a lot of traffic means many users have visited the site and are familiar with its content. They might not have found what they needed but they know what L3T is about and would take a reference on it the next time they would need it. The average RF at the other hand tells us about the interest of the user despite the number of visits. When we look at figure 7 displaying the RFA of June we can see a small dot at the top-right edge of the graph. This dot represents moodle.uni-graz.at at the first place for the monthly ranking. Although *facebook* with a larger circle has the highest number of visits on average it has a smaller RFA quotient than *moodle*. Moodle only forwarded one visitor that month but that person was so interested in the page that s/he spent over 40 minutes reading taking over 20 actions, which are far up from *facebook's* average values.

So finally, it must be pointed out that the best way to tell the importance of a site is, if it ranks in the same area in both diagrams. This is for example the case for www.checkpoint-elearning.de (154 visits, 1330 actions) and www.e-teaching.org (164 visits, 1554 actions) in the yearly diagrams (Figure 5 and Figure 6). They have more or less the same amount of visits and actions with a similar ratio between both. For such sites we can draw the conclusion that quantitative and qualitative values are valid. It can also be stated that if one site is positioned in the upper right area of the diagram than it offers interesting potential in our sense. So for sites occupying the same area we can estimate that the assumption we intended with our research question is true, but for the rest of sites the fluctuation is too big to make a clear distinction.

Besides the monthly reports there are weekly analysis as well. The amount of data is relatively small for drawing conclusions but is sufficiently meaningful for staying up to date with the newest developments regarding your website´s popularity. It can also be used for history purposes to compare relevant changes.

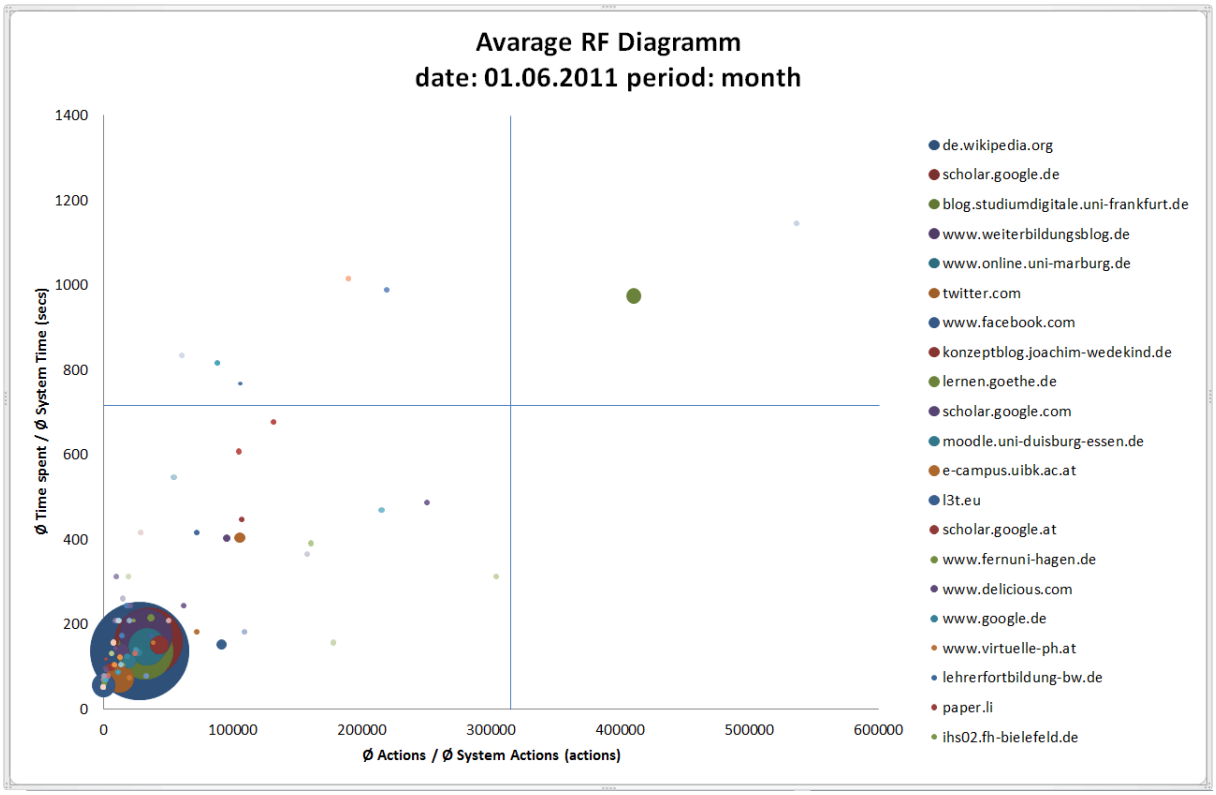


Figure 6 : RFA period: June 2011, month

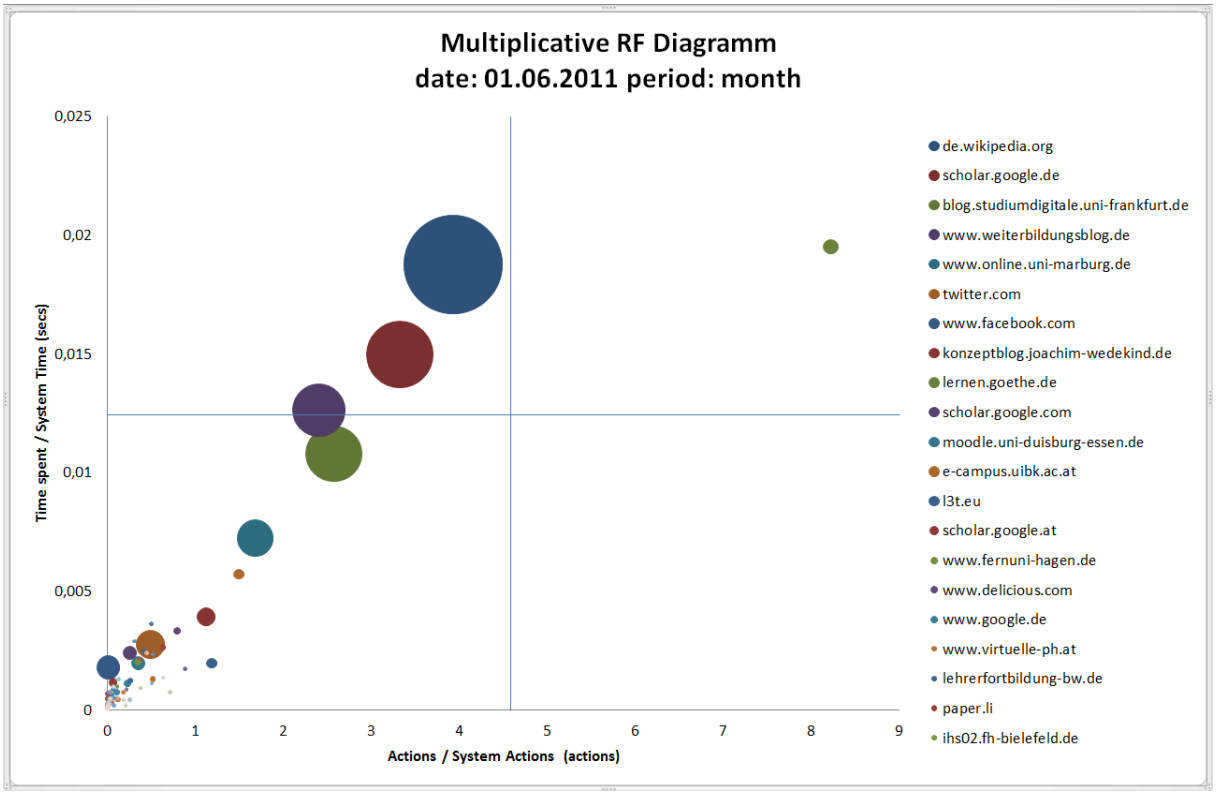


Figure 7 : RFM period: June 2011, month

V. Conclusions

This paper focuses the question whether web analytic tools help us to filter relevant web visitors by interpreting their link history. Therefore two new measurement methods to rank the effectiveness of reference websites were set. Furthermore these methods were implemented into an analytics system and by exporting the data complex graphs could be built with the help of external tools.

On base of such reports two different factors were calculated. The first one was the multiplicative reference factor which results from bringing raw data in connection with each other and the second one was the average reference factor as an outcome of the average values. The tested example (L3T project) has shown that the final diagrams help to interpret the usefulness of external references to the example project website. Web analytics remain a big field for online-business. Ranking systems will become more sophisticated trying to differentiate real chances to separate from the noise of Internet.

References References Referencias

1. A Day, R. (2011) How to Write and Publish a Scientific Paper, Greenwood ABC-CLIE LLC
2. Ebner, M., Schön, S. (2011) *Lehrbuch für Lernen und Lehren mit Technologien, BookOnDemand, Germany, http://l3t.tugraz.at*
3. Hartley, J. (2008) *Academic writing and publishing: a practical guide*, New York, Routledge
4. Kaushik, A. (2007) *Web Analytics*, Wiley Publishing, Inc., Indianapolis, Indiana

Hyperlinks

digitalenterprise.org, Managing the digital enterprise, 12.07.2011 [online] <http://digitalenterprise.org/metrics/metrics.html>
thomsonreuters.com, The Thomson Reuters Impact Factor, 12.07.2011 [online] <http://thomsonreuters.com/products_services/science/free/essays/impact_factor/>
piwik.org, Piwik Open Source Web Analytics, 12.07.2011 [online] < http://piwik.org/features/>

This page is intentionally left blank

Global Journal of Computer Science and Technology
Volume 11 Issue 20 Version 1.0 December 2011
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Detection of QRS Complexes in ECG Signals Based on Empirical Mode Decomposition

By S.A.Taouli, F.Bereksi-Reguig

Dept. of genius electric and electronic, Tlemcen-algeria

Abstract - Arrhythmia is one kind of diseases that gives rise to the death and possibly forms the immedicable danger. The most common cardiac arrhythmia is the ventricular premature beat. The main purpose of this study is to develop an efficient arrhythmia detection algorithm based on Empirical Mode Decomposition (EMD). This algorithm requires the following stages: band-pass Butterworth filters, Empirical Mode Decomposition, sum the first three Intrinsic Functions Mode (IMFs), and take its absolute value, retain the amplitudes, find the position of the maximum. The excellent performance of the algorithm is confirmed by a sensitivity of 99.82 % (204 false negatives) and a positive predictivity of 99.89% (114 false positives) against the MIT-BIH arrhythmia database.

Keywords : *ECG signal, Empirical Mode Decomposition, QRS detection.*

GJCST Classification : *J.3, I.5.4*

Strictly as per the compliance and regulations of:

Detection of QRS Complexes in ECG Signals Based on Empirical Mode Decomposition

S.A.Taouli [α], F.Bereksi-Reguig [Ω]

Abstract - Arrhythmia is one kind of diseases that gives rise to the death and possibly forms the immedicable danger. The most common cardiac arrhythmia is the ventricular premature beat. The main purpose of this study is to develop an efficient arrhythmia detection algorithm based on Empirical Mode Decomposition (EMD). This algorithm requires the following stages: band-pass Butterworth filters, Empirical Mode Decomposition, sum the first three Intrinsic Functions Mode (IMFs), and take its absolute value, retain the amplitudes, find the position of the maximum. The excellent performance of the algorithm is confirmed by a sensitivity of 99.82 % (204 false negatives) and a positive predictivity of 99.89% (114 false positives) against the MIT-BIH arrhythmia database.

Keywords : ECG signal, Empirical Mode Decomposition, QRS detection.

I. Introduction

The Electrocardiogram signal which represents the electric activity of the heart is characterized by a periodic behaviour or quasi periodical. It is typically composed of three called significant waves; P wave, QRS complex and T wave (see fig.1). The detection of the R-peaks and consequently of the QRS complexes in an ECG signal provides information on the heart rate, the conduction velocity, the condition of tissues within the heart as well as various other abnormalities and, thus, it supplies evidence to support the diagnoses of cardiac diseases. For this reason, it has attracted considerable attention over the last three decades.

The algorithms in the relevant bibliography adapt a range of different approaches to yield a procedure leading to the identification of the waves under consideration. These approaches are mainly based on derivative-based techniques [1], [2], *classical* digital filtering [3]–[5], adaptive filtering [6], [7], Tompkins method [8],wavelets [9], Christov's algorithm [10], genetic algorithms [11], Hilbert Transform [12] and zero-crossing-based identification techniques [13].

Author [α] : Teacher and researcher of Biomedical Engineering Research Laboratory, Dept. of genius electric and electronic, Tlemcen-algeria, Telephone: +213 43 28 56 8
E-mail : s_taouli@mail.univ-Tlemcen.dz.
Author [Ω] : Prof. and director of Biomedical Engineering Research Laboratory, E-mail : fethi.bereksi@mail.univ-Tlemcen.dz

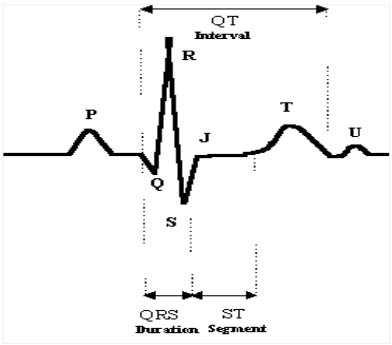


Fig.1 : An ECG bit with typical parameter values.

The Empirical Mode Decomposition (EMD) is a new method designed by N. E. Huang for nonlinear and non-stationary signal analysis [14]. The key part of this method is that any complicated data set can be decomposed into a finite and often small number of Intrinsic Mode Functions (IMFs) that admits well behaved Hilbert transforms. This decomposition method is adaptive, and, therefore, highly efficient. Since the decomposition is based on the local characteristic time scale of the data, it is applicable to nonlinear and non-stationary processes.

The major advantage of the EMD is that the basis functions are derived from the signal itself. Hence, the analysis is adaptive, in contrast to the wavelet method where the basis functions are fixed. In this paper, a detection method based on the EMD approach is proposed. The EMD is based on the sequential extraction of energy associated with various intrinsic time scales of the signal starting from finer temporal scales (high frequency modes) to coarser ones (low frequency modes). The total sum of the IMFs matches the signal very well and therefore ensures completeness.

In this paper, the EMD is used for ECG QRS complex detection. Therefore, the algorithm consists of several steps, namely, band-pass Butterworth filter, decomposition of the ECG signal into a collection of AM–FM components (called Intrinsic Mode Functions (IMF)), sum the first three Intrinsic Functions Mode (IMFs), and take its absolute value, retain the amplitudes, find the position of the maximum.

The proposed algorithm is evaluated by using the ECG MIT–BIH database [15] and is compared to

other methods. As we will show later, very promising results are obtained.

II. Empirical Mode Decomposition

A new non-linear technique, called Empirical Mode Decomposition method, has recently been developed by N.E.Huang *et al* for adaptively representing non-stationary signals as sums of zero mean AM-FM components. EMD is an adaptive, high efficient decomposition with which any complicated signal can be decomposed into a finite number of Intrinsic Mode functions (IMFs). The IMFs represent the oscillatory modes embedded in the signal, hence the name Intrinsic Mode Function.

The starting point of EMD is to consider oscillations in signals at a very local level. It is applicable to non-linear and non-stationary signal such as ECG signal.

An Intrinsic Mode function is a function that satisfies two conditions:

i. The number of extrema and the number of zero crossings must differ by at most 1.
ii. At any point the mean value of the envelope defined by maxima and the envelope defined by minima must be zero.

a) Sifting Process

The basic principle of this method is to identify the intrinsic oscillatory modes by their characteristic time scales in the data empirically and then decompose the data.

A systematic way to extract the IMFS is called the Sifting Process and is described below:

1. Identify all the extrema (maxima and minima) of $x(t)$.
2. Find the upper envelope $e_{\max}(t)$ of the $x(t)$ by passing a natural cubic spline through the maxima, and similarly, find the lower envelope $e_{\min}(t)$ of the minima.
3. Compute the average:

$$m(t) = [e_{\min}(t) + e_{\max}(t)]/2 .$$

4. Get an IMF candidate from $h(t) = x(t) - m(t)$ (extract the detail).
5. Check the weather properties $h_i(t)$ is an IMF. If $h_i(t)$ is not an IMF, repeat the procedure from step 1. If $h_i(t)$ is an IMF, then set $r = x(t) - h_i(t)$ and then $h_i(t) = c_i$.

The procedure from step 1 to step 5 is repeated by sifting the residual signal. The sifting processing ends when the residue r satisfies a predefined stopping criterion. The $h_i(t)$ $(i = 1.....n)$ are being sorted in descending orders of frequency. Finally, the original $x(t)$ can be reconstructed by a linear superposition as given in equation 1.

$$x(t) = \sum_{i=1}^{n} c_i(t) + r_n(t) \tag{1}$$

In practice, after a certain number of iterations, the resulting signals do not carry significant physical information. To prevent this, we go for some boundary conditions. We can stop the sifting process by limiting the normalized standard deviation (SD).

The SD is defined as:

$$SD = \sum_{t=0}^{T} \frac{\left|h_{1(k-1)}(t) - h_{1k}(t)\right|^2}{h_{1(k-1)}^2(t)} \tag{2}$$

The SD is set between 0.2 and 0.3 for proper results [14]. When the SD is smaller than a threshold, the first IMF component from the data, designated as

$$c_1(t) = h_{1k}(t) \tag{3}$$

is obtained. Then $c_1(t)$ is separated from $x(t)$ to obtain

$$x(t) - c_1(t) = r_1(t) \tag{4}$$

Since the residue, $r_1(t)$ still contains information of longer period components, it is treated as the new data and subjected to the same sifting process as described above. This procedure can be repeated on all the subsequent $r_i(t)$, and the result is

$$r_{i-1}(t) - c_i(t) = r_i(t), \quad i = 1,....., N \tag{5}$$

where $r_0(t) = x(t)$ and $c_i(t)$ is the ith IMF of $x(t)$. The whole procedure terminates either when the component $c_n(t)$ or the residue $r_n(t)$ becomes very small or when the residue $r_n(t)$ becomes a monotonic function. Combining equation 4 and equation 5 yields the EMD of the original signal.

The sifting process was applied on an ECG signal to obtain the various IMFs. This has been represented in Fig.2 and Fig.3. The EMD method is a powerful tool for analyzing ECG signal. It is very reliable as the base functions depend on the signal itself. EMD is very adaptive and avoids diffusion and leakage of signal.

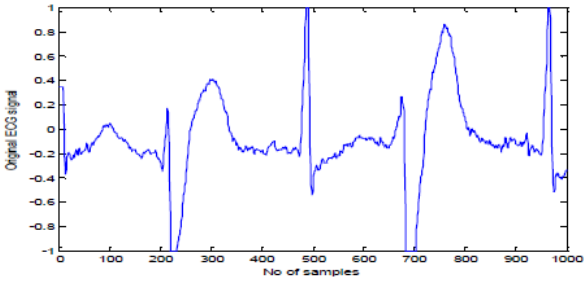


Fig.2 : An ECG signal (201 of MIT-BIH database) containing 1000 samples.

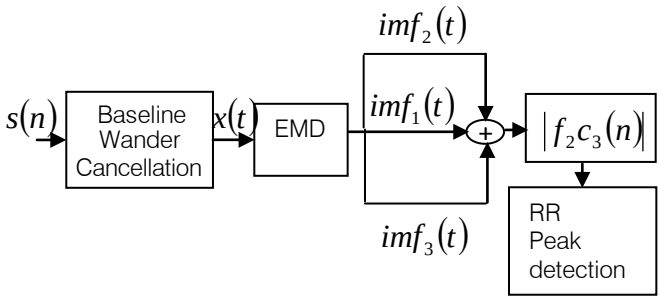


Fig.3 : The various IMFs of the ECG signal.

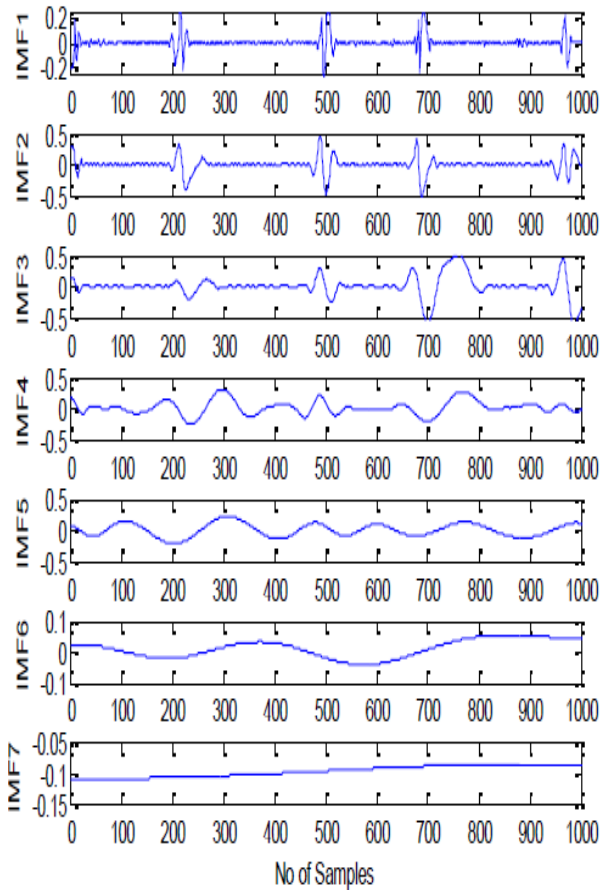


Fig.4 : Block diagram describing the structure of our QRS complex detection.

III. Description of the Implemented Method

Fig.4 illustrates a block diagram describing the structure of our QRS complex detection algorithm. It consists of three blocs: Band-Pass Filter, Empirical Decomposition signal, sum the first three Intrinsic Functions Mode IMFs, take its absolute value, retain the amplitudes, and finally, find the position of the maximum.

a) Preprocessing

We first apply a moving average filter of order 5 to the signal. This filter removes high frequency noise like interspersions and muscle noise. Then, drift suppression is applied to the resulting signal. This is done by a high pass filter with a cut off frequency of 1Hz. Finally, a low pass Butterworth filter with a limiting frequency of 30 Hz is applied to the signal in order to suppress needless high frequency information even more. Fig.5 illustrates respectively; noisy ECG signal (record 101) $s(n)$, and the resulting filtered ECG signal $s_r(n)$.

b) Decomposing ECG into IMFs

The primary EMD is applied on $x(t)$ and the IMFs are obtained to locate the fiducial points in the ECG signal. The EMD of $x(t)$ (equation 1) is given by [14], where $c_i(t)$ is the *i*th IMF and $r_n(t)$ is the residue.

The IMFs are obtained by applying EMD on the filtered ECG signal $x(t)$. These IMFs and the ECG signal are then used to determine the fiducial points of the ECG signal.

c) R Peak Detection

Since the R wave is the sharpest component in the ECG signal, it is captured by the lower order IMFs which also contain high frequency noise. Past analysis using the EMD of clean and noisy ECG indicates that the QRS complex is associated with oscillatory patterns typically presented in the first three IMFs [16].

In our analysis, we have also found similar results. We denote the sum of first three IMFs as fine to coarse three, $f_2c_3(t)$ given by

$$f_2c_3(t) = \sum_{i=1}^{3} c_i(t) \qquad (6)$$

The oscillations associated with QRS complex in $f_2c_3(t)$ are much larger than those due to noise. Fig. 6 shows $f_2c_3(t)$ with $x(t)$ for a single ECG beat. It reveals that the R-peak in the ECG signal is detected by the peak of $f_2c_3(t)$.

Therefore, the R-peak detection comprises the following steps which are also illustrated in Fig. 7 for a series of ECG beats.

(I) Sum the first three IMFs to get $f_2c_3(t)$ and take its absolute value as $a(t)$.

(II) Retain the amplitudes of $a(t)$ larger than a threshold, T, where T is statistically selected to be half of the maximum value of $a(t)$ and make others zero. This eliminates the noise.

(III) Find the position of the maximum of a segment of time duration t_R starting from the first non zero value of $a(t)$ (Fig. 7). This is the first R-peak position. Similarly, find all other R-peak positions until the end of $a(t)$ is reached.

According to the width of QRS complex which is normally 100 ms with variation of $\pm$20 ms [6], we select t_R to be about 200 ms. We have considered the absolute value of $f_2c_3(t)$ since R-wave, and thus $f_2c_3(t)$, give a negative peak in some ECG leads.

After finding the R-peak position, t_0, we can find whether the peak is positive or negative from the value of $f_2c_3(t_0)$. If $f_2c_3(t_0)$ is positive, then the R-peak is positive since the base of $f_2c_3(t)$ is zero.

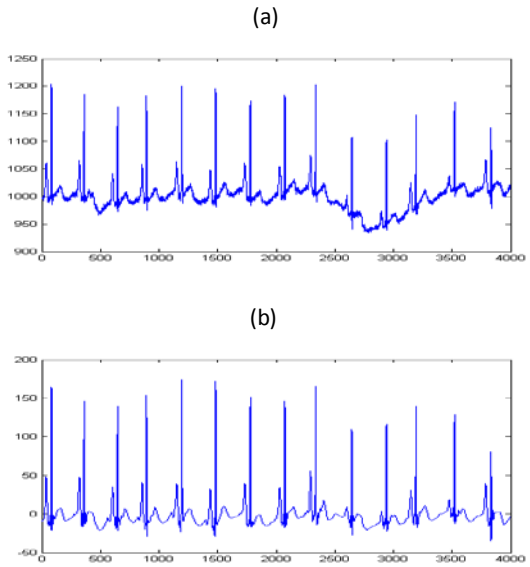


Fig.5 : (a) original ECG signal 222; (b) output of the band-pass Butterworth filter.

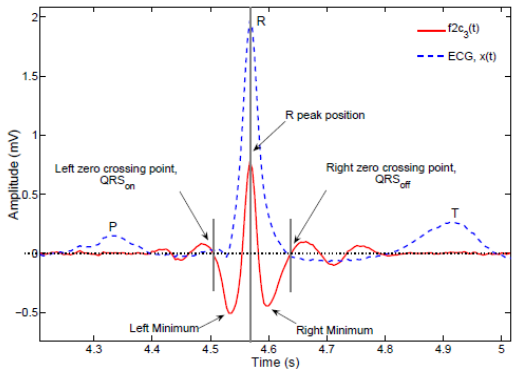


Fig.6 : Illustration of the QRS complex detection.

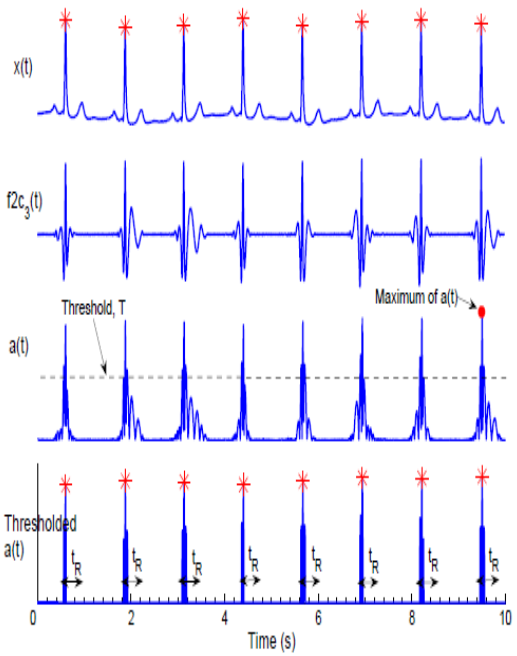


Fig.7 : steps for the R-peak detection.

IV. Results and Discussion

The algorithm was tested against a standard ECG database, i.e. the MIT-BIH Arrhythmia Database. The database consists of 48 half-hour ECG recordings and contains approximately 109,000 manually annotated signal labels. ECG recordings are two channel, however for the purpose of QRS complex detection only the first channel was used (usually the MLII lead). Database signals are sampled at the frequency of 360 Hz with 11-bit resolution spanning signal voltages within $\pm$5 mV range.

QRS complex detection statistic measures were computed by the use of the software from the Physionet Toolkit provided with the database. The two most essential parameters we used for describing the overall performance of the QRS complex detector are: sensitivity Se and positive predictivity +P.

The sensitivity and positive predictivity of the detection algorithms are computed by

$$Se = \frac{TP}{TP + FN} \quad (7)$$

$$+P = \frac{TP}{TP + FP} \quad (8)$$

where TP is the number of true positives, FN the number of false negatives, and FP the number of false positives [17]. The sensitivity reports the percentage of true QRS complexes that were correctly detected. The positive predictivity reports the percentage of detected QRS complexes which were in reality true QRS complexes.

Table.1 shows he results of the algorithm for all the records of the MIT-BIH. Figures 8, 9, 10, 11, and 12 give detection examples performed over tapes from MIT-BIH database. The exact QRS complexes are almost found correctly.

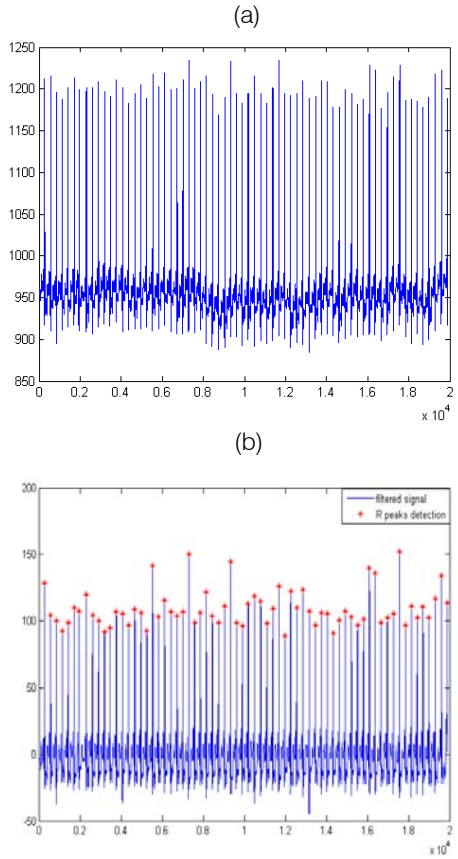
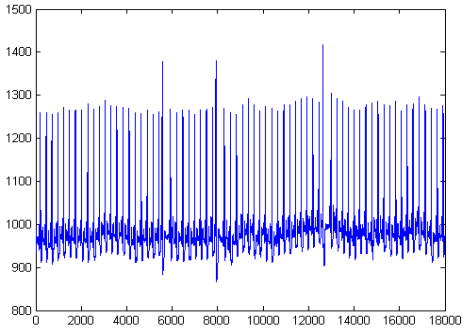


Fig.8 : (a) original ECG signal 100; (b) output of the band-pass Butterworth filter (in blue) and QRS detected (in red).

Record No.	Total (No. of beats)	FP	FN	Se	P
100	2273	0	0	100	100
101	1865	0	0	100	100
102	2187	0	1	99.95	100
103	2084	0	0	100	100
104	2230	2	1	99.96	99.91
105	2572	0	3	99.88	99.61
106	2027	5	2	99.90	99.75
107	2137	0	0	100	100
108	1763	7	14	99.21	99.60
109	2532	0	2	99.92	100
111	2124	0	1	99.95	100
112	2539	0	0	100	100
113	1795	0	0	100	100
114	1879	0	0	100	100
115	1953	0	0	100	100
116	2412	0	14	99.42	100
117	1535	1	0	100	99.93
118	2275	0	0	100	100
119	1987	0	0	100	100
121	1863	0	1	99.95	100
122	2476	2	0	100	99.92
123	1518	0	0	100	100
124	1619	0	1	99.94	100
200	2601	2	10	99.62	99.92
201	1963	0	15	99.24	100
202	2136	1	2	99.91	99.95
203	2982	2	29	99.03	99.93
205	2656	0	7	99.74	100
207	1862	14	26	98.60	99.24
208	2956	0	10	99.66	100
209	3004	8	1	99.97	99.73
210	2647	4	15	99.4	99.85
212	2748	1	0	100	99.96
213	3251	2	3	99.91	99.94
214	2262	4	3	99.87	99.82
215	3363	6	1	99.9	99.82
217	2208	1	1	99.95	99.95
219	2154	3	10	99.54	99.86
220	2048	2	0	100	99.90
221	2427	15	1	99.96	99.39
222	2484	0	5	99.80	100
223	2605	1	11	99.58	99.96
228	2053	14	2	99.90	99.32
230	2256	2	5	99.78	99.91
231	1886	0	0	100	100
232	1780	5	1	99.94	99.72
233	3079	0	1	99.97	100
234	2753	0	5	99.82	100
Total	109809	114	204	99.82	99.89

Table.1 : Performance of the algorithm using MIT/BIH database.

(a)



(b)

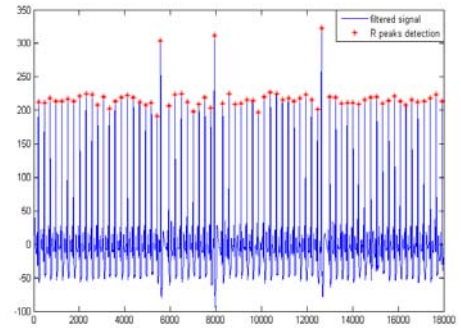
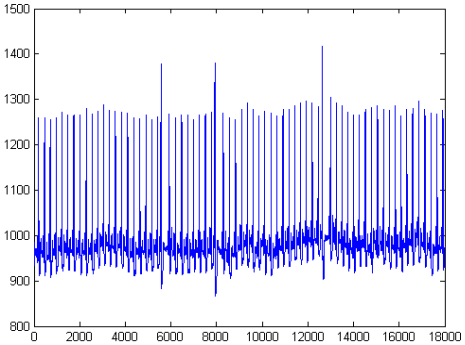


Fig.9 : (a) original ECG signal 105; (b) output of the band-pass Butterworth filter (in blue) and QRS detected (in red).

(a)



(b)

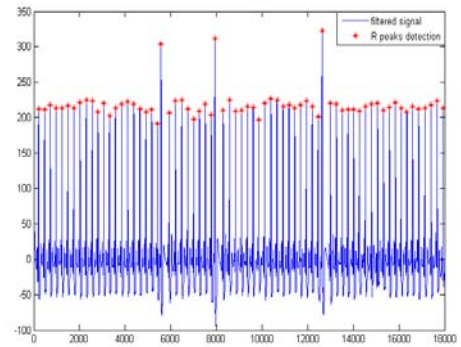
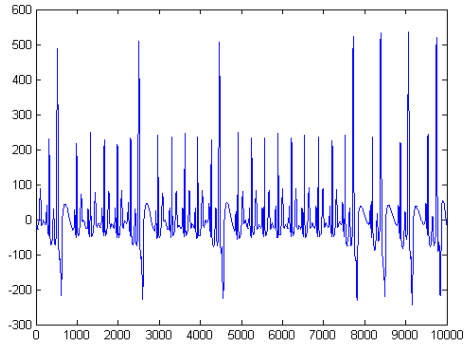


Fig.10 : (a) original ECG signal 108; (b) output of the band-pass Butterworth filter (in blue) and QRS detected (in red).

(a)



(b)

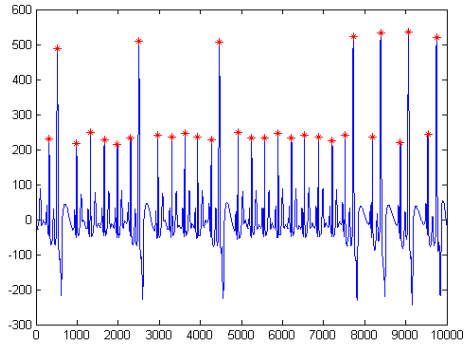
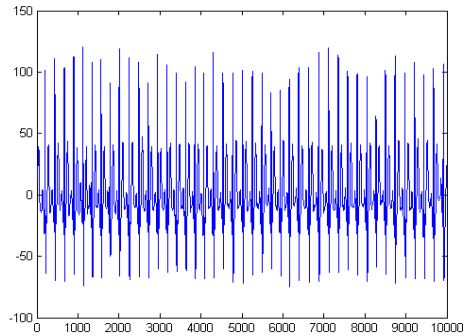


Fig.11 : (a) original ECG signal 119; (b) output of the band-pass Butterworth filter (in blue) and QRS detected (in red).

(a)



(b)

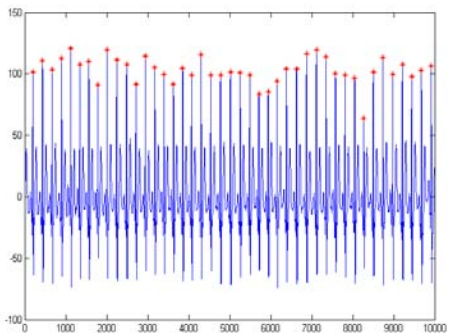


Fig.12 : (a) original ECG signal 219; (b) output of the band-pass Butterworth filter (in blue) and QRS detected (in red).

The average sensitivity of the algorithm is 99.82% and its positive predictivity is 99.89 %. The EMD method is found to have a good sensitivity and predictivity. Moreover this method is much more evolved than others. It is because the fast oscillatory QRS complex is highly detectable in the lower order IMFs irrespective of other characteristic wave amplitude.

Algritms	P (%)	Se (%)
Proposed Algorithm	99.89	99.82
Kohler [13]	88.70	99.57
Pan [8]	99.07	98.55
Zheng [9]	98.07	94.18
Christov's [10]	99.65	99.74
Martineze [18]	99.86	99.80
Madeiro [19]	98.96	98.47

Table.2 : Comparison of the performance.

Comparing the sensitivity and predictivity of the different methods in Table. 2 we find that EMD is a better choice for R peak detection.

V. Conclusion

We have developed a new algorithm based on the EMD for the automatic detection of QRS complex. The algorithm is evaluated for all of records obtained from the MIT-BIH. The proposed algorithm exhibits better performance than the threshold based technique and achieves high sensitivity Se=99.82 % and predictivity P=99.89 % for the QRS complex detection. The EMD method works not only for lead II but also for other leads. Only three lower order IMFs are needed to completely identify the QRS complex in the ECG signal.

References Références Referencias

1. X. Afonso, W.J. Tompkins, and T.Q. Nguyen, S. Luo, "ECG beat detection using filter banks," IEEE Trans. Biomed. Eng. vol. 46, pp. 192–202, 1999.
2. J. Fraden, M.R. Neumann, "QRS wave detection," Med. Biol. Eng.Comput. vol. 18, pp. 125–132, 1980.
3. S.E. Fischer, S. A. Wickline, and C. H. Lorenz, "Novel real-time R wave detection algorithm based on the Vectorcardiogramfor accurate gated magnetic resonance acquisitions," Magn. Reson. Med., vol. 42, no. 2, pp. 361–70, 1999.
4. L. Keselbrener, M. Keselbrener, S. Akselrod, "Nonlinear high pass filter for R-wave detection in ECG signal," Med. Eng. Phys., vol. 19, no. 5, pp. 481–484, 1997.
5. J. Leski, E. Tkacz, "A new parallel concept for QRS complex detector," Proc. 14th Annu. Int. Conf. IEEE Engineering in Medicine and Biology Society, Part 2, Paris, France, pp. 555–556, 1992.
6. A. Kyrkos, E. Giakoumakis, and G. Carayannis "Time recursive prediction techniques on QRS detection problem," Proc. 9th Annu. Conf. IEEE Engineering in Medicine and Biology Society, Boston MA, pp. 1885–1886, 13-16 Nov 1987.
7. K.P. Lin, W.H. Chang, "QRS feature extraction using linear prediction," IEEE Trans. Biomed. Eng., vol. 36, pp.1050–1055, 1989.
8. J. Pan, Tompkins, WJ, "A Real-Time QRS Detection Algorithm," IEEE Transactions on Biomedical Engineering. 1985:32, 230-236.
9. Li C, Zheng C, C. Tai, "Detection of ECG Characteristic Points Using Wavelet Transforms," IEEE Transactions on Biomedical Engineering. 1995:42, 21-28.
10. Ivaylo I. Christov, "Real time electrocardiogram QRS detection using combined adaptive Threshold," BioMed.Eng.Online 3 (2004) 28, ttp://www. biomedical-engineering-online.com/content/3/1/28.
11. R. Poli, S. Cagnoni, and G. Valli, "Genetic design of optimum linear and nonlinear QRS detectors," IEEE Trans. Biomed. Eng., vol. 42, pp. 1137–1141, 1995.
12. S.K. Zhou, J.T. Wang, and J.R. Xu, "The real-time detection of QRS complex using the envelop of ECG," (New Orleans, LA), p. 38, in Proc. 10th Annu. Int. Conf., IEEE Engineering in Medicine and Biology Society, New Orleans, LA, 1988.
13. B.U. Kohler, C. Hennig, R. Orglmeister, "The principles of software QRS detection," Engineering in Medicine and Biology Magazine,IEEE, vol. 21, pp. 42 – 57, Jan.-Feb. 2002.
14. N. E. Huang, Z. Shen, and S. R. Long, M. C. Wu, Shih H. H., Zheng Q., Yen N. C., Tung C. C., Liu H. H., "The empirical mode decomposition and hilbert spectrum for nonlinear and nonstationary time series analysis," Proc.R. Soc. Lond., pp. 454:903{995, 1998.
15. MIT–BIH Arrhythmia Database Directory, Harvard University–Massachusetts Institute of Technology Division of Health Sciences and Technology, July 1992.
16. M. B. Velasco, B. Weng, and K. E. Barner, "ECG signal denoising and baseline wander correction based on the empirical mode decomposition," Comput.Bio. Med., 38:1-13, 2008.
17. (ANSI/AAMI EC57), "Testing and reporting performance results of cardiac rhythm and ST segment measurement algorithms," (AAMI Recommended Practice/American National Standard), 1998.
18. J.P. Martinez, R. Almeida, and S. Olmos, A. Rocha, Laguna P., "Awavelet-based ECG delineator: evaluation on standard databases," IEEE Trans Biomed Eng, 51:570–81, 2004.
19. Joào P.V. Madeiro , Paulo C. Cortez, Francisco I. Oliveira, Robson S. Siqueira., "A new approach to QRS segmentation based on wavelet bases and adaptive threshold technique," IEEE Trans Medical Engineering & Physics 29, pp. 26–37, 2007.

This page is intentionally left blank

Global Journal of Computer Science and Technology
Volume 11 Issue 20 Version 1.0 December 2011
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Specific Growth Rate and Sliding Mode Stabilization of Fed-Batch Processes

By Yuri Pavlov
Bulgarian Academy of Sciences

*Summary-*The subject of this paper is specific growth rate control of a fed-batch biotechnological process. The objective of the paper is to present comfortable tools and mathematical methodology that permits control stabilization of biotechnological processes with synchronized utilization of different mathematical approaches. The control design is based on the equivalent transformations to Brunovsky normal form of an enlarged Monod-Wang model, on a chattering optimal control and sliding mode control solutions. This approach permits new precise control solutions for stabilization of continuous and fed-batch cultivation processes. In the paper are investigated Monod-Wang kinetic model and it singular Monod form. The simpler Monod and Monod-Wang models are restricted forms of Wang-Yerusalimsky model. The Wang-Yerusalimsky kinetic model could be accepted as a common model. A second order sliding mode is investigated and compared with standard sliding mode algorithms. The sliding mode control permits to solve the control problems with smaller quantity of priory information and elimination of parameters and measurements noises.

Keywords : *Sliding mode control, Fed-batch process, Monod kinetic, Monod-Wang model, Optimal control, Brunovsky normal form.*

GJCST Classification : *D.4.1, H.2.m*

Strictly as per the compliance and regulations of:

Specific Growth Rate and Sliding Mode Stabilization of Fed-Batch Processes

Yuri Pavlov

Summary - The subject of this paper is specific growth rate control of a fed-batch biotechnological process. The objective of the paper is to present comfortable tools and mathematical methodology that permits control stabilization of biotechnological processes with synchronized utilization of different mathematical approaches. The control design is based on the equivalent transformations to Brunovsky normal form of an enlarged Monod-Wang model, on a chattering optimal control and sliding mode control solutions. This approach permits new precise control solutions for stabilization of continuous and fed-batch cultivation processes. In the paper are investigated Monod-Wang kinetic model and it singular Monod form. The simpler Monod and Monod-Wang models are restricted forms of Wang-Yerusalimsky model. The Wang-Yerusalimsky kinetic model could be accepted as a common model. A second order sliding mode is investigated and compared with standard sliding mode algorithms. The sliding mode control permits to solve the control problems with smaller quantity of priory information and elimination of parameters and measurements noises.

Keywords : *Sliding mode control, Fed-batch process, Monod kinetic, Monod-Wang model, Optimal control, Brunovsky normal form.*

I. INTRODUCTION

Biotechnological processes are relatively difficult objects for control. Their features have been discussed repeatedly. Among the most-widely used control models for Biotechnological Processes are the so called unstructured models, based on mass balance. In these models the biomass is accepted as homogeneous, without internal dynamic. Most widely used are models based on the description of the kinetic via the well known equation of Monod or some of its modifications (Neeleman, 2002; Galvanauskas, 1998; Staniskis, 1992 Pirt, 1975;).

One of the most important characteristics of biotechnological processes, which make the control design more difficult, is the change of cell population state. A serious obstacle is the existence of noise of non Gaussian type. This type of noise appears in the measurement process as well as in the process of the determination of the structure parameters of the model. But may be the most serious obstacle is provoked by the differences in the rate of changes of the elements of the state space vector of the control system. Combined with the strong nonlinearity of the control system of the Monod type this feature of the control system leads to numerical instability or to unsatisfactory performance of the control algorithms (Neeleman, 2002; Tzonkov, 2006; Roeva, 2007).

The use of the classical methods of the linear control theory is embarrassed, mainly due to the fact that the noise in the system is not of Gaussian or colored type. The changes of the values of the structural parameters of the Monod kinetics models also lead to bad estimates when using Kalman filtering (Diop, 2009). Another serious flaw is that using classical linearization and control solutions via the feeding rate, the linear system is not observable (Wang, 1987). In addition, the Monod kinetics models are characterized by another feature of the optimal control solutions. The dynamic optimization based on the Pontryagin maximum leads to singular optimal control problems (Alekseev, 1979; Krotov, 1973). The above problems have led to development of extended dynamical models in which the dynamic of the changes of the growth rate of the BTP is described by separate equation on the general differential equation. Such extended observable models based on Monod kinetics are the Monod-Wang and Wang-Yerusalimsky models used in the paper (Pavlov, 2008).

These characteristics of biotechnological processes and models have led to search for solutions via approaches and methods related to a wide range of contemporary mathematical areas (DeLisa, 2001; Levisauskas, 2003; Roeva, 2007; Bamieh, 2007; Montseny, 2008; Diop, 2009). Such areas are adaptive systems, nonlinear systems, theory of variable structure systems and their main direction sliding mode control (SMC) (Emelyanov, 1993; Selişteanu, 2007; Mohseni, 2009). In the last decade up to date methods and approaches in the areas of functional analysis, differential geometry and its modern applications in the areas of nonlinear control systems as reduction, equivalent diffeomorphic transformation to equivalent systems and optimal control have been used (Neeleman, 2002; Pavlov, 2001; Mahadevan, 2001; Bamieh, 2007; Montseny, 2008).

In the paper is proposed a new control solution based on a contemporary differential geometric approach for exact linearization of non-linear Monod type models. In our control solution are used observable model based on Monod kinetics, namely the Monod-Wang and Wang-Yerusalimsky kinetic models. Based on

Author : Institute of Information and Communication Technologies, Bulgarian Academy of Sciences, E-mail : yupavlov14@hotmail.com

these models a control design for optimal control and stabilization of the specific growth rate of fed-batch biotechnological processes is presented. The control is written based on information of the growth rate (Neeleman, 2002).

II. Monod and Monod-Wang Biotechnological Models

Most widely used are models based on the description of the kinetic via the well known equation of Monod or some of its modifications. The rates of cell growth, sugar consumption, concentration in a yeast fed-batch growth are commonly described as follows:

$$\begin{aligned}\dot{X} &= \mu_m \frac{S}{K_S + S} X - \frac{F}{V} X \\ \dot{S} &= -k\mu_m \frac{S}{K_S + S} X + \frac{F}{V}(S_0 - S) \\ \dot{V} &= F\end{aligned} \qquad (1)$$

This differential equation is often part of more general and complex dynamic models. Here X is the concentration of the biomass, S is the substrate concentration, V is the volume of the bioreactor. The maximal growth rate is denoted by μ_m and K_S is the coefficient of Michaelis-Menten. With k we denote a constant typical for the corresponding process. The feeding rate is denoted by F. If the process is continuous (F/V) is substituted by the control D, the dilution rate of the biotechnological process (BTP). The third equation is dropped off. Often used models are described in table 1 (Staniskis, 1992; Zelic, 2004; Galvanauskas, 1998; Tzonkov, 2006).

Table 1

Model	μ
1	$\mu_{\max} \frac{S}{(k_s + S)}$
2	$\mu_{\max} \frac{S}{(k_s + S)} \frac{k_i}{(k_i + A)}$
3	$\mu_{\max} \frac{S}{(k_s + S + S^2/k_i)}$

The first model is the well known Monod type model (Roeva, 2004, 2007), the second is the Yerusalimsky model (Galvanauskas, 1998) and the third model includes inhibition term in the denominator. The non-observability of the Monod model has led to the development of the widened dynamical models, in which the dynamics of the specific growth rate of the BTP is described via separate equation in the system of differential equations. The dynamics of the growth rate μ in the Monod-Wang model is modeled as a first order lag process with rate constant m, in response to the deviation in the growth rate. This model called also the model of Monod-Wang determines a linear observable system in the classical linearization (Wang, 1987; Pavlov, 2007).

$$\begin{aligned}\dot{X} &= \mu X - \frac{F}{x_4} X \\ \dot{S} &= -k\mu X + \frac{F}{V}(S_0 - S) \\ \dot{\mu} &= m(\mu_m \frac{S}{K_S + S} - \mu) \\ \dot{V} &= F\end{aligned} \qquad (2)$$

This model concerns a fed-batch biotechnological process. Obviously model (1) is a singular form of model (2). The comparison of both models is shown in Figures (1, 2, 3):

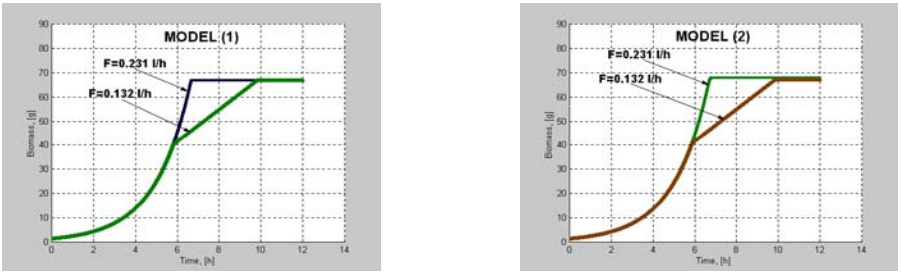


Figure1 : Growth of the biomass using Monod model (1) and Wang-Monod model (2).

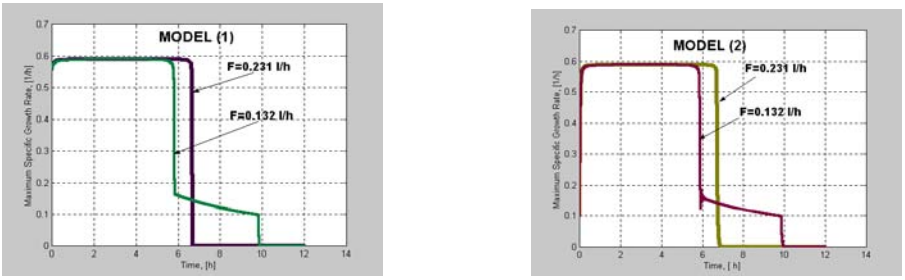


Figure2 : Specific growth rate using Monod model (1) and Wang-Monod model (2).

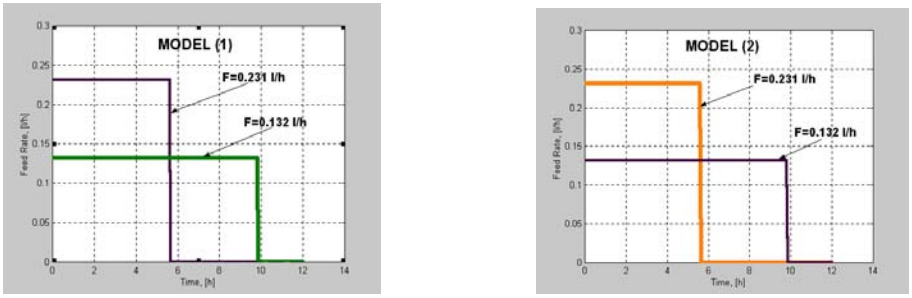


Figure 3 : Feeding rate using Monod model (1) and Wang-Monod model (2).

One general description of the fed-batch biotechnological process looks like (Pavlov, 2007).

$$\begin{aligned}
\dot{X} &= \mu X - \frac{F}{V} X, \\
\dot{S} &= -k\mu X + (So - S)\frac{F}{V}, \\
\dot{\mu} &= m(\mu_m \frac{S}{(K_S + S)} - \mu), \\
\dot{V} &= F, \\
\dot{A} &= = k_3 \mu X - \frac{F}{V} A.
\end{aligned} \tag{3}$$

Here X denotes the concentration of biomass, [g/l]; S – the concentration of substrate (glucose), [g/l]; V - bioreactor volume, [l]; F – substrate feed rate, [h^{-1}]; S_0 – substrate concentration in the feed, [g/l]; μ_{max} - maximum specific growth rate, [h^{-1}]; K_S – saturation constant, [g/l]; k and k_3 – yield coefficients, [g/g], m – rate coefficient [-];. The dynamics of μ in the Monod-Wang model is modeled as a first order lag process with rate constant m, in response to the deviation in μ. The last equation describes the production of acetate (A). This equation is dynamically equivalent to the first one after the implementation of a simple transformation ($X = (1/k_3)\ A$). That is why we replace A with X in Yerusalimsky model. The best description is given by the so called model of Wang-Yerusalimsky:

$$\begin{aligned}
\dot{X} &= \mu X - \frac{F}{V} X, \\
\dot{S} &= -k\mu X + (So - S)\frac{F}{V}, \\
\dot{\mu} &= m(\mu_m \frac{S}{(K_S + S)} \frac{k_i}{(k_i + X)} - \mu), \\
\dot{V} &= F, \\
\dot{A} &= = k_3 \mu X - \frac{F}{V} A.
\end{aligned} \tag{4}$$

In the formula X is the concentration of biomass, [g/l]; S–the concentration of substrate (glucose), [g/l]; V-bioreactor volume, [l]; F–substrate feed rate (control input), [h^{-1}]; S_0–substrate concentration in the feed, [g/l]; μ_{max}-maximum specific growth rate, [h^{-1}]; K_S–saturation constant, [g/l]; k, k_3–constants, [g/g]; m–coefficient [-]; E–the concentration of ethanol, [g/l]; A–the concentration of acetate [g/l]. The system parameters are as follows: μ_m=0.59 [h^{-1}], K_S=0.045 [g/l], m=3 [–], S_0=100 [g/l], k=1/$Y_{S/X}$,, k=2 [–], k_3=1/$Y_{A/X}$, k_3=53 [–], k_i=50 [–], F_{max}= 0.19 [h^{-1}], V_{max}=1.5 [ ] . These data desribed an *E. Coli* process (Cockshott, 1999) and are chosen close to data in table 2 (Roeva, 2004, 2007):

Table 2

Parameter	Model 1	Model 2	Model 3
μ_{max} , [h^{-1}]	0,55	0,52	0,54
k_S , [gl^{-1}]	0,039	0,027	0,029
k_i , [gl^{-1}]	51,3	53,6	50,8
$Y_{S/X}$, [gg^{-1}]	0,501	0,498	0,497
$Y_{A/X}$, [gg^{-1}]	0,015	0,015	0,015

The last equation describes the production of acetate (A). This equation is dynamically equivalent to the first one after the implementation of a simple transformation ($X = (1/k_3)A$). The initial values of the state variables are: $X(0)=0.99$; $S(0)=0.01$; $\mu(0)=0.1$; $A(0) = 0,03$; $V(0)=0.5$.

The following mathematical condition ($k_E \to \infty$) determines the Wang-Monod model as a restricted form of the Wang-Yerusalimsky model (4). The Monod model is a singular form of Wang-Monod model obtained by omission of the third equation. That is why the Wang-Yerusalimsky model is a more general model form.

Interesting moment is that these models are dynamically equivalent to the following Brunovsky normal form (Pavlov, 2001, 2004, 2007):

$$\begin{aligned} \dot{Y}_1 &= Y_2 \\ \dot{Y}_2 &= Y_3 \\ \dot{Y}_3 &= W \end{aligned} \qquad (5)$$

Here by W is noted the control input. This model is linear. The non-linearity of model (1) is transformed and included in the input function W (Montseny, 2008; Bamieh, 2007; Elkin, 1999; Gardner, 1992). The input function W depends from the space vector of model (1) and that has to be underlined because this is a limitation of the application of the Pontryagin maximum principle (Alekseev, 1979; Krotov, 1973; Hsu, 1972). Different diffeomorfic transformations of the Monod, Wang and Yerusalimsky models are analyzed in details in the following papers (Pavlov, 2001, 2004, 2007, 2008). The Brunovsky form is a linear model and permits easy optimal control solutions with application of the Pontryagin's maximum principle.

The complexity of the biotechnological systems and their singularities make them difficult objects for control. They are difficult to control also because of the fact that it is difficult to determine their optimal technological parameters. These parameters can depend on very complicated technological, ecological or economical market factors. Their taking into account in one mathematical model directly is impossible for the time being. Because of this reason often in practice expert estimates are used. From outside the estimates are expressed only by the qualitative preferences of the Biotechnologist. The preferences themselves are in rank scale and bring the internal indetermination, the uncertainty of the qualitative expression, which is a general characteristic of human thinking. Because of this reason here the mathematical models from the Utility theory and stochastic programming can be used (Kivinen, 2004; Fishburn, 1970; Keeney, 1993; Aizerman, 1970).

Thus the incomplete information usually is compensated with the participation of imprecise human estimations. Our experience is that the human estimation of the process parameters of a cultivation process contains uncertainty at the rate of [10, 30] %. Here is used a mathematical approach for elimination of the uncertainty in the DM's preferences based both on the Utility theory and on the Stochastic programming (Pavlov, 2010, 2011). The algorithmic approach permits exact mathematical evaluation of the optimal specific growth rate of the fed-batch cultivation process according to the DM point of view even though the expert thinking is qualitative and pierced by uncertainty. The assessed utility criteria are shown on the following figure 4:

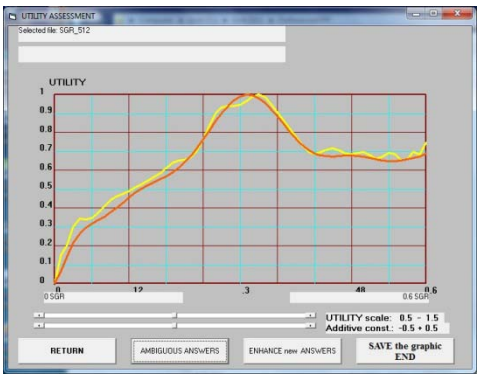


Figure 4 : Expert utility versus Growth rate

Thus we achieve totally analytical mathematical description of the complex system "Technologist-biotechnological process "(Pavlov, 2010, 2011).

III. Optimal Control and Stabilization of the Growth Rate

The presentation of the control design follows the presentations in papers (Pavlov, 2004, 2007, 2008). We use the general model (Technologist-biotechnological process). We preserve the notation $U(.)$ for the DM utility function (Pavlov, 2010; Fishburn, 1970; Keeney, 1993). The control design of the fed-batch process is based on the next subsidiary optimal control problem:

Max($U(\mu(T_{int}))$), *where the variable* μ *is the specific growth rate,* ($\mu \in [0, \mu_{max}]$, $D \in [0, D_{max}]$). *Here* $U(\mu)$ *is an aggregation objective function (the utility function – fig.4)* and D is the control input (the dilution rate):

$$\max(U(\mu)),\ \mu\in[0,\mu_{\max}],\ t\in[0,T_{\text{int}}],\ D\in[0,D_{\max}]$$

$$\begin{aligned}\dot{X} &= \mu X - DX\\ \dot{S} &= -k\mu X + (So - S)D\\ \dot{\mu} &= m(\mu_m \frac{S}{(K_S + S)} - \mu)\end{aligned} \tag{6}$$

When T_{int} is sufficiently small the optimization is in fact "time minimization". The differential equation in (6) describes *a continuous fermentation process*. The model permits exact linearization to the next Brunovsky normal form (Goursat, as regard to the differential forms) (Gardner, 1992; Elkin, 1999; Pavlov 2001):

$$\begin{aligned}\dot{Y}_1 &= Y_2,\\ \dot{Y}_2 &= Y_3,\\ \dot{Y}_3 &= W.\end{aligned} \tag{7}$$

The Brunovsky normal form of Wang-Yerusalimsky model (4) is the same (Pavlov, 2008). Here W denotes the control input. The new state vector (Y_1, Y_2, Y_3) is:

$$\begin{aligned}Y_1 &= u_1,\\ Y_2 &= u_3(u_1 - ku_1^2),\\ Y_3 &= u_3^2(u_1 - 3ku_1^2 + 2k^2u_1^3) + m(\mu_m \frac{u_2}{(K_S + u_2)} - u_3)(u_1 - ku_1^2),\end{aligned} \tag{8}$$

$$\begin{bmatrix} u_1(X,S,\mu)\\ u_2(X,S,\mu)\\ u_3(X,S,\mu)\end{bmatrix} = \begin{bmatrix} \frac{X}{S_o - S}\\ S\\ \mu\end{bmatrix}.$$

The derivative of the function Y_3 determines the interconnection between W-model (7) and D-model (6). The control design is a design based on the Brunovsky normal form and application of the Pontrjagin's maximum principle step by step for sufficiently small time periods T. The optimal control law has the analytical form (Pavlov, 2007):

$$D_{opt} = sign\left(\left(\sum_{i=1}^{6} ic_i\mu^{(i-1)}\right)(T-t)\left[\frac{(T-t)\mu(1-2kY_1)}{2} - 1\right]\right)D_{\max}, \tag{9}$$

$$where: sign(r) = 1, r > 0,\ sign(r) = 0, r \le 0.$$

The optimal control law of Wang-Yerusalimsky model (4) has the same form (Pavlov, 2008).This type of control may be used only for cumulative criteria for which the Bellman principle is valid in the optimal control (Hsu, 1972). For example, such are the amount of biomass at the end of the process and the time-minimization optimal control. The sum is the derivative of the utility function $U(\mu)$.The time interval T can be the step of discretization of the differential equation solver.

It is clear that the "time-minimization" control is determined from the *sign* of the utility derivative. Thus, the control input is D=$D_{\max}$ or D=0. The solution is a *"time-minimization"* control (if the time period T is sufficiently small) (Pavlov, 2004). The control brings the system back to the set point for minimal time in any case of specific growth rate deviations. The demonstration is shown in (Pavlov, 2007).

The previous solution permits easy determination of the control stabilization *of the fed-batch process*. The control law is based on the solution of the next optimization problem:

Max($U(\mu(T_{int}))$), *where the variable* μ *is the specific growth rate,* ($\mu\in[0,\ \mu_{max}]$, $F\in[0,\ F_{max}]$). *Here* $U(\mu)$ *is the utility function in figure (3)* and F is the control input (the substrate feed rate):

$$\max(U(\mu(T_{\text{int}}))),\ \mu\in[0,\mu_{\max}],\ t\in[0,T_{\text{int}}],\ F\in[0,F_{\max}]$$

$$\begin{aligned}\dot{X} &= \mu X - \frac{F}{V}X\\ \dot{S} &= -k\mu X + (So - S)\frac{F}{V}\\ \dot{\mu} &= m(\mu_m \frac{S}{(K_S + S)} - \mu)\\ \dot{V} &= F\end{aligned} \tag{10}$$

The control law *of the fed-batch process* has the same form (9) because $D(t)$ is replaced with $F(t)/V(t)$ in the fed-batch model. Thus, the feeding rate $F(t)$ takes $F(t)$=$F_{\max}$ or $F(t)$=0, depending on $D(t)$ which takes D=$D_{\max}$ or D=0.

We conclude that the control law (9) bring the system to the optimal point (optimal growth rate) with a" time minimization" control, starting from any deviation point of the specific growth rate (Fig. 5).

Thus, we design the next control law:

1. At the interval [0, t_1] the control is "time-minimization" control (9), where $\mu(t_1)=(\mathbf{x_{30}-\varepsilon})$, $\varepsilon>0$, $x_{30}=max(U(\mu))$. D is replaced with $F=\gamma F_{max}$, $1\geq\gamma>0$, when $D=D_{max}$. The choice of γ depends on the step of the equation solver and is not a part of the optimization (here $\gamma=0.123$);
2. At the interval $[t_1, t_2]$ the control is $F=0$ ($\mu(t_1)=(\mathbf{x_{30}-\varepsilon})$, $\mu(t_2)=\mathbf{x_{30}}$ - to be escaped an overregulation);
3. After this moment the control is the control (9) with $F=\gamma F_{max}$, when $D=D_{max}$ (chattering control with $1\geq\gamma>0$).

The deviation of the fed-batch process with this control is shown on figures (5, 6).

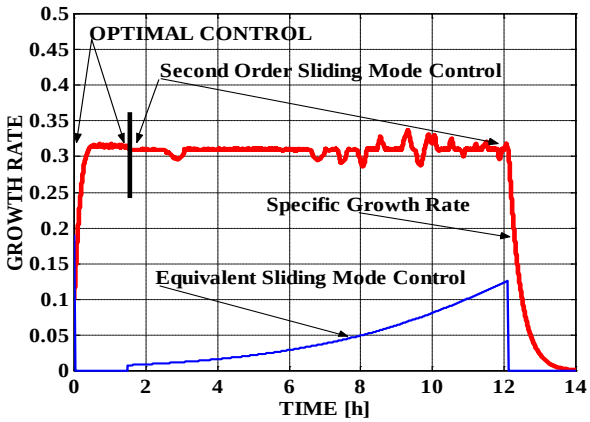


Fig. 5 : Stabilization of the fed-batch process

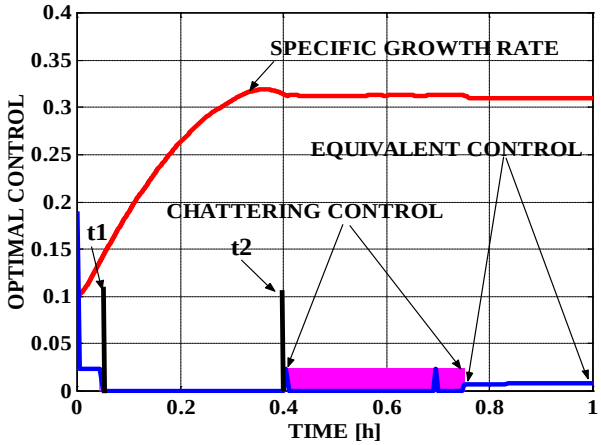


Fig. 6 : Optimal profile

After the stabilization of the system in equivalent sliding mode control position the system can be maintained around the optimal parameters with sliding mode control (Fig.5, 6). Possible solution in sliding mode is alternation of μ_m (as a function of the temperature and the acidity in the bioreactor) or alternation of F (Pirt, 1975; Pavlov, 2007). The iterative utility function design and the iterative corrections in the DM preferences permit adjustment of the control law and of the optimal control final results in agreement with the changes in the opinion of biotechnologist. The procedure could be interprets as learning procedure in the two opposite directions, in direction to biotechnologist or in direction to the final optimal solution.

IV. Mathematical Problems Arising From the Sliding Mode Control

Control solution results are shown in control systems based on the solutions of variable structure systems (Selişteanu, 2007; Mohseni, 2009). Here a different problem arises. Good control via sliding mode control is possible when the system is led to the initial position in a point from the area of the "equivalent control solution" (Pavlov, 2007, 2008). This is a specific task for fed-batch control via information about the growth rate of the biomass.

A common manifestation in sliding mode control is some overregulations of the biotechnological process. Such overregulations are shown in figures (7 and 8). In case of start in sliding mode in system conditions different from the area of "equivalent sliding mode control" then the process arrives in some over regulations (Utkin, 1981).

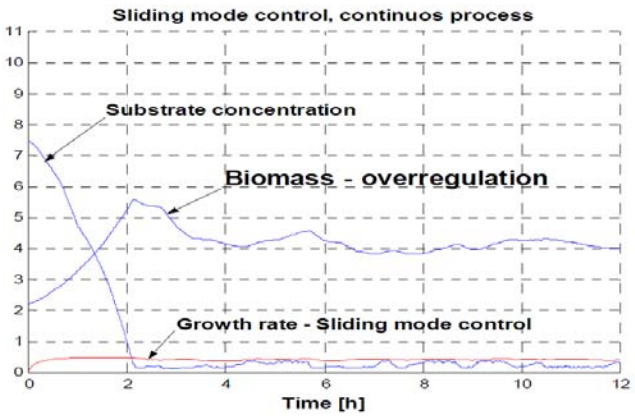


Fig.7 : Continuous process – overregulation of the biomass in SMC

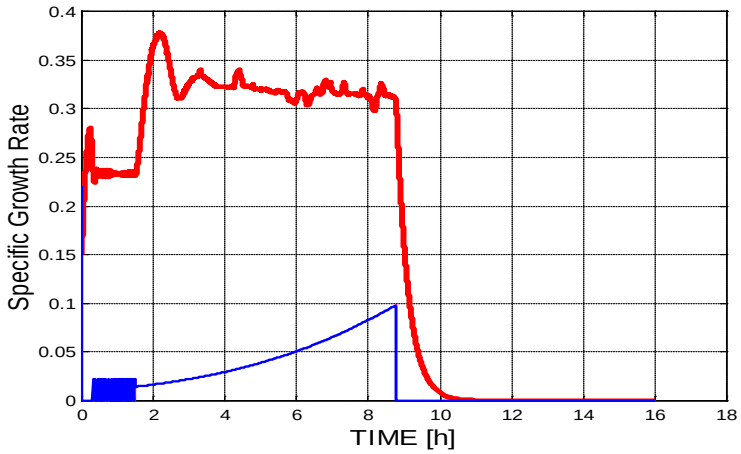


Fig.8 : Fed batch process- overregulation of the growth rate in SMC

These characteristics of biotechnological processes table new mathematical control problems for discussion and resolution. The overregulations in SMC are provoked by the differences in the rate of changes of the elements of the state space vector of the control system. It is needed control solution that fixes the system in "equivalent control" position, staring from any initial positions.

These characteristics of biotechnological processes and models have led to search for solutions via approaches and methods related to a wide range of contemporary mathematical areas. Such areas are differential geometry and its modern applications in the areas of nonlinear control systems as diffeomorphic transformation to equivalent systems. Solutions that fix the system in "equivalent control" position, staring from any initial positions are showed in (Fig. 9, 10).

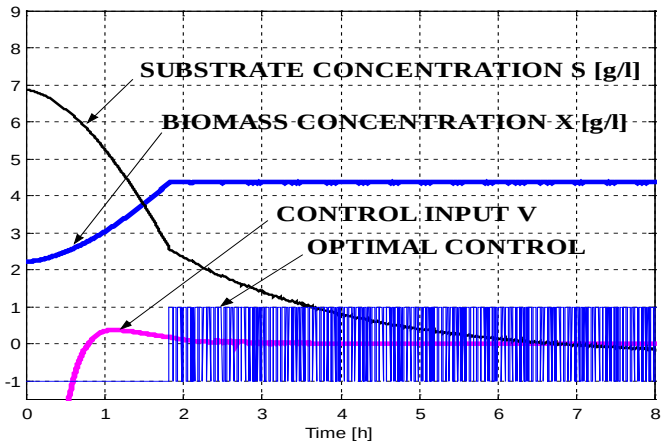


Fig.9 : Continuous process – Optimal feed rate and fixation of the biomass

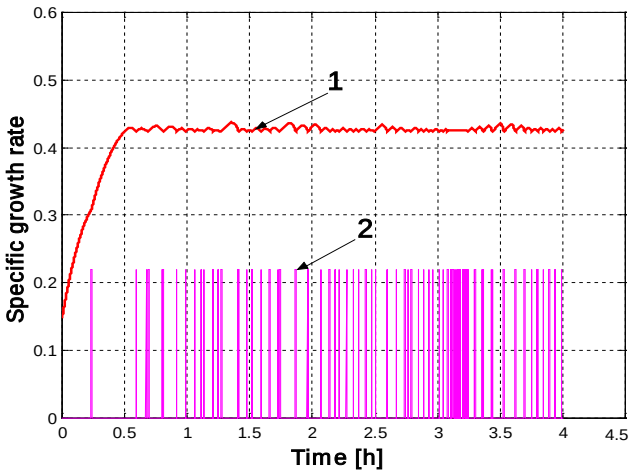


Fig.10 : Fed batch process, Chattering control: growth rate (1); feed rate control (2)

Detailed descriptions of such controls are discussed in (Pavlov, 2007, 2008). In the last decade up to date methods and approaches in the areas of functional analysis, differential geometry and its modern applications in the areas of nonlinear control systems as reduction, equivalent transformation to equivalent systems have been used for surmount the discussed difficulties (Pavlov, 2005; Bamieh, 2007; Montseny, 2008; Diop, 2009).

V. Sliding Mode Control and Stabilization of the Fed-Batch Process

The sliding mode control is a good solution for stabilization under varying conditions (parameters deviations, noises etc.) (Emelyanov, 1993, 1996; Utkin 1987; Selişteanu, 2007). In the paper is demonstrated a sliding mode control for stabilization of the specific growth rate in "the best" growth rate (Pavlov, 2007).

For some types of BTP it is possible to choose the control via the temperature and/or via changing the acidity in the bioreactor (Pirt, 1975). What we mean is indirect influence on the biomass maximum growth rate, which, according to the contemporary researches, is one of the main factors, determining the quality of the cultivation process (Neeleman, 2002). Here the problem about the observability of the control system arises again, because this directly concerns the possibility for satisfactory identification of the state space vector of the control system and more specifically for the determination of the specific growth rate of the BTP. This group of questions is still a topical branch in the theory of the biotechnological control systems (Diop, 2009).

The sliding mode in the paper is realized with Wang-Monod model (3). This more exotic SM control solution is obtained with alternations of the maximum specific growth rate $\mu_m(T, pH)$ through changes of the temperature (t^o) and the acidity of the bioreactor medium (pH)(Pirt, 1975) . This control gives us the possibility to use the temperature (t^o) and the acidity (pH) as input control values. More classical SM solutions with substrate concentration S as control value could be seen in the literature (Selişteanu, 2007; Mohseni, 2009).

The sliding affine subspace is defined by the equation $S(\mu) = (\mu - 0{,}31) = 0$. The general stability conditions are derived from the Liapunov's function $(S(\mu))^2$ (Utkin, 1981). In sliding mode control the substrate concentration S in the bioreactor is constant. The substrate concentration S is constant $Se = 0{,}0498$. The equivalent growth rate control is determined exactly and the SM control is possible (Utkin, 1981):

$$Ue\mu = \frac{(Ks + S)\mu}{S} \tag{11}$$

The feeding rate F(t) is derived from the substrate concentration: $F(t)=(kX(t)\mu(t)V(t)/(So-S_e)$, where $X(.)$ is the quantity of biomass in the bioreactor. Deviations of the system in sliding mode are showed in Fig. (11, 12).

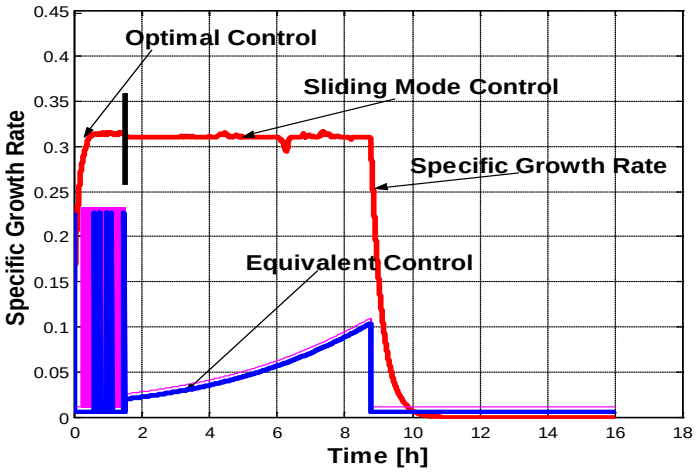


Fig.11 : Specific Growth Rate stabilization in sliding mode

The mathematical model and the corresponding stability conditions determine the SM control law:

$$Control \Rightarrow \Delta\mu_m = -\left[\left|\frac{(Ks + S)\mu}{S} - \mu_m^1\right| + \mu_m^2\right] sign(Sl_1) \tag{12}$$

The variations of the temperature (T) and the acidity (pH) assure the chattering of μ_m around the equilibrium $(\mu_m=\mu_{m0}+\Delta\mu_m)$,

$$\mu_m^1 = 0.31, \mu_{m0} = \frac{(Ks + Se)\times 0.31}{Se}. \tag{13}$$

The value μ_m^2 is a sufficiently small supplementary value. This SM control law eliminates the deviations of the parameters, noises and structure modifications. This solution overcomes successfully some of the difficulties mentioned above.

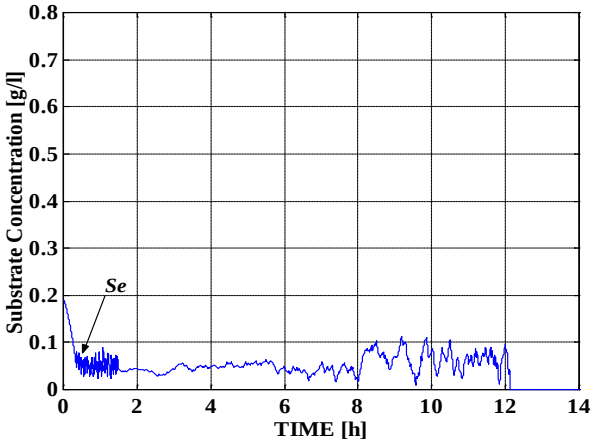


Fig.12 : Substrate concentration S in sliding mode

The Russian scientists Emelyanov, Korovin and Levant evolve high-order sliding mode methods in control systems (Emelyanov, 1993, 1996). We propose in our investigation a second order sliding mode control following Emelyanov and Korovin. The control algorithms of second order are used so that the system deviations become cooler but a little more imprecise. Out of this approach the second order SM manifold becomes:

$$S_1 \cap \dot{S}_1, \text{where } S_1 = (\mu - 0.31) \text{ and } \dot{S}_1 \text{ is the time derivative.} \quad (14)$$

Here is used the so-called "contraction" algorithm [5]. After Emelyanov the second order SM control input in the "contraction" algorithm becomes:

$$Control \Rightarrow \Delta\mu_m = -\left[\frac{(1{,}15K_s + 1{,}15S)1{,}15\mu}{0{,}85S} - \mu_m^1\right| + \mu_m^2\Big] \times$$
$$\times \left(\frac{2}{3}\text{sign}(S_1) + \frac{1}{3}\text{sign}\left(\left(\mu_m \frac{S}{(S+K_s)} - \mu\right)(\mu_m - 0.59)\right)\right) \quad (15)$$

It is known that this algorithm ends for finite time (Emelyanov, 1993, 1996). The input in second order SM is smoother but the control becomes is more imprecise. The performances of the system with this SM control are showed in Fig. (13, 14) (Pavlov, 2007, 2008).

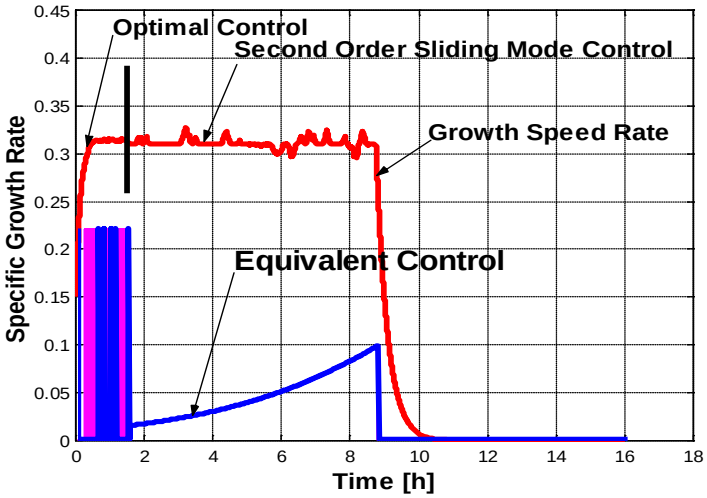


Fig.13 : Second order SM - μ

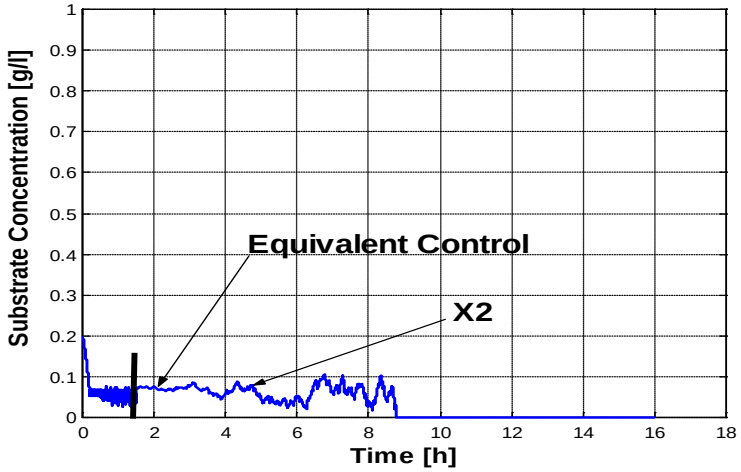


Fig.14 : Second order SM - substrate concentration S - (x_2)

The devolving from the "discontinuity" to "continuity" in sliding mode control not only raise the control quality but permits to solve control problems with smaller quantity of priory information (Emelyanov, 1993, 1996).

By now we have reached a full mathematical description of the complex system "Biotechnologist-fed-batch process". We have overcome the restrictions connected with the observability of the Monod kinetics; we have overcome the obstacles with the singularities of the optimal control via finding and using of the Brunovsky normal form of the differential equation. The system was led to the working point from the "equivalent control in sliding mode" smoothly and stabilized in the optimal specific growth rate position (Pavlov, 2007). The solution and the determination of the optimal profile was

done via synchronized usage of several mathematical approaches for modeling, reduction of nonlinear system, application of the Pontryagin maximum principle.

VI. Conclusion

A methodology for specific growth rate optimal control is developed. This approach aims utilization of control based only on specific growth rate measurement. In the paper are investigated the possibilities of the second order sliding mode. We have overcome the restrictions connected with the observability of the Monod kinetics through Monod-Wang and Wang-Yerusalimsky models; we have overcome the obstacles with the singularities of the optimal control via finding and using of the Brunovsky normal form of the differential equation. The system was led to the working point from the "equivalent control in sliding mode" smoothly and stabilized in the optimal specific growth rate position. This solution permits to win through difficulties arising from the biotechnological peculiarities in order to be obtained good control solutions.

The inclusion of a value model as objective function as part of a dynamical system reached a full mathematical description of the complex system "Biotechnologist-fed-batch process". This is done with the use of the expected utility theory and the stochastic programming. Such a good objective function would allow the user to vary iteratively his value judgments and to correct iteratively the control law in agreement with his value judgments.

References References Referencias

1. Aizerman, M., E. Braverman, L.Rozonoer. (1970). Potential Function Method in the Theory of Machine Learning. Moscow, Nauka, 1970.
2. Alekseev V., V. Tihomirov, S. Fomin.(1979). Optimal Control. Moscow, Nauka, 1979.
3. Bamieh, L. (2007). On Discovering Low Order Models in Biochemical Reaction Kinetics, *2007 American Control Conference*, July 11-13, New York, USA, 2007.
4. Cockshott A. R., I. D. L. Bogle (1999). Modelling the Effects of Glucose Feeding on a Recombinant *E. coli* Fermentation, Bioprocess Engineering, 20, 83-90.
5. DeLisa M., H. Chae, W. Weigand, J. Valdes, G. Rao, W. Bentley (2001). Generic Model Control of Induced Protein Expression in High Cell Density Cultivation of *Escherichia coli* Using On-line GFP-fusion Monitoring, Bioprocess and Biosystems Engineering, 24, 83-91.
6. Diop S.,I. Simeonov. (2009). On the Biomass Specific Growth Rates Estimation for Anaerobic Digestion using Differential Algebraic Techniques. International Journal Bioautomation. V. 13, Issue: 3, p.p. 47-56.
7. Elkin V. (1999). Reduction of Non-linear Control Systems: A Diferential Geometric Approach, Mathematics and its Applications, Vol. 472, Handbound, Kluwer.
8. Emelyanov S., S. Korovin and A. Levant (1996). High-order sliding modes in control systems. Computational mathematics and modelling, 1996, vol. 7, no.3, pp. 294–318.
9. Emelyanov S., S. Korovin, A. Levant. (1993). Higher-order Sliding Modes in Control Systems, Diferential Equations, 29 (11), 1993, 1627-1647, http://www.zentralblatt-math.org/zbmath/search/?q=an%3A0815.93015
10. Fishburn, P. (1970). Utility Theory for Decision-Making, Proceedings, NewYork, Wiley.
11. Galvanauskas V., R. Simutis, N. Volk, A. Lubbert (1998). Model Based Design of a Biochemical Cultivation Process, Bioprocess Engineering, 18, 227-234.
12. Gardner R., W. Shadwick, The GS algorithm for exact linearization to Brunovsky normal form, *IEEE Trans. Autom. Contro* , 1992, 37, No.2, 224-230.
13. Hsu J., A. Meyer, (1972). Modern. Control Principles and Applications, McGRAW-HILL, New York.
14. Keeney R, H. Raiffa (1993). Decision with Multiple Objectives: Preferences and Value Tradeofs, Cambridge University Press, Cambridge & New York, (1976) 1993.
15. Kivinen. J. , Smola, A., Williamson R. (2004). Online Learning with Kernels, IEEE Transactions on Signal Processing, vol. 52, N. 8, August 2004.
16. Krotov V., V. Gurman. (1973). Methods and Problems in the Optimal Control. Moscow, Nauka, 1973.
17. Levisauskas D., V. Galvanauskas, S. Henrich, K. Wilhelm, N. Volk, A. Lubbert (2003). Model-based Optimization of Viral Capsid Protein Production in Fed-batch Culture of recombinant *Escherichia coli*, Bioprocess and Biosystems Engineering, 25, 255-262.
18. Mahadevan R., Agrawal S. (2001). Differential flatness based nonlinear predictive control of fed-batch bioreactors, Control Engineering Practice, Volume 9, Number 8, August 2001, pp. 889-899 (11).
19. Mohseni, S, V. Babaeipour, A. Vali. (2009). Design of sliding mode controller for the optimal control of fed-batch cultivation of recombinant E. Coli. Chemical Engineering Science. V. 64, Issue: 21, Elsevier, Pages: 4433-4441.
20. Montseny, E. & Doncescu A. (2008). Operatorial Parametrizing of Controlled Dynamic Systems-Application to the Fed-Batch Bioreactor Control Problem. 17th World Congress The International Federation of Automatic Control. Seoul, Korea, p.p. 7486-7490.

21. Montseny, E. & Doncescu A. (2008). Reduction of Complexity via Operatorial Parametric Formulations for Some Nonlinear Dynamic Problems of Biology. 22nd International Conference on Advanced Information Networking and Applications - Workshops (aina workshops 2008), pp.790 795.
22. Neeleman R. (2002). Biomass Performance: Monitoring and Control in Biopharmaceutical production, Thesis, Wageningen University, Netherlands, 2002. http://edepot.wur.nl/121354
23. Pavlov Y. (2001). Exact Linearization of a Non Linear Biotechnological Model /Brunovsky Model/, Comptes Rendus de l'Academie Bulgares des Sciences (Proceedings of Bulgarian Academy of Sciences), N10, 2001, 25-30, http://adsabs. harvard. edu/abs/2001CRABS..54j..25P
24. Pavlov Y. (2007). Brunovsky Normal Form of Monod Kinetics and Growth Rate Control of a Fed-batch Cultivation Process, Online journal Bioautomation, V. 8, So_a, Bulgaria, 2007, 13-26. http://clbme. bas.bg/bioautomation/
25. Pavlov Y. (2008). Equivalent Forms of Wang-Yerusalimsky Kinetic Model and Optimal Growth Rate Control of Fed-batch Cultivation Processes. Bioautomation, 2008, 11, Suppl., 1-12.
26. Pavlov Y. (2010). Preferences, Utility Function and Control Design of Complex process, Bucharest, Romania, Proceedings in Manufacturing Systems, V. 5, 4, 225-231, http://www.icmas.eu/ Volume5_No4_2010.htm#pp_22512
27. Pavlov Y., K. Ljakova. (2004). Equivalent Models and Exact Linearization by the Optimal Control of Monod Kinetics Models. BIOautomation, 2004, v.1, 231, Sofia, 42 – 56.
28. Pavlov, Y., (2011): Preferences based Stochastic Value and Utility Function Evaluation, Proceedings of "InSITE' 2011", InSITE Conferences, June 18-23, Novi Sad, Serbia, http://proceedings. informingscience.org/InSITE2011/index.htm.
29. Pirt J. (1975). Principles of Microbe and Cell Cultivation. Blackwell Scientific publications, Oxford.
30. Roeva O., T. Pencheva, B. Hitzmann, St. Tzonkov (2004). A Genetic Algorithms Based Approach for Identification of *Escherichia coli* Fed-batch Fermentation, Bioautomation, 1, 30-41.
31. Roeva, O. & all. (2007). Multiple model approach to modelling of *Escherichia coli* fed-batch cultivation extracellular production of bacterial phytase. Electronic Journal of Biotechnology, Pontificia Universidad Católica de Valparaíso – Chile, Vol.10 No.4, p.p. 592-603.
32. Selişteanu D., E. Petre, V. Răsvan. (2007). Sliding mode and adaptive sliding mode control of a class of nonlinear bioprocesses. Int. J. Adaptive Control and Signal Processing. V. 21, 795–822, Wiley InterScience, (www.interscience.wiley.com).
33. Staniskis, J.-K., Levisauskas, D., Smutis, U., Viesturs, M. Kristapsons (1992). Automation of Biotechnological Process: measurements, optimization and control. Zinatne, Riga, 1992.
34. Tzonkov, St., B. Hitzmann. (2006). Functional State Approach to Fermentation Process Modelling, Prof. Marin Drinov Academic Poublishing House, Sofia, Bulgaria, 2006.
35. Utkin. V. (1981). Sliding Mode and Applications in Variable Structure Control. Nauka, 1981 (in Russian).
36. Wang T., C. Moore, D. Birdwell. (1987), Application of a Robust Multivariable Controller to Non-linear Bacterial Growth Systems. Proc. of the 10-th IFAC Congress on Automatic Control, Munich, 39-56, http://www.ifac-control.org/events/congresses
37. Zelic B., D. Vasic-Racki, C. Wandrey, R. Takors. (2004). Modeling of the Pyruvate Production with *Escherichia coli* in a Fed-batch Bioreactor, Bioprocess and Biosystems Engineering, 26, 249-258.

    http://css.iict.bas.bg/staff/CV_Yuri%20Pavlov_E.pdf or

    http://www.researchgate.net/profile/Yuri_Pavlov_Juryi/

This page is intentionally left blank

Global Journal of Computer Science and Technology
Volume 11 Issue 20 Version 1.0 December 2011
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

An Approach for Effort Estimation having Reusable Components in Software Development

By Jyoti Mahajan, Devanand
University of Jammu, India

Abstract - Estimation of the effort required for development has been researched for over 25 years now. Still there exists no concrete solution to estimate the development effort. Prior experience in similar type of projects is a key for business today. This paper proposes an Effort Estimation Model named REBEE based on the reusable matrices to effectively estimate the effort to be involved for development. A project is assumed to consist of multiple modules and the reusability factor of each module is considered in the technique described here. REBEE utilizes fuzzy logic and dynamic neural networks to achieve its goal. Based on the experimental evaluation discussed in this paper it is evident that this model accurately predicts the effort involved on heterogeneous project types.

Keywords : *Software Effort Estimation, Software Reusability, Dynamic Neural Networks, Fuzzy Logic, REBEE.*

GJCST Classification : *D.2.9*

Strictly as per the compliance and regulations of:

An Approach for Effort Estimation having Reusable Components in Software Development

Jyoti Mahajan [α], Devanand [Ω]

Abstract - Estimation of the effort required for development has been researched for over 25 years now. Still there exists no concrete solution to estimate the development effort. Prior experience in similar type of projects is a key for business today. This paper proposes an Effort Estimation Model named REBEE based on the reusable matrices to effectively estimate the effort to be involved for development. A project is assumed to consist of multiple modules and the reusability factor of each module is considered in the technique described here. REBEE utilizes fuzzy logic and dynamic neural networks to achieve its goal. Based on the experimental evaluation discussed in this paper it is evident that this model accurately predicts the effort involved on heterogeneous project types.

Keywords : Software Effort Estimation, Software Reusability, Dynamic Neural Networks, Fuzzy Logic, REBEE.

I. Introduction

SOFTWARE EFFORT ESTIMATION is crucial to derive the effort involved in the successful completion of any project. Effort estimation techniques facilitate financial estimates, delivery timelines, help in beneficial resource allocation and scheduling, monitoring progress and also help in risk management. According to a recent survey conducted by McKinsey for NASSCOM [1] the IT and allied industries are expected to bring in revenues of about $225 Billion by 2020 in India alone and the current revenues are about $76 Billion. It is evident from these figures the growth rate of the software industry is impressive. The recent years have observed that software contracts are awarded to organizations having prior experience in handling similar project types.

Prior experience in the related project is the key for business growth. Organization benefiting from the software contracts would have multiple reusable modules for their future work. More over organizations develop codes so that they could be reused with some modifications for future use. This conservative approach adopted by the industry is to ensure timely deliveries, quality, reliability and financial assurance of their investments.

Author [α] : Assistant Professor in Computer Engineering Department, Govt. College of Engineering & Technology, Jammu, India. E-mail : jyoti_1972@sify.com.
Author [Ω] : Professor in Department of Computer Science & IT, University of Jammu, India. E-mail : padhadevanand@yahoo.com

COCOMO [3] and COCOMO 2.0[4], DELPHI [5], Function Point [6], Planning Poker [7], Use Case Point [8], Expert judgment [9], IBM – FSD [10] are the world known based estimation techniques, which are commonly used for Software Effort Estimation. These models exhibited a gross error of effort estimation. COCOMO with effort adjustment factor [11] provides about 30% improvement in effort variance, whereas when it is used with fuzzy logic, trapezoidal function and Gaussian functions showed improved performance [12]. Multiple software effort estimation techniques were integrated together to get the better result as compare to the regularly used estimation techniques, which was the big failure in terms of consistency when tested against several cases.

It was found that to achieve the good accuracy, Support Vector regression was combined with clustering approach. The estimation algorithm was vastly improved by the Mantel's correlation randomization test named Analogy-X [15]. This made the researchers to work even harder on the after effects of Schedule and Budget pressure on Effort Estimation and the development cycle time. Researchers have to be very careful while Chronological Splits are assigned for the testing and training purpose. Even Global Software Developments gets an inaccurate estimation technique being executed in different location of all over the world.

It has become very difficult to decide which model like COCOMO is best suitable for the development of the estimation model because of the different efforts to achieve estimation technique available in the market and the same outputs. The best solution for the estimation technique can be the judgment and the formal based model. In spite of all these available models and approaches, research shows the failure of projects due to various reasons [13]. Project Failures due to improper estimation techniques is also studied [14]. Based on this study it is evident that appropriate effort estimation techniques are critical for project success. The current existing techniques provide no proper estimation and are not applicable for varied project types.

To estimate effort for heterogeneous project types this paper discusses REBEE in the further sections of the paper. The remaining paper is organized as follows. The next section discusses the importance of

reusability and its adoption in the industry today. The third section discusses the REBEE model proposed. Section 3 also presents the Fuzzy rules to derive the reusability matrix and its use with dynamic neural networks to estimate effort. The penultimate section presents the experimental evaluation conducted using REBEE. The conclusion of the research presented here is discussed in the last section.

II. Reusablity and its Importance

The software industry today has witnessed various changes in its formulation, maintenance and management strategies to adapt to the dynamic changes it has experienced and for greater profitability. Experience held with organization in relevant or similar projects provides them with an business advantage as discussed earlier. These organizations possess modules which could be altered or used in total for their upcoming projects. The work described in this paper utilizes this knowledge of these reusable components to predict the effort required for the remaining work at hand. Incorporation and importance of reusability is currently been actively considered by major corporations now. Reusability is being considered for appraisals of employees of an organization [16] to reduce costs and maximizing profits [17]. Through these studies it is evident the adoption and importance of reusable components in the industry today and effort estimation using based on reusability could answer the anomalies that exist in the current estimation techniques adopted.

Fellow researchers have incorporated reusable weights into the existing COSYMO for cost estimation [18].Incorporation of the reusable parameters with the taguchi model [19], COCOMO2 [20],COCOMO [11] and COCOMO81[20] have been closely observed and these models exhibit considerable improvements but the error of estimation still exist. The error in estimation is basically due to the fact that the deficiencies of reusability's were not considered [21] which was considered to develop REBEE.

III. Rebee

a) *REBEE Preliminaries*

REusability Based Effort Estimation technique abbreviated as REBEE [2] consists of 4 phases as shown in Fig 1.

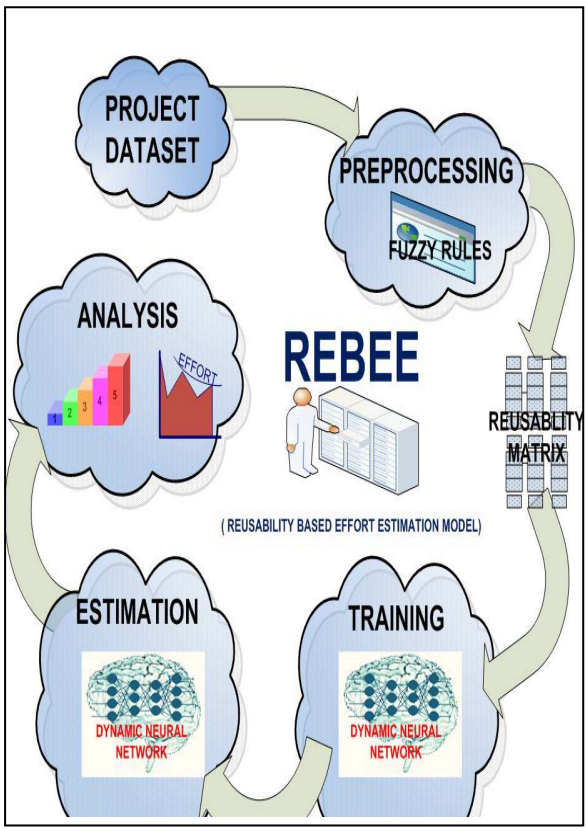


Figure 1 : REBEE Model

The effort estimation technique proposed consists of a pre processing phase where in the project data considered is analyzed to basically derive the reusability matrix. A project is assumed to be split into a number of modules and the reusability of each module is analyzed to derive the reusability matrix using fuzzy rules.

Estimation of the effort involved to achieve the project goals have been achieved using dynamic neural networks. Prior to estimation the dynamic neural networks are trained using the back propagation algorithm. The trained neural network could be used for estimation the effort involved. The results obtained could be analyzed for resource utilization, financial analysis, delivery time line assertion and many more critical analyses.

b) *Reusability Matrix using Fuzzy Logic*

A project is said to be composed of m modules. Modules could be either reusable or could be considered as new modules (m_n). Each reusable module is analyzed using a judgment model to arrive at the reusable component present. The modules are analyzed at an implementation level and for characterization a threshold ϑ is defined which is arrived based on the judgment model. On characterization the modules are further classified into 3 categories as

- Completely reusable.

A module is considered to be completely reusable if it could be utilized without any changes or

without altering any code or design and is represented as m_{cr}

- Reusable with fractional adaptation

A module is considered as a reusable model with partial adaption if at the implementation level the changes to be incorporated are less than the threshold ϑ and is represented as m_{fr}

- Reusable with prominent adaptation

If the changes to be incorporated are greater than the threshold ϑ then the module is considered as a reusable module with prominent adaption represented by m_{pr}.

Let Δ represent the changes to be incorporated into a module m for it to be compatible with the project for which estimation is to be achieved. Applying the fuzzy rules the modules could be characterized as follows

$$\begin{Bmatrix} m = m_{cr} \text{ if and only if } \Delta = 0 \\ m = m_{fr} \text{ if and only if } \Delta < \vartheta \\ m = m_{fr} \text{ if and only if } \Delta \geq \vartheta \end{Bmatrix}$$

Consider R to represent the reusable matrix. The effort involved to develop the modules earlier is represented as $\mathcal{E}$. Let us consider that there exist $x, y \text{ and } z$ number of $m_{cr}, m_{fr} \text{ and } m_{pr}$ modules and their development efforts considered be defined as $\mathcal{E}_{cr}, \mathcal{E}_{fr} \text{ and } \mathcal{E}_{pr}$. Then the reusability matrix obtained based on fuzzy logic could be represented as

$$R = \begin{bmatrix} m_{cr1} & \mathcal{E}_{cr1} & m_{fr1} & \mathcal{E}_{fr1} & m_{pr1} & \mathcal{E}_{pr1} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ m_{crx} & \mathcal{E}_{crx} & m_{fry} & \mathcal{E}_{fry} & m_{prz} & \mathcal{E}_{prz} \end{bmatrix}$$

c) Estimation using Dynamic Neural Networks

To estimate the effort involved REBEE uses neural networks. Neural networks of static type are not considered to develop this effort estimation technique as they possess adaptive and learning capabilities for only static in-out relationships. To effective adapt and learn the dynamic input output of the non linear matrices REBEE uses dynamic neural networks. The dynamic Neural Network Adopted in this model is as shown in Fig 2.

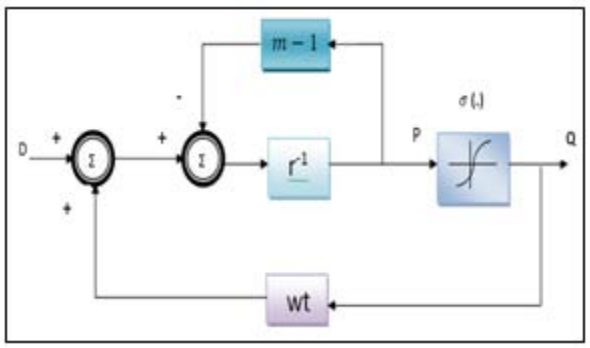


Figure 2 : Dynamic Neural Network with Back Propagation Learning

Dynamic neural networks have been considered as they could be utilized to observe effort related dynamics of the input pattern matrices. The use of dynamic neural networks is not only related to obtaining effort related dynamics but also could be utilized to obtain non effort related dynamics observed for effort related input matrices.

The reusable matrix obtained from the pre processing phase is considered for training of the dynamic neural networks. The training is achieved using the back propagation algorithm. The output of the dynamic neural network $r(k)$ with respect to the input $p(k)$ is given by

$$p(k+1) = -(m-1)p(k) + wtq(k) + d$$
$$r(k) = \sigma\big(p(k)\big)$$

Where σ represents the sigmoid activation function and $(m-1)$ is the feedback where m is the learning rate constant.

The error of estimation $E(k)$ is defined as

$$E(k) = \frac{1}{2}\big(p_d(N) - p(N)\big)^2 + \frac{1}{2}\sum_{k=0}^{N-1}[p_d(k) - p(k)]^2$$

$$= \frac{1}{2}e^2(N) + \frac{1}{2}\sum_{K=0}^{N-1} e^2(k)$$

The weight update function $\Delta wt(k)$ propagated through the dynamic neural network is given as

$$\Delta wt(k) = -m\frac{\partial E}{\partial wt} = m\sum_{k=0}^{N-1} r(k+1) f_{wt}(p(k), wt)$$

The updated weights propagated to the next neuron based on the previous neuron is given as

$$wt(k+1) = \{wt(k)$$
$$- m_{wt} \sum_{k+0}^{N-1} r(k+1)\, f_{wt}(p(k), wt)\}$$

The trained neural network is queried with the project data provided which provides the effort estimated on the remaining modules using the following equation where E represents the effort.

$$p(k+1) = -(m\mathrm{E} - 1)p(k) + \mathrm{E}f(p(k), wt) + \mathrm{E}d(k)$$

This section of the paper described the REBEE technique proposed through this paper. The validation of this model is provided in the next section.

IV. Experimental Validation of the Rebee Technique

This section of the paper would discuss the experimental evaluation of the discussed REBEE model. For evaluation 39 projects of NASA Goddard Space Flight Center Greenbelt, Maryland is considered [22]. The dataset consists of projects related to simulators and altitude ground support systems developed by the Flight Dynamics Division of Goddard Space Flight Center situated in Maryland USA. The simulator projects considered were categorized into dynamic simulators and telemetry simulators. The 39 projects considered were said to be developed in 3 phases. Phase 1 consist of the design Phase. The coding was considered as the second phase and the last phase was the testing phase. For evaluation purpose the effort involved in providing support towards these projects developed was not considered.

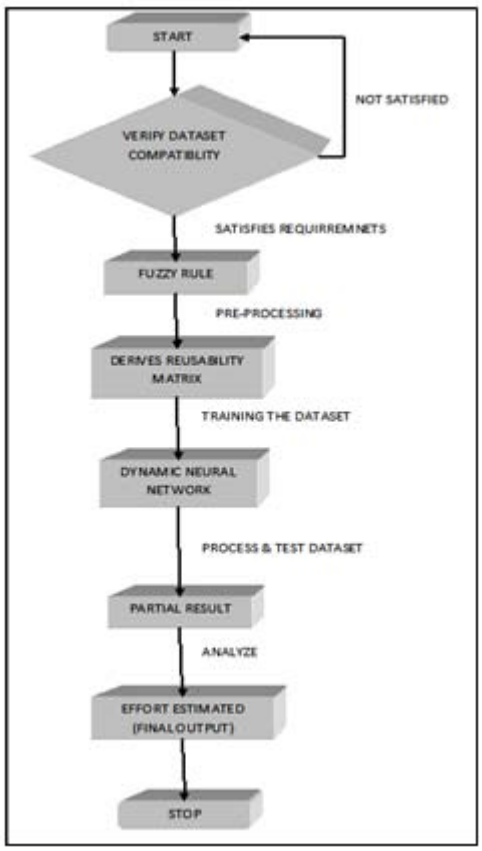


Figure 3 : Experimental Evaluation Flow Diagram

The data set considered provided details with respect to the number of lines of source code required in developing these projects. Reusability of the code was also considered in the development of the projects in the data set. The data set defined reusability of 3 types. A completely reusable code was considered if there were no changes to be incorporated for the new project considered. If the changes to be incorporated in the code were less than 25% (i.e. threshold ϑ in REBEE) then it was considered to be a reusable code that requires slight modification. If the modification exceeded the threshold ϑ the code was considered to be reusable but with extensive modification. For evaluation presented here these matrices were considered to derive the reusability matrix$R$.

REBEE was developed using C# on a visual Microsoft Visual Studio 2010 platform. The reusability matrix derived using the fuzzy rule was provided to the dynamic neural network in the training process. The trained dynamic neural network on querying provides the effort estimated phase wise and for the entire project. The experimental evaluation process considered is shown as a flow chart in Fig 3.The dataset considered consists of heterogeneous project having varied development platforms and also exhibiting varying reusability levels. For evaluation projects were clustered into 4 types mentioned below

- Minor Reuse
- Standard Reuse
- High Reuse
- Maximum Reuse types.

If the reusability of a project was found to be less than or equal to 20% it was considered to be of Minor Reuse Type. If the reusability percentage of a project was between twenty and fifty, it was considered as a project of Standard Reuse type. If the percentage of reusability of a project was between fifty and eighty it was considered as a project of High Reuse. Projects embodying components which were more than 80% reusable was considered as maximum reusable projects. This clustering was adopted to provide for effective and efficient training to neural network to understand the dynamics of reusability. The effort estimated versus the actual effort involved in the design phase of the 39 projects is shown in Fig 4.The effort estimated using REBEE for the coding and the testing phase is shown in Fig 5 and Fig 6. The effort estimation for the entire project which includes the design, coding and the testing phase is as shown in Fig 7. The horizontal axis of the graphs represent the project ID and the effort in man hours id plotted on the vertical axis of the graph.

The results obtained from the evaluation of the 39 projects considered exhibited a low average error in effort estimation of about 1.25%. The average error in effort estimation for the design phase was 1.34%, 1.38% for the coding phase and 2.29% for the testing phase respectively. Based on the graphical data provided and the low average error of estimation it is evident that the reusability based effort estimation technique presented in this paper could be effectively utilized to estimate the effort involved in developing a project.

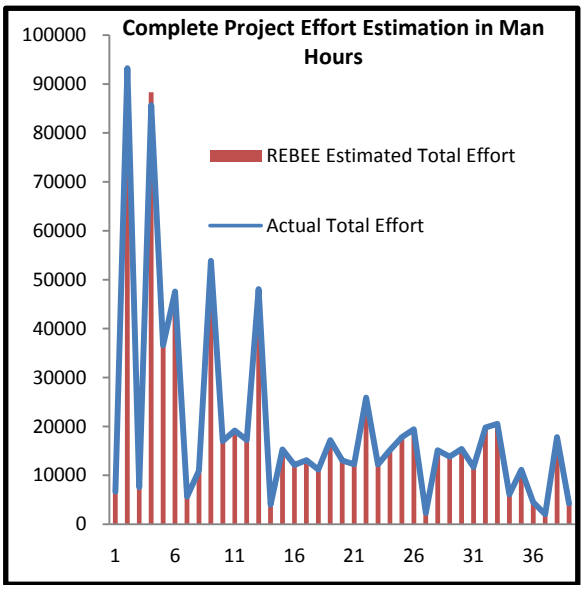


Figure 4 : Effort Estimation using REBEE Versus Actual Effort for 39 NASA Projects

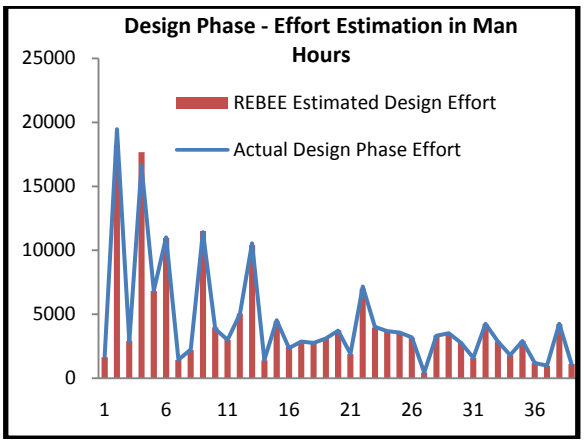


Figure 5 : Effort Estimation using REBEE Versus Actual Effort for the Design Phase

V. Concluding Remarks

Accurate effort estimation techniques are critical for the successful project execution. The importance of reusability and its remarkable acceptance by the industry today is evident from the research work presented through this paper. This paper discusses a reusability based effort estimation technique named REBEE.

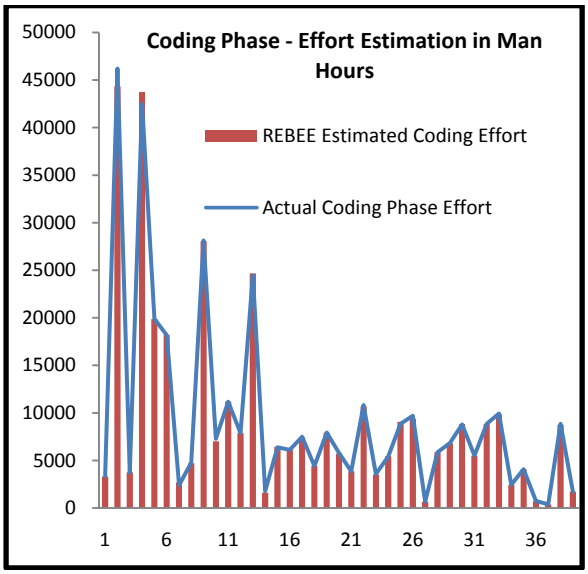


Figure 6 : Effort Estimation using REBEE Versus Actual Effort for the Coding Phase

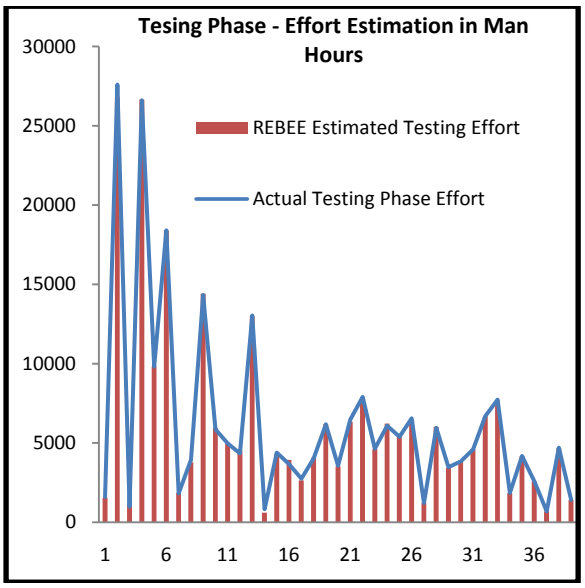


Figure 7 : Effort Estimation using REBEE Versus Actual Effort for the Testing Phase

REBEE achieves effective effort estimation utilizing the benefits of fuzzy logic and dynamic neural networks. Training of the dynamic neural networks is achieved using the back propagation algorithm. Fuzzy rules are adopted in constructing the reusability matrix which is utilized by the neural network to understand the dynamics of the effort involved in constructing the reusable components. Based on this understanding the dynamic neural network estimates the remaining effort involved in project completion.

The REBEE model discussed is evaluated on 39 NASA projects which are of different kinds. The development languages for these projects also varied from project to project. The reusability level of the

projects varied from about 0% to a high of 96%. The effort estimated using REBEE on all the 3 project phases i.e. Design, Coding and Testing and on the cumulative effort required in developing the projects showed high levels of accuracy. The average estimation error for all the 39 projects was also a low of about 1.25% which proves the efficiency of REBEE. From the evaluation results obtained it could be concluded that reusability based effort estimation technique discussed in this paper could be a possible solution for accurate effort estimation for projects of varied types which is not possible with the currently existing effort estimation techniques.

Acknowlewdgement

The authors would like to express their cordial thanks to Prof. Bhopinder Singh, Principal of Government College of Engineering and Technology, Jammu for their financial support and advice.

References References Referencias

1. NASSCOM "Perspective 2020: Transform Business, Transform India" http://www.nasscom.in/upload/Perspective%202020%20Press%20release%20presentation.pdf
2. J. Mahajan, Devanand, K. Dhruve, "REBEE Reusability Based Effort Estimation Technique using Dynamic Neural Network", *Global Journal of Computer Science and Technology*, volume 11 Issue 7 ver 1.0 May 2011.
3. B.W. Boehm, W.W. Royce, Le COCOMO Ada, *Genie logiciel & Systemes experts*, 1989.
4. B.W. Boehm, et al., "Cost Models for Future Software Life Cycle Processes: COCOMO2.0", *Annals of Software Engineering on Software Process and Product Measurement*, *Amsterdam,* 1995.
5. Website:http://www.stellman-greene.com/aspm /images/ch03.pdf.
6. Meli, R., L. Santillo, "Function point estimation methods: a comparative overview", in Proc. 1999 *The European Software Measurement Conference – Amsterdam,* October 6-8.
7. Webreference : http://www.mountaingoatsoftware.com/system/presentation/file/51/bayXP_070320_PlanningAgileProjects.pdf
8. S. Nageswaran "Test effort estimation using use case points" in *14th International Internet Software Quality Week 2001*, *San Francisco, California, USA,* June 2001.
9. M. Jørgensen, "Practical Guidelines for Expert-Judgment- Based Software Effort Estimation," *IEEE Software,* vol. 22, pp. 57-63, May-June 2005.
10. C.E. Walston, A.P. Felix, "A method of programming measurement and estimation," *IBM Systems Journal*, vol. 16, no.1, 1997.
11. M.J. Basavaraj, K.C Shet, "Empirical validation of Software development effort multipliers of Intermediate COCOMO Model" *Journal of Software*, vol. 3, vo. 5, pp 65 MAY 2008.
12. C.S. Reddy, KVSVN Raju, "An Improved Fuzzy Approach for COCOMO's Effort Estimation using Gaussian Membership Function". *Journal of Software*, vol. 4, no. 5, pp. 452-459, 2009.
13. C.E.L. Peixoto, J.L.N. Audy, R. Prikladnicki, "Effort Estimation in Global Software Development Projects: Preliminary Results from a Survey," in Proc. 2010 *5th IEEE International Conference on Global Software Engineering, ICGSE*, pp.123-127.
14. K. Molkken, M. Jorgensen, "A Review of Surveys on Software Effort Estimation," Proc. 2003 *International Symposium on Empirical Software Engineering (ISESE'03), pp. 223.*
15. E. Kocaguneli, A. Tosun, A. Bener. "AI-Based Models for Software Effort Estimation" in Proc. *36th EUROMICRO Conference on Software Engineering and Advanced Applications*, pp.323-326.
16. P.S. Sandhu, H. Singh, "Automatic Reusability Appraisal of Software Components using Neuro-Fuzzy Approach", *International Journal of Information Technology*, vol. 3, no. 3, pp. 209-214, 2006.
17. P.S. Sandhu, H. Kaur, A. Singh, "Modeling of Reusability of Object Oriented Software System", *Journal of World Academy of Science, Engineering and Technology,* no. 56, pp 162 August 2009.
18. G. Wang, R. Valerdi, J. Fortune, "Reuse in Systems Engineering", *IEEE Systems Journal*, vol. 4, no. 3, pp 376-384, September 2010.
19. P. S. Sandhu, P. Blecharz, H. Singh, "A Taguchi Approach to Investigate Impact of Factors for Reusability of Software Components", *Journal of World Academy of Science, Engineering And Technology*, vol 25, pp 135-140, 2008.
20. CH.V.M.K.Hari, P.V.G.D.P Reddy, J.N.V.R.S Kumar, G.SriRamGanesh. CH.V.M.K. Hari., "Identifying the Importance of Software Reuse in COCOMO81, COCOMOII", *International Journal of Computer Science and Engineering JCSE,* vol. 1 no. 3, pp 142-147, 2009.
21. N. Ozarin, "Lessons Learned on Five Large-Scale System Developments" *IEEE Instrumentation & Measurement Magazine*, nol. 11, Issue- 1, pp 18-23, February 2008.
22. S. Condon, M. Regardie, M. Stark, etal., "Cost and Schedule Estimation Study Report", Goddard Space Flight Center Greenbelt, Maryland 20771. SEL-93-002 .pp 1- 119 November 1993.

Global Journal of Computer Science and Technology
Volume 11 Issue 20 Version 1.0 December 2011
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Cost Model for Reengineering an Object Oriented Software System

By Dr. Ashok Kumar, Bakhshsish Singh Gill
Kurukshetra University, Kurukshetra

Abstract - The cost of reengineering of object-oriented software is often significantly less than the cost of developing new software. Object oriented software systems are more reusable. Reengineering of software systems rather than developing new software will save precious time and resources. Reengineering reduces the cost of maintenance by increasing the software quality and reducing complexity.To justify reengineering, the cost of reengineering software must be estimated and compared with the cost of new software. The cost of reengineering depends upon many factors but major factors are the portion of the software (number of objects) to be reengineered and complexity (interrelationship between objects) of the software. In this paper efforts are done to present a reengineering cost estimation model. On the basis of this model, software managers can take a decision whether to maintain, reengineer or retire the software.

Keywords : *Objects, reengineering, complexity, fine object, faulty object.*

GJCST Classification : *D.1.5*

Strictly as per the compliance and regulations of:

Cost Model for Reengineering an Object Oriented Software System

Dr. Ashok Kumar [α], Bakhshsish Singh Gill [Ω]

Abstract - The cost of reengineering of object-oriented software is often significantly less than the cost of developing new software. Object oriented software systems are more reusable. Reengineering of software systems rather than developing new software will save precious time and resources. Reengineering reduces the cost of maintenance by increasing the software quality and reducing complexity.To justify reengineering, the cost of reengineering software must be estimated and compared with the cost of new software. The cost of reengineering depends upon many factors but major factors are the portion of the software (number of objects) to be reengineered and complexity (interrelationship between objects) of the software. In this paper efforts are done to present a reengineering cost estimation model. On the basis of this model, software managers can take a decision whether to maintain, reengineer or retire the software.

Keyterms : Objects, reengineering, complexity, fine object, faulty object.

I. Introduction

The ability to accurately estimate the time and cost of reengineering software is the key factor for successful of reengineering project. Cost estimation is needed before reengineering is initiated. The primary objective is to enable the client and software engineer to perform a cost benefit analysis. The estimate can be in terms of person-month (PM), which can be translated into actual rupees cost. Cost estimation is not easy task; many factors in estimation are not quantifiable. Also reengineering area is young and needs much maturity and improvement. Quality of software design matters in the process of estimation. Easiness in software understanding, maintenance and reengineering depends upon the decomposition of system.

In successive generation of languages decomposition is supported differently. The advancement in the software technology, from machine language to assembly to procedural to object-oriented languages, helps programmers to estimate time and efforts for software development. Object - oriented technology is more helpful in measuring reengineering cost as it uses objects and not algorithms as its fundamental building blocks. In this context, object is not object of some object oriented language but it is a conceptual module than can be plugged in and plugged out from the software system. Reengineering identifies reusable components (objects) and analyzes the changes that would be needed to regenerate them for reuse within new software architecture. The use of a repeatable, clearly defined and well understood software objects, has make reengineering more effective and reduced the cost of reengineering.

II. What is an Object?

I thought of an object in the context of object-oriented technology as independent component that can be pulled out and plugged in the software system. Object is taken as a private, separable independent module of software. If we pull out an object from a software system, it is working system without much affecting the whole system except the job done by that particular object. As in the other physical systems, a component is plugged out, repaired and plugged in the system again. Additional screws, nuts and bolts are required for this purpose. We must develop a universal language of such type. We must have a set of additional instructions as nuts and bolts to plug-out and plug-in the objects in the whole system. Following figure shows an object which is an independent unit of software that can be interfaced with the software system.

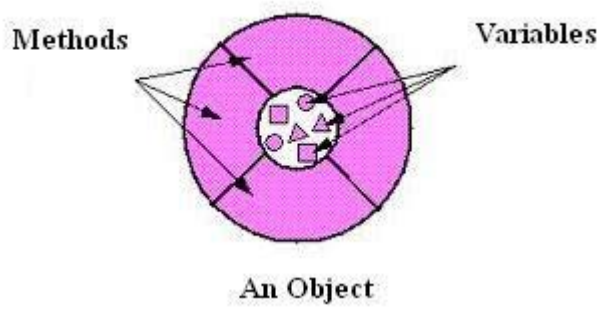


Fig. 1

The object oriented approach attempts to manage the complexity inherent in the real world problems by abstracting out knowledge and encapsulating it [1]. Object is an instance of a class and has an identity and stores attribute values [2].

Author [α]: Professor, Department of Computer Applications, Kurukshetra University, Kurukshetra, Phone: 01744-238195(Office), 01744-239231(Residence)
Author [Ω] : Sr. Programmer, Computer Centre, Guru Nanak Dev University, Amritsar-143001, E-mail bbssgill@yahoo.com, Phone 0183-2258802-09 Ext. 3297(Office), 0183-2502813(Residence) , Mobile 9988112620

Here in this piece of work, Object is seen at a higher level of abstraction and is taken as independent module or unit that can be plugged in or plugged out of the software system. As software ages some objects become faulty (new term coined). Faulty objects are indentified and modified. Faulty object is that which hang without responding or if responding to some operation, its response is incorrect. Candidate software system is disbanded; all objects of the system are separated. Faulty objects are identified and collected for reengineering. Old design of the software is examined (Reverse Engineering). Then redesigning of the structure of the system to improve the quality of software system is done (transformation of the architecture). According to new quality and modern design objects are integrated (Forward Engineering).

Following is the example of object oriented software system with eight objects like real world objects. Circles are objects and lines represent communications to send messages between objects. The object in the system is characterized with three properties Identity, State and Behavior. Identity distinguishes it from others, state is the data stored in it and behavior describes the methods by which the objects can be used.

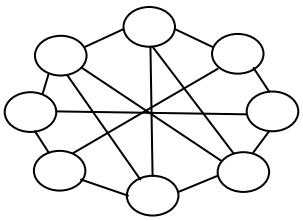


Fig. 2 : object oriented software system

Abstraction is good tool for reengineering object oriented design as it helps in reducing complexity. Large systems are complex having more objects as each additional object increases the complexity of the system [3].

III. Need for Reengineering

Software maintenance starts after delivery of the software to correct faults, to improve performance and other attributes of the software. Maintenance plays an important role in the life cycle of a software system. Maintenance is the last stage of the software life cycle. After the product has been released, the maintenance phase keeps the software up to date with environment changes and user requirements changes. With recurring maintenance, complexity increases and software quality decreases. As the software is maintained, errors are introduced. Many studies have shown that each time an attempt is made to decrease the failure rate of a system, the failure rate got worse. On average, more than one error is introduced for every repaired error. In this way maintenance cost goes on increasing with time. Software maintenance can account for 60 to 80 percent of the total life cycle of software product. More than 90 % of the total cost of software goes to maintenance and evolution of the software product [4].

After a certain period, there is a crucial point when it is difficult to maintain the system or maintenance cost is too much high. Maintenance problems are a driving force behind re-engineering. Reengineering is the only way to avoid development cost. But what is the cost of reengineering software? If we do not know how can we go for reengineering? If the cost of reengineering is known then it can be compared with the cost of the new system.

In the following figure, maintenance cost is raising high from red point D onward. At this time we think of reengineering or retiring the software because maintenance cost increases rapidly. System can be maintained well if this situation does not arise.

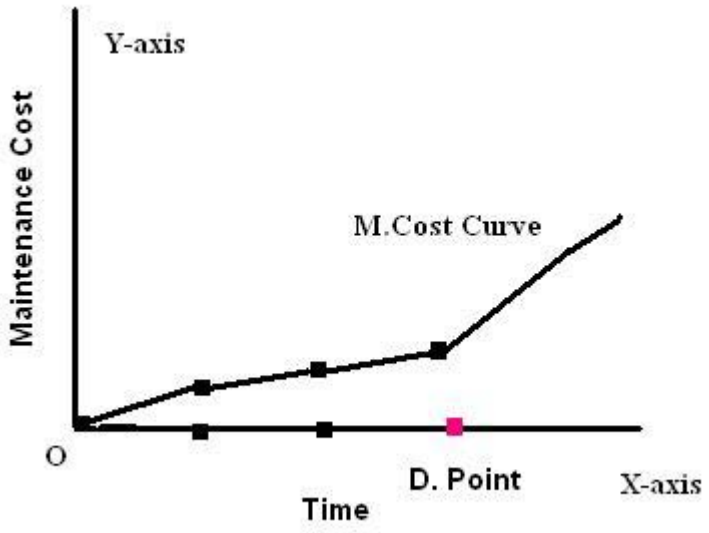


Fig. 3 : Decision point D

Now software managers are worried for making decision for reengineering at point D. Name D is given as it is a decision point for the software managers. If we retire the system then we have to bear the cost of new software and naturally it will be high cost.

At this time, the cost model will help the software managers to compare the quoted cost of new software with cost of reengineering. Certainly reengineering will attract the software managers. Reengineering can not be escaped. Reengineering is the only way to utilize the resources fully and the problem of backlog of software will also be solved.

IV. Reengineering Cost Model

Object-oriented paradigm has changed the scene for reengineering. Object-oriented software system is all about objects. Object-Oriented software system is being more reusable and hence more suitable for reengineering. Reengineering of software systems rather than developing new software will save precious time of skilled engineers and legacy resources. Reengineering reduces the cost of maintenance and to escape the new software development. Maintenance cost increases as software ages. Maintenance problems are a driving force behind reengineering. To justify reengineering, the cost of reengineering software must be calculated and it should be less than the cost of purchasing new software with a great difference. The cost of reengineering depends upon many factors but major factors are the portion of the software (number of objects) to be reengineered and complexity (interrelationship between objects) of the software. Cost model will help organizations whether to reengineering the software system or to buy new software. This is a major decision faced by the software managers. In this paper efforts are done to present a cost model for reengineering legacy object oriented software system.

To calculate the cost of reengineering the following factors are taken into consideration.

1. Number of objects to be reengineered.
2. Size of the object (Number of attributes)

Each object has its own attributes, but attributes are taken into consideration according to requirement specification and business process. For example attributes of object employee are name, employee identification code, address, mobile phone, landline phone, age, height, color, basic pay, grade pay and many more. If software is required for payroll of the employee, the attributes like height, age, color etc is not required. Number of attributes depends upon the size of the problem.

Reengineering cost depends upon the number of objects to be reengineered. It means reengineering cost of an object is to be calculated to calculate the reengineering cost for the software system. The candidate object is called faulty object. On average half of the objects could be candidate objects. Following is the figure of software system with some 7 faulty objects. This system can be maintained as faulty objects are less than half.

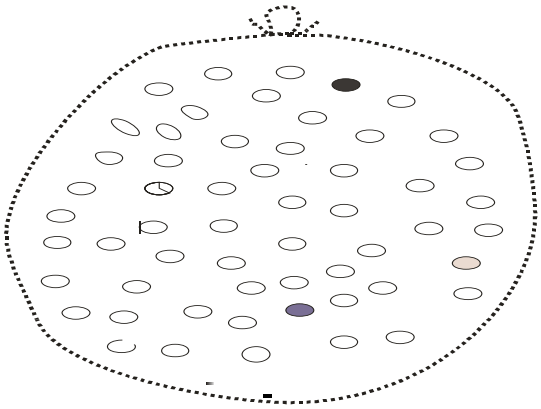


Fig. 4 : Application System with faulty objects

Application software system (in figure 3) can be maintained by modifying the faulty objects and need not reengineering. Number of faulty objects increases with the age of software. System is candidate for reengineering when the faulty objects number reaches to half. These faulty objects can be reengineered and can be plugged to enhance the functionality of the application.

V. Reengineering Cost of the Candidate Object

Traditional software measurement techniques are not satisfactory for measuring productivity and predicting efforts for object oriented software systems. The Source Lines of Code (SLOC) metric and the Function Point metric both were for programming environment putting the data and procedures separate. In object oriented paradigm data and procedures are combined. In object oriented approach the role of UML is supreme. It was designed to provide a standard for software modeling languages. It is a graphical notation for object-oriented analysis and design. UML provides a framework for describing a set of models that capture the functional and structural semantics of any complex information system. UML constructs in object oriented software can be used for estimation of resources like efforts & cost etc. While calculating the efforts of reengineering it is important to include information about communication between objects and reuse through inheritance in the size of the object (Lines of code) as well. An object is small piece of source code that can be maintained or reengineered.

Common and simple approach for measuring efforts for developing small software with single variable is as under

Efforts = a*(SIZE)b where a and b are constants determined by regression analysis applied to historical data [5]. SIZE is a variable and the value of this variable depends upon the size of the object. The SIZE is the

number of lines of code. This model is for the structured software systems. This model measures the efforts for developing software from scratch. Reengineering the legacy software object will take the efforts to half.

Efforts for reengineering small piece of source code as an object can be calibrated as under

Efforts == [a*(number of attributes)b] / 2 where a, b are constants and can be determined from historical data(from past experience) of reengineered software systems. If we denote number of attributes of an object involved in computations by A, then the above model will be as under

Efforts = E1= [a*(A)b] / 2 Person Months for an object say O1.

This model estimates the total efforts for reengineering an object, a small piece of code that can be plugged in with the object oriented application. Cost of reengineering all the faulty objects will be estimated by adding all above such Ei's. Let us suppose there are n faulty objects then cost of reengineering of all the objects will be $E_1+E_2+E_3+\ldots\ldots\ldots E_n$.

VI. Reengineering Cost of Software System

In the beginning, behavior of Legacy software system (Object-Oriented) is examined. The system is disbanded; objects are identified and separated for reengineering. Cost model for reengineering an object is presented above as efforts for reengineering an object O_1 will be E_1. With this model, reengineering cost of all the faulty objects is calculated separately. Let us suppose our candidate system is with n faulty objects say $O_1, O_2, O_3,\ldots\ldots\ldots\ldots O_n$ Reengineering cost of all the n objects will be added and is equal to $E_1+E_2+E_3+\ldots\ldots\ldots E_n$. Now all the objects are fine and we need to integrate them into a system. At this stage software architecture will also be changed (improved). There will be additional efforts (cost) for identifying the faulty objects, transformation of the architecture and integrating them into the new design. We denote it by C_n; the constant is to be determined after verifying the results by empirical data available from the past reengineered systems. Then the total efforts for reengineering the object oriented software system will be as under

$$E = E_1+E_2+E_3+\ldots\ldots\ldots E_n. + C_n$$

E is total Person Months of reengineering of software system with n faulty objects. Efforts $E_1, E_2, E_3,\ldots\ldots\ldots E_n$ are person months of reengineering n faulty objects $O_1, O_2, O_3,\ldots\ldots\ldots\ldots O_n$ respectively. Person Months can be multiplied by the current rupees rate of Person Month work.

Estimated reengineering cost = Estimated Effort * current Rate of Person-Month. If we denote current rate in rupees for person months by R then cost model will be as under

Cost = E*R

VII. Results and Conclusions

In this piece of work cost model for reengineering object oriented software system is presented which will be valuable to both the community's software managers and software engineers. Firstly cost model for reengineering an individual object is presented as Efforts = [a*(A)b] / 2 Person Months where constants a and b are to be determined, A is the number of attributes of the object. Cost model for reengineering software system is 'Cost = E * R'

This model is indispensable to organizations as they can settle the deal for reengineering software and can escape buying the new software.

VIII. Future Work

In this paper, software system is viewed as system of real world objects. Object is seen as packed separable module that can be plugged in and plugged out of the software system. System is disbanded (split up/break up) and faulty objects are identified for reengineering. These objects are renovated and arranged as to improve the design structure, packed to work as a system. On this concept reengineering cost model is calibrated.

The future work is to test it for suitability to fit in on the basis of analysis of past data. The constants 'a' 'b' and 'Cn' are unknown and to be determined. These constants can be found out from the past experience by collecting empirical data from reengineered object-oriented software projects. Near about 50-80 projects can be judged to fit this model. With suitable values of above constants in discussion, the reengineering cost model for object oriented software systems is ready. This model will facilitate both the communities the software engineers and the software managers.

References References Referencias

1. Brock R.W.,Wilkerson B., Wiener L. (2007) "Designing Object-Oriented Software", Prentice-Hall of India, New Delhi p. 5.
2. Bernd Bruegge, Dutoit Allen H., "Object-Oriented Software Engineering Using UML, Patterns, and Java", Pearson Education (Singapore), p.724.
3. Halladay S., Wiebel M., "Object-Oriented Software Engineering", BPB Publications, New Delhi. P. 35.
4. Erlikh, L. (2000). "Leveraging legacy system dollars for E-business". (IEEE) IT Pro, May/June 2000, 17-23. Down loaded on 24-02-2011 from the site: http://users.jyu.fi/~koskinen/smcosts.htm
5. P. Jalote (1996). "An Integrated Approach to Software Engineering", Narosa Publishing House , New Delhi. P. 88.

Books

1. Sal Valenti, "Successful Software Reengineering", IRM Press, 1331 E., Chocolate Avenue, Hershey, 2002.
2. Robert S. Arnold, "Software Reengineering", IEEE Computer Society Press Los Alamitos,California
3. Roger S. Pressman, "Software engineering", 3rd ed., McGraw-Hill, New York, 1992.
4. Grady Booch, "Object-Oriented Analysis and Design with Applications", Pearson Education, Singapore, 2003.
5. IAN Sommerville, "Software Engineering", Addison-Wesley Publishing Company, Singapore, 1994.
6. K.K.Aggarwal and Yogesh singh, " Software engineering", New age International (P) Ltd., Publishers, New Delhi, 2002.
7. Nasib Singh Gil, " Software Engineering: software reliability, Testing and Quality Assurance", Khanna Book Publishing Co.(P) Ltd., New Delhi, 2002.

Web Sites

http://journals.ecs.soton.ac.uk/java/tutorial/java/objects/object.html dated 1/8/2011
http://softwaredesign.com/objects.html dated 13/8/2011

This page is intentionally left blank

Global Journal of Computer Science and Technology
Volume 11 Issue 20 Version 1.0 December 2011
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

SEAD-FHC: Secure Efficient Distance Vector Routing with Fixed Hash Chain length

By Prasuna V G, Dr. S. Madhusudhana Verma
Rayalaseema University, Kurnool, Andhra Pradesh

Abstract - Ad hoc networks are highly dynamic routing networks cooperated by a collection of wireless mobile hosts without any assistance of a centralized access point. Secure Efficient Ad hoc Distance Vector (SEAD) is a proactive routing protocol, based on the design of Destination Sequenced Distance Vector routing protocol (DSDV). SEAD provides a robust protocol against attackers trying to create incorrect routing state in the other node. However, the computational cost creating and evaluating hash chain increases if number of hops in routing path increased. In this paper, we propose Secure Efficient Ad hoc Distance Vector with fixed hash chain length in short SEAD-FHC protocol to minimize and stabilize the computational complexity that leads minimization in delay time and maximization in throughput. A series of simulation experiments are conducted to evaluate the performance.

Keywords : *Mobile ad hoc networks; Ad hoc network routing; Secure routing; SEAD; Hash chains.*

GJCST Classification : *E.2, E.3*

Strictly as per the compliance and regulations of:

SEAD-FHC: Secure Efficient Distance Vector Routing with Fixed Hash Chain length

Prasuna V G [α], Dr. S. Madhusudhana Verma [Ω]

Abstract - Ad hoc networks are highly dynamic routing networks cooperated by a collection of wireless mobile hosts without any assistance of a centralized access point. Secure Efficient Ad hoc Distance Vector (SEAD) is a proactive routing protocol, based on the design of Destination Sequenced Distance Vector routing protocol (DSDV). SEAD provides a robust protocol against attackers trying to create incorrect routing state in the other node. However, the computational cost creating and evaluating hash chain increases if number of hops in routing path increased. In this paper, we propose Secure Efficient Ad hoc Distance Vector with fixed hash chain length in short SEAD-FHC protocol to minimize and stabilize the computational complexity that leads minimization in delay time and maximization in throughput. A series of simulation experiments are conducted to evaluate the performance.

Keywords : Mobile ad hoc networks; Ad hoc network routing; Secure routing; SEAD; Hash chains.

I. Introduction

Secure Ad Hoc network routing protocols are complex to design, due to the generally highly dynamic nature of an ad hoc network and due to the need to operate efficiently with limited resources, including network bandwidth and the CPU processing capacity, memory, and battery power (energy) of each individual node in the network. Existing insecure ad hoc network routing protocols are often highly optimized to spread new routing information quickly as conditions change, requiring more rapid and often more frequent routing protocol interaction between nodes than is typical in a traditional (e.g., wired and stationary) network. Expensive and cumbersome security mechanisms can delay or prevent such exchanges of routing information, leading to reduced routing effectiveness, and may consume excessive network or node resources, leading to many new opportunities for possible Denial-of-Service attacks through the routing protocol.

Routing protocols for ad hoc networks generally can be divided into two main categories: Periodic protocols and On-demand protocols. In a periodic (or proactive) routing protocol, nodes periodically exchange routing information with other nodes in an attempt to have each node always know a current route to all destinations (e.g.,[22,23,24,25,26, 27,28]). In an on-demand (or reactive) protocol, on the other hand, nodes exchange routing information only when needed, with a node attempting to discover a route to some destination only when it has a packet to send to that destination (e.g., [1,29,30]). In addition, some ad hoc network routing protocols are hybrids of periodic and on-demand mechanisms (e.g., [31]).

Each style of ad hoc network routing protocol has advantages and disadvantages. In this paper, we focus on securing ad hoc network routing using periodic (or proactive) protocols, and in particular, using distance vector routing protocols. Distance vector routing protocols are easy to implement, require relatively little memory or CPU processing capacity compared to other types of routing protocols, and are widely used in networks of moderate size within the (wired) Internet [32,33,34]. A number of proposed periodic ad hoc network routing protocols are based on adapting the basic distance vector routing protocol design for use in mobile wireless ad hoc networks, including PRNET [26], DSDV [28], WRP [27], WIRP [25], and ADV [23]. Distance vector routing has also been used for routing within a zone in the ZRP hybrid ad hoc network routing protocol [31].

Ad-hoc network is a computer network in which the communication links are wireless and the devices on it communicate directly with each other. This allows all wireless devices within range of each other to discover and communicate in a peer-to-peer fashion without involving central access points.

An ad-hoc network tends to feature a small group of devices all in very close proximity to each other. Performance degrades as the number of devices grows, and a large ad-hoc network quickly becomes difficult to manage.

To design an Ad hoc network routing protocol is challenging, and to design a secure one is even more difficult. There are many research focus on how to provide efficient [35, 36] and secure [37, 38] communication in ad hoc networks.

The Secure Efficient Ad hoc Distance Vector (SEAD) [40] protocol uses one-way hash chains to prevent an attacker from forging better metrics or sequence numbers. But SEAD does not prevent an attacker from tampering other fields or from using the learned metric and sequence number to send new routing updates. In this paper, we proposed a new

Author α : Assocaite Prof., Department Of MCA, Basaveswara Institute Of Information Technology, Hyderabad, AndhraPradesh, INDIA-500027.

Author Ω : Professor & Head, Department of OR & SQC, Rayalaseema University, Kurnool, Andhra Pradesh, India – 518002.

protocol to improve security of SEAD. We also conduct some simulation experiments to evaluate the performance of our proposed protocol.

II. Problem Definition

The problem with many routing protocols for ad hoc networks is that those protocols are vulnerable to security attacks. The attacks can be classified as passive or active attacks. In a passive attack, a malicious node ignores operational requirements of the network. For example, an intermediate node along a route does not forward a packet, or hides routing information. Multiple routes and redundant messaging can alleviate passive attacks.

In an active attack, the malicious node introduces false information, e.g., a false distance vector, a false destination sequence, or a false route request. This confuses routing procedures and degrades network performance. With a false route, the malicious node can intercept and comprise packets.

Misdirecting is another active attack. Here, an intermediate node forwards packets along incorrect paths. This attack affects the source node by directing packets away from the intended destination node.

The AODV protocol uses destination sequence numbers to indicate how recently the routing information was generated. When multiple routes are available, the source node always selects a route associated with a largest destination sequence number.

A malicious node can fabricate a false large destination sequence number to attract traffic. Even worse, a deceived node can propagate, in good faith, a false route to other nodes to exacerbate the impact of the attack. In this case, the attacker can maliciously attract and discard data traffic.

A malicious node can also consume a large amount of the network bandwidth by broadcasting fictitious destination addresses to which no node can reply. This delays other traffic and can cause packets to be dropped, lowering overall network performance.

III. Related Work

There are known techniques for minimizing 'Byzantine' failures caused by nodes that through malice or malfunction exhibit arbitrary behavior such as corrupting, forging, and delaying routing messages. A routing protocol is said to be Byzantine robust when it delivers any packet from a source node to a destination as long as there is at least one valid route [3]. However, the complexity of that protocol makes it unsuitable for ad hoc networks.

Papadimitrators et al [4] described a secure routing protocol (SRP) that prevents impersonation and replay attacks for on-demand routing. The protocol disables route caching and provides end-to-end authentication with an HMAC primitive [5]. However, that protocol cannot prevent vicious request flooding because there is no mechanism for authenticating source and intermediate nodes.

Dahill et al[6] introduced another technique uses hop-by-hop authentication. Every node is required to sign and authenticate every message. That increases processing requirements and the size of messages.

Zapata [7] introduced another technique requires that each node has access to a certified public key of all network nodes to validate all routing packets. The originator of a message appends an RSA signature, and a last element of a hash chain, i.e., a result of n consecutive hash calculations on a random number[8, 9]. As the message traverses the network, intermediate nodes can validate cryptographically the signature and the hash value, generate a k^{th} element of the hash chain, with k being the number of traversed hops, and add the hash chain to the message [10].

However, public-key cryptography imposes a high processing overhead on the nodes and may be unrealistic for practical low-cost, ad hoc networks of low-complexity devices, such as sensors. Hash chaining requires that the nodes have synchronized clocks[11]. However, that technique can only discover attacks long after they happened.

Hauser et al[12] avoid that defect by using hash chains to reveal the status of specific links in a link-state algorithm. Their method also requires synchronization of the nodes.

Hu[13] introduced another technique called SEAD that uses a node-unique hash chain that is divided into segments. The segments are used to authenticate hop counts. However, DSDV distributes routing information only periodically.

In many applications, reactive or on demand routing protocols are preferred. With on demand routing, source nodes request routes only as needed. On demand routing protocols performs better with significantly lower overhead than periodic routing protocols in many situations [13]. The authentication mechanism of Ariadne[13] is based on TESLA[15]. They use only efficient symmetric-key cryptographic primitives. The main drawback of that approach is the requirement of clock synchronization, which is very hard for wireless ad hoc networks.

Most secure routing protocols are based on authentication in the route discovery process. Some techniques detect faulty links based on observation of misbehavior during packet forwarding.

Marti et al [16] described a protocol for detecting and avoiding routers that drop or modify packets in ad hoc networks running DSR protocol. They have trusted nodes monitoring neighboring nodes. That technique does not work well in multi-rate wireless networks because nodes might be able to intercept packets forwarded with different modulations schemes. In addition, that method is vulnerable to collusion and

misbehavior because there is no authentication.

Awerbuch et al[17] invention was based on adaptive probing techniques. However, malicious nodes can differentiate probing packets from normal data packets, and therefore, can selectively forward the probing packets to avoid detection.

Herzberg et al[18] described a combination of acknowledgements, timeouts and fault announcements, to detect packet forwarding faults. This proposal empirically described by Avramopoulos et al[19]. However, that protocol requires a separate authentication password for each of the intermediate router, thus adding more communication overhead when multi-hops are used.

A secure dynamic routing (SDR)[20] protocol is entirely on demand, and uses two primary mechanisms, route discovery and route maintenance. When a source node has a packet to send to a destination node but does not have a route to that destination node, the source node broadcasts a route request (RREQ) packet. The packet specifies the destination and a unique RREQ broadcast identifier. A receiving node attaches its own node address to a list in the RREQ and rebroadcast the RREQ. When the RREQ reaches the destination node, or any intermediate node that knows a route to the destination, that node sends a route reply (RREP) packet back to the source node, including an accumulated list of addresses from the source to the destination node. When the RREP reaches the source node, it stores the route in its route cache. Route maintenance is a mechanism for detecting changes in the topology of the network that can make a stored route invalid. This is done with a route error packet.

IV. SEAD-FHC

a) An algorithmic description of the SEAD-FHC

1. A method authenticates packets that are transmitted serially in a network.
2. A current password is selected for a current packet to be transmitted.
3. p_c Includes current data d_c.
4. A secure hash function $f_{(h)}$ is applied to the pw_c current password to form a current tag t_c.
5. A password pw_n is selected for a packet p_n that is in sequence and fallows p_c, which includes data d_n, and $f_{(h)}$ is applied to pw_n to form a tag t_n.
6. $f_{(h)}$ Is then applied to the d_n, t_n and pw_c to obtain a hashed value H_c.
7. p_c Is then transmitted that includes the H_c, d_c, t_c, password pw_p of packet p_p that sent before p_c in sequence to authenticate d_c.

b) Algorithm to authenticate sequence transmission of the packets

Countersign $cs_{(p_c)}$ will be selected for p_c that includes d_c to be transmitted.

$$t_c = f_{(h)}(cs_{(p_c)})$$

Countersign $cs_{(p_n)}$ will be selected for p_n with data d_n to be transmitted in sequence,

$$t_n = f_{(h)}(cs_{(p_n)})$$

Apply $f_{(h)}$ to the d_n, t_n and $cs_{(p_c)}$ that creates authentication tag for p_n referred as at $_{(p_n)}$

$$at_{(p_n)} = f_{(h)}(< d_n, t_n, cs_{(p_c)} >)$$

Transmit p_c from a source node n_s to a destination node n_d through hops in path selected through optimal route selection strategy.

The currently transmitting packet contains $at_{(p_n)}, d_c, t_c$ and a countersign $cs_{(p_p)}$ of packet p_p that transmitted before p_c to authenticate d_c.

In the interest of route maintenance, every hop in rout contains a cache that maintains hop list describing the route selected using an optimal route selection model. We apply $f_{(h)}$ on cache of each hop of the route to verify the integrity of the hop list cached.

c) Architecture of the proposed protocol

Proposed model provides an authentication protocol for a wireless ad hoc network where packets are transmitted serially. By serially, we mean a current packet p_c is immediately preceded by a previous packet p_p, and followed immediately by a next packet p_n.

More particularly, during a route discovery phase, we provide secure route selection, i.e., a shortest intact route, that is, a route without any faulty links. During route maintenance phase, while packets are forwarded, we also detect faulty links based on a time out condition. Receiving an acknowledgement control packet signals successful delivery of a packet.

For packet authentication, we use $f_{(h)}$ described by Benjamin Arazi et al [21]. The hash function encodes a countersign to form a tag.

By $f_{(h)}$ we mean that the countersign cannot be decoded from the tag and the countersign is used only once, because part of its value lies in its publication after its use. We have adapted that protocol for use in an ad hoc network where multiple packets need to be sent sequentially. Therefore, if a number of packets are sent sequentially, the countersign needs to be refreshed each time. Thus, a single authentication is associated with a stream of future packets that is significant difference between proposed and existing hash chain techniques. The existing models require stream of future events. In addition, the countersign is used to authenticate p_c but not for future packets.

As an advantage over prior art asymmetric digital signature or secret countersigns do not need to be known ahead of time or distributed among the nodes after the system becomes operational. It should also be noted, that each countersign is used only one time, because the countersign is published to perform the authentication.

The $f_{(h)}$ as implemented by the proposal is ideal for serially communicating packets along a route in an ad hoc network, without requiring the nodes to establish shared secret countersigns beforehand.

The protocol includes the following steps. Select a random countersign cs_r. Form a tag t_r, $t_r = f_{(h)}(cs_r)$, Construct a message mac_r Form a hash value $H_r = f_{(h)}(< mac_r, t_r, cs_r >)$, and make it public. Perform the act and reveal mac_r, t_r, cs_r to authenticate the act.

V. Simulation and Results Discussion

The experiments were conducted using NS 2. We build a simulation network with hops under mobility and count of 100 to 1400. The simulation parameters described in table 1. We assume that each node has a memory buffer large enough to ensure that normal packets are never dropped because of congestion. Authentication ensures that the buffer is properly allocated to valid packets. Buffers also protect against traditional DoS, in which malicious nodes flood the network with unauthenticated packets. Malicious nodes that send packets frequently could otherwise quickly consume all allocated buffer space.

We authenticate route request (RREQ) by $f_{(h)}$ at source node and broadcast identifier in the route discovery phase, and data control packets in the packet forwarding phase. Thus, we prevent malicious requests and replay attacks. We also use a per-hop hashing to verify that no intermediate hop is omitted in a node list describing a route. A route reply (RREP) is authenticated by a destination node and therefore, attackers cannot cheat other nodes by fabricating routing information.

Table1 : Simulation parameters that we considered for experiments

Number of nodes	100 to 1400
Maximum velocity	20 m/s
Dimensions of space	1500 X 300 m2
Nominal radio range	250 m
Source destination pairs	20
Source data rate (each)	4 packets/s
Application data payload size	512 bytes/packet
Total application data load	327 kbps
Raw physical link bandwidth	2 mbs
Periodic route update interval	15s
Periodic updates missed before link is declared broken	3
Maximum packets buffered per node per destination	5
Hash length	80 bits

Our authentication mechanism is different than existing secure routing protocols based on digital signature, because only efficient symmetric key cryptography is used. Our method is also better than existing hash chain based protocols, because a node stores only one countersign, while hash chain based protocols store multiple countersigns, which increases memory requirements.

To detect faulty links, we use acknowledgements, timeouts, and fault announcements; these can also be authenticated by our $f_{(h)}$. Therefore, we need only a single authentication tag for each data and control packet; thereby bandwidth and memory usage is low.

With faulty link detection, all passive and active attackers that fail to forward data packets and that maliciously misdirect data packets are recognized and avoided in subsequent routings.

a) Protocol Description

i. *Secure Route Discovery*

In on demand routing protocols, e.g., DSR, a source node initiates route discovery to find a route when the source node has a packet to send to a destination node, and the source node does not store a route to the destination node in its route cache. The source node does this by broadcasting a RREQ control packet to neighboring nodes. Neighboring nodes rebroadcast the request, until the request eventually finds its way to the destination node so that intermediate nodes on the route can be discovered. We authenticate the RREQ control packet with hash function $f_{(h)}$.

ii. *RREQ Authentication*

The routing path between source node n_s and destination node n_d contains $n_h, n_{h+1}..n_{h+z}$ as

intermediate hops, where 'z' is count of the intermediate hops.

The source node selects two random countersigns cs_r and $cs_{r'}$, and broadcasts a first RREQ:

$$
\begin{aligned}
n_{s(id)} &=< n_s(a_{id}), n_s(b_{id}) = 1 > \\
sig_{n_s} &= f_{(ds)}(n_s(id),\ f_{(h)}(cs_r)) \\
n_{s+1(id)} &=< n_{s+1}(a_{id}), n_{s+1}(b_{id}) = 2 > \\
RREQ_i &= \{n_{s(id)},\ f_{(h)}(cs_r), sig_{n_s}),\ f_{(h)}(n_{s+1(id)},\ f_{(h)}(cs_{r+1}), cs_r), n_d(a_{id}),\ f_{(h)}(n_s, n_d)\}
\end{aligned}
\tag{1}
$$

In Eq(1) $f_{(ds)}$ is optimal digital signature function, a_{id} is node address identity and b_{id} is broadcast id.

$f_{(ds)}(n_s(id),\ f_{(h)}(cs_r))$ is a digital signature to verify $(n_s(id),\ f_{(h)}(cs_r)$ by other nodes, so that every intermediate node and the destination can verify that the $(a_{id}, b_{id},\ f_{(h)}(cs_r))$ in the $RREQ_i$ packet is valid and indeed generated by the claimed n_s.

A hop node in the route path generates a route entry by storing the a_{id} of n_s, $b_{id}=1$, $hcs_r = f_{(h)}(cs_r)$, and $h_{e2} = f_{(h)}(n_{s+1},\ f_{(h)}(cs_{r'}), cs_r)$. These values can verify future route requests from the same source node. The component $< a_{id}, b_{id} >$ uniquely identifies $RREQ$.

The value b_{id} is incremented whenever the source node issues a new $RREQ$.

The secret key $k_{(n_s, n_d)}$ is shared between n_s, n_d. This needs only be used for the first packet.

Because of the broadcast nature of the $RREQ$ control packets, every node in the ad hoc network eventually receives the $RREQ_i$ after a time '$m\Delta$', where m is a diameter of the network, and Δ is a maximum delay at intermediate hop.

After a time interval '$m\Delta$', the n_s sends next route request $RREQ_{i+1}$. Therefore, the source node selects next random countersign cs_{r+2}, and broadcasts $RREQ_{i+1}$:

$$
\begin{aligned}
n_{s+1(id)} &=< n_{+1}(a\ ), n_{+1}(b\ ) = 2 > \\
cs_r\ &= f_{(ds)}(n_{s+1}(id), f_{(h)}(cs_{r+1})) \\
n_{s+2(id)} &=< n_{s+2}(a_{id}), n_{s+2}(b_{id}) = 3 > \\
RREQ_{i+1} &= \{n_{s+1(id)},\ f_{(h)}(cs_{r+1}), sig_{n_{s+1}}),\ f_{(h)}(n_{s+2(id)},\ f_{(h)}(cs_{r+2}), cs_{r+1}), n_d(a_{id}),\ f_{(h)}(n_s, n_d)\}
\end{aligned}
\tag{2}
$$

The intermediate node finds the route entry associated with the claimed source node, and performs $f_{(h)}$ on cs_r that received in $RREQ_{i+1}$ and checks the equality with hcs_r that received in $RREQ_i$, which stored in the route entry. If $f_{(h)}(cs_r)$ is equal to hcs_r then n_h applies $f_{(h)}$ on $(n_{s+1(id)},\ f_{(h)}(cs_{r+1}), cs_r)$ that received through $RREQ_{i+1}$ and checks if the result is the same as h_{e2} stored in the route entry, if valid, the authenticity of $(n_{s+1},\ f_{(h)}(cs_{r+1}))$ is verified. Thus, n_h is assured that $RREQ_{i+1}$ is from the claimed source node and the present b_{id} is valid. The n_h then updates its routing entry by recording b_{id} that received through $RREQ_{i+1}$, $hcs_r = f_{(h)}(cs_{r+1})$ and $h_{e2} = (n_{s+2},\ f_{(h)}(cs_{r+2}), cs_{r+1})$, which are used to authenticate $RREQ_{i+2}$.

In general, before sending a k^{th} route request $RREQ_k$, the source node waits a time interval $m\Delta$ after sending the previous request $RREQ_{k-1}$. Then, the source node selects a new random countersign cs_{k+1}, and broadcasts $RREQ_k$:

As a part of process at n_h, appends its own address to the intermediate node list in the $RREQ$, performs the per-hop hashing, which is achieved by calculating a new hash tag by hashing its own address concatenated with the old hash tag, and replacing the old hash tag, then rebroadcasts the RREQ. If any check fails, the RREQ is dropped.

Thus, with per-hop hashing, an attacker cannot delete an intermediate node from the node list, because the attacker does not have the secret countersign between the intermediate node and the destination node.

When the $RREQ$ reaches the' n_d', then n_d verifies it by checking if $k_{(n_h,n_d)}$ If the check succeeds, then the integrity of this $RREQ$ is verified, along with the authenticity of its origin and every intermediate node along the path from node n_s to node n_d.Then n_d sends a $RREP$ back to the source node, including an authenticated copy of the accumulated list of addresses from the $RREQ$ i.e., the packet data for the $RREQ$ control packet.

The $RREP$ control packet contains

$$n(lst)_h =< n_h, n_{h+1}, ..n_{h+z} > ...where\ 'z'\ represents number\ of\ \text{int}ermediate\ hops$$

$$< b_{id}, (n_s, n(lst)_h, n_d),\ f_{(h)}(n_d, n_{h+z}),\ f_{(h)}(n_d, n_{h+z-1}),\ f_{(h)}(n_d, n_{h+z-2}), ...,\ f_{(h)}(n_d, n_{h+1}),\ f_{(h)}(n_d, n_h),\ f_{(h)}(n_d, n_s) >$$

Where b_{id} is for the source n_s to verify the freshness of the reply. .As the $RREP$ packet passes through intermediate nodes back to the source node, each node checks the corresponding authentication tag, and stores the route information in its route cache. The source node then selects a shortest route to the destination node without previously detected faulty links.

iii. *Data transmission and malicious hop detection*

Here in this section we describe the procedure of authentication data packets forwarded from the source node to the destination node, along the selected route, while checking for faulty links. In DSR, the source route information is carried in each packet header.

To send a packet m_i that is a part of data to be sent to destination node n_d, the source node n_s picks two counter signs cs_r, cs_{r+1} and fixes the time limit to receive either one of packet delivery acknowledgement ack or a control packet mn_{ack} that acknowledges about malicious link in the route path. The source node sends message with the format

$$msg_i = \{m_i,\ f_{(h)}(cs_r),\ f_{(d\ )}(m_i,\ f_{(h)}(cs_r)),\ f_{(h)}(m_{i+1},\ f_{(h)}(cs_{r+1}), cs_r)\}$$

to the n_h along the route.

Here $f_{(ds)}(m_i,\ f_{(h)}(cs_r))$ is a digital signature to verify $(m_i,\ f_{(h)}(cs_r)$ by intermediate hops of the route selected, so that every 'n_h' and 'n_d' can verify that $(m_i,\ f_{(h)}(cs_r))$ is valid and indeed generated by the claimed n_s.

Then each hop updates route table entry for source node S by recording $f_{(h)}(cs_r)$ as $hcs_r(n_s)$, $f_{(h)}(m_{i+1},\ f_{(h)}(cs_{r+1}), cs_r)$ as $h_{e2}(n_s)$, which is used to authenticate an immediate fallowing message msg_{i+1} in sequence.

When sending the data packet m_{i+1}, the n_s selects another countersign cs_{r+2} and forwards the msg_{i+1} to the first hop of the selected path:

$$msg_{i+1} = \{m_{i+1},\ f_{(h)}(cs_{r+1}), cs_r,\ f_{(h)}(m_{i+2},\ f_{(h)}(cs_{r+2}), cs_{r+1})\}$$

Each node on the route calculates $f_{(h)}(cs_r)$ and compares with $hcs_r(n_s)$ that available in routing table, if results equal then cs_r will be authenticated as valid. The n_h then calculates $f_{(h)}(m_{i+1},\ f_{(h)}(cs_{r+1}), cs_r)$, and compares with $h_{e2}(s_n)$ result is equivalent then claims the validity of $(m_{i+1},\ f_{(h)}(cs_{r+1}))$. The node then updates its routing entry by recording $hrc_{r+1} = f_{(h)}(rc_{r+1})$ and $h_{(e2)}(n_s) = f_{(h)}(m_{(i+2)},\ f_{(h)}(cs_{r+2}), r_{r+1})$, and and forwards the data packet to the node along the route as specified in the header of the packet header.

During the packet sending process described earlier, if any of the checks fails, then the packet is dropped. If both checks succeed, then the node updates its routing entry associated with n_s. If the check at n_h, then either n_{h-1} or $f_{(h)}(m_{i+1},\ f_{(h)}(cs_{r+1}), cs_r)$ in msg_i has been modified, or node n_{h-1} modified $f_{(h)}(m_{i+1},\ f_{(h)}(cs_{r+1}), cs_r)$ in msg_{i+1}. In either case, the current hop node n_h drops the packet. Consequently, hop node n_{h-1} does not receive a valid ack after time out, and the node can report a malicious activity at (n_{h-1}, n_h) connection, or the hop node n_{h-2} reports about malicious activity between (n_{h-2}, n_{h-1}) to n_s. In either case, the fault link includes the malicious node n_{h-1}.

In our proposed model the authentication tag of each packet limited to two hashes and one countersign; while in the existing models required N authentication tags for a route with N hops. Therefore, our method has a lower communication and storage overhead.

The packet authentication process at n_d is identical to the authentication process at any intermediate hop n_h. If any of the checks fails, then the packet is dropped. If both checks succeed, the packet is delivered successfully, and schedules the 'ack' for transmission along the reverse of path of the route. The ack reflects the packet identification number i.

The destination node also appends an authentication tag to the ack message for the nodes on the reverse path. The authentication tag bears the same structure as the one generated by the source node. Specifically, when sending ack_i, for the packet 'm_i', the destination node randomly selects two countersigns cs_{re} and cs_{re+1}, and sends the following information:

$$ack_i, f_{(h)}(cs_{re}), f_{(ds)}(ack_i, f_{(h)}(ack_i)), f_{(h)}(ack_{i+1}, f_{(h)}(cs_{re+1}), cs_{re}).$$

Similarly, $f_{(ds)}(ack_i, f_{(h)}(cs_{re}))$ is used to verify $(ack_i, f_{(h)}(cs_{re}))$ by each node along the reverse path of the route. When sending the acknowledgement for packet 'm_i', the destination selects a new countersign cs_{re+1} and forwards:

$$(ack_{i+1}, f_{(h)}(cs_{re+1}), cs_{re}, f_{(h)}(ack_{i+2}\, f_{(h)}(cs_{re+2}), cs_{re+1})).$$

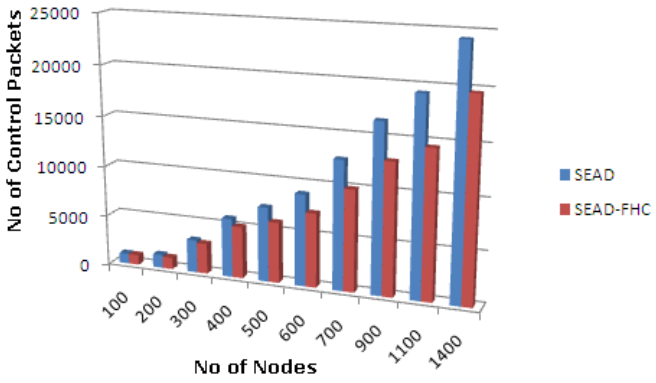
If the timeout at an intermediate node expires, then that node sends mn_{ack} with an identification number according to our hash function for authentication of the mn_{ack} by the upstream nodes. When a node receives the ack, the node verifies its authenticity and that a timeout is pending for the corresponding data packet. If the 'ack' is not authentic or a timeout is not pending, the node discards the ack. Otherwise; the node cancels the timeout and forwards the 'ack' to the next node.

When a node receives mn_{ack}, it verifies its authenticity, and that a timeout is pending for the corresponding data packet, and that the link reported in the mn_{ack} is the first downstream to the node that generated mn_{ack}. If the mn_{ack} is not authentic, or a timeout is not pending, or the link is not the downstream to the node reporting 'mn_{ack}', then the node drops mn_{ack}. Otherwise, the node cancels the timeout and further forwards the mn_{ack} control packet. Upon receiving 'mn_{ack}', the source node deletes the link that connecting n_h referred in mn_{ack} and finds a new route. In this proposed model, the packets are always received as in the order they sent. This is because all packets are forwarded along the same route in DSR. In the case of congestion and buffering, the messages are stored in a first-in-first-out buffer according to the order that they are received.

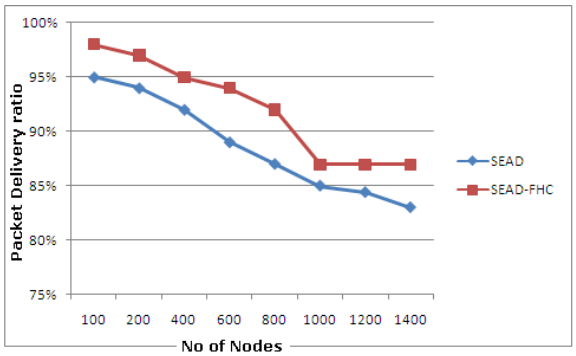
When the source node wants to use another path to the destination node, the source node selects a new countersign and authenticates the countersign with every node along the new route, and reinitiates the entire process, as described above.

b) Results Discussion

Here we describe the scalability of SEAD-FHC over SEAD in terms of control packet that costs resource utilization. We can observe that SEAD-FHC is almost similar to SEAD when node count is fewer. But we can observe that SEAD-FHC improving the minimization of the control packets when node count increased. It is obvious since the SEAD-FHC stabilizing the delay time even at maximum node count, which helps in minimizing packet drops due to delay and improves throughput. This results as fewer control packet utilization.



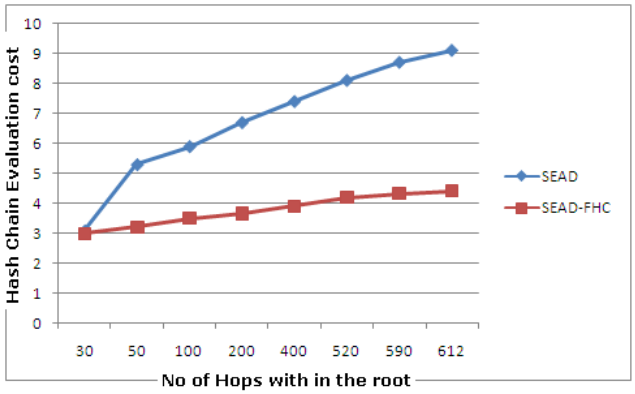
Here we describe the scalability of SEAD-FHC over SEAD in terms of packet delivery ratio. Since Hash chain computation cost is drastically minimized in SEAD-FHC, the delay time minimized and throughput increased.



Here we describe the performance of SEAD-FHC over SEAD in terms of Hash chain evaluation cost. Let λ be the cost threshold to evaluate each hash in hash chain. We measure the Hash chain evaluation cost as

$$\frac{\sum_{i=1}^{z}\sum_{j=1}^{n}\lambda}{z}$$

, here z is number of nodes and n is number of hashes, as of the chaining concept of SEAD z=n but in SEAD-FHC n always 2



VI. Conclusion

Here in this paper we proposed a secure efficient distance vector routing with fixed hash chain length in short we referred as SEAD-FHC. We argued that fixed hash chain limits the computation cost and resource utilization. We empirically demonstrated that SEAD-FHC is scalable and performs well over SEAD. In future experiments can target to extend this protocol to support path restoration mechanism. Here SEAD-FHC relies on new route detection upon link failure.

References Références Referencias

1. Perkins: "Ad hoc On-Demand Distance Vector Routing," Proceedings of the IEEE Workshop on Mobile Computing Systems and Applications, February 1999.
2. Wood: "Denial of Service in Sensor Networks," IEEE Computer Magazine, October 2002.
3. Perlman: "Network Layer Protocols with Byzantine Robustness," Ph.D. thesis, MIT LCS TR-429, October 1998.
4. Papadimitrators: "Secure Routing for Mobile Ad Hoc Networks," SCS Communication Networks and Distributed Systems Modeling and Simulation Conference, January 2002.
5. "The Keyed-Hash Message Authentication Code (HMAC)," No. FIPS 198, National Institute for Standards and Technology (NIST), 2002.
6. Dahill: "A Secure Routing Protocol for Ad Hoc Networks," Technical Report UM-CS-2001-037, University of Massachusetts, August, 2001.
7. Zapata: "Secure Ad hoc On-Demand Distance Vector Routing," ACM Mobile Computing and Communications Review (MC2R), July 2002.
8. Rivest: "A method for obtaining Digital Signatures and Public Key Cryptosystems," Comm. of ACM, February 1978,
9. Lamport: "Password Authentication with Insecure Communication," Comm. of ACM, November 1981.
10. Lamport: "Constructing Digital Signature Based on a Conventional Encryption Function", 1979.
11. Cheung: "An Efficient Message Authentication Scheme for Link State Routing", Computer Security Applications Conference, 1997.
12. Hauser: "Reducing the Cost of Security in Link State Routing," Symposium on Network and Distributed Systems Security, February 1997.
13. Hu: "Ariadne: A secure On-Demand Routing Protocol for Ad hoc Networks", MobiCom, September 2002.
14. Y. C. Hu, D. B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," Ad Hoc Networks Journal, 1, 2003, pp.175-192.
15. Perrig: "Efficient and Secure Source Authentication for Multicast," Network and Distributed System Security Symposium, February 2001.
16. Marti: "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," ACM International Conference on Mobile Computing and Networking, August 2000.
17. Awerbuch: "An On-Demand Secure Routing Protocol Resilient to Byzantine Failures," ACM Workshop on Wireless Security, September 2002.
18. Herzberg : "Early Detection of Message Forwarding Faults," SIAM J. Comput., Vol. 30, no. 4, pp. 1169-1196, 2000.
19. Avramopoulos: "A Routing Protocol with Byzantine Robustness," The 2003 IEEE Sarnoff Symposium, March 2003.
20. Johnson: "Dynamic Source Routing in Ad Hoc Wireless Networks," Mobile Computing, Kluwer Academic Publishers, 1996.
21. Benjamin Arazi: "Message Authentication in Computationally Constrained Environments", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 8, NO. 7, JULY 2009.
22. B. Bellur, R.G. Ogier, A reliable, efficient topology broadcast protocol for dynamic networks, in: Proceedings of the Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 99), March 1999, pp. 178–186.
23. R.V. Boppana, S. Konduru, An adaptive distance vector routing algorithm for mobile, ad hoc networks, in: Proceedings of the Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2001), 2001, pp. 1753–1762.
24. T. Clausen, P. Jacquet, A. Laouiti, P. Minet, P. Muhlethaler, A. Qayyum, L. Viennot, Optimized Link

State Routing Protocol, Internet-draft, draft-ietf-manet-olsr- 05.txt, October 2001, Work in Progress.
25. J.J. Garcia-Luna-Aceves, C.L. Fullmer, E. Madruga, D. Beyer, T. Frivold, Wireless Internet Gateways (WINGS), in: Proceedings of IEEE MILCOM 97, November 1997, pp. 1271–1276.
26. J. Jubin, J.D. Tornow, The DARPA Packet Radio network protocols, Proceedings of the IEEE 75 (1) (1987) 21–32.
27. S. Murthy, J.J. Garcia-Luna-Aceves, An efficient routing protocol for wireless networks, Mobile Networks and Applications 1 (2) (1996) 183–197.
28. C.E. Perkins, P. Bhagwat, Highly Dynamic Destination- Sequenced Distance-Vector routing (DSDV) for mobile computers, in: Proceedings of the SIGCOMM 94 Conference on Communications Architectures, Protocols and Applications, August 1994, pp. 234–244.
29. D.B. Johnson, D.A. Maltz, Dynamic source routing in ad hoc wireless networks, in: T. Imielinski, H. Korth (Eds.), Mobile Computing, Kluwer Academic Publishers, Dordrecht, 1996, pp. 153–181.
30. V.D. Park, M.S. Corson, A highly adaptive distributed routing algorithm for mobile wireless networks, in: Proceedings of INFOCOM 97, April 1997, pp. 1405–1413.
31. Z.J. Haas, A routing protocol for the reconfigurable wireless network, in: 1997 IEEE 6th International Conference on Universal Personal Communications Record: Bridging the Way to the 21st Century (ICUPC 97), vol. 2, October 1997, pp. 562–566.
32. C. Hedrick, Routing Information Protocol, RFC 1058, November 1988.
33. G.S. Malkin, RIP version 2 protocol applicability statement, RFC 1722, November 1994.
34. G.S. Malkin, RIP version 2, RFC 2453, November 1998.
35. N. Abramson, The ALOHA system—another alternative for computer communications, in: Proceedings of the Fall 1970 AFIPS Computer Conference, November 1970, pp. 281–285.
36. F. Baker, R. Atkinson, RIP-2 MD5 Authentication, RFC 2082, January 1997.
37. S. Basagni, K. Herrin, E. Rosti, D. Bruschi, Secure Pebblenets, in: ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc 2001), Long Beach, CA, October 2001, pp. 156–163.
38. J. Broch, D.A. Maltz, D.B. Johnson, Y.-C. Hu, J.G. Jetcheva, A performance comparison of multi-hop wireless ad hoc network routing protocols, in: Proceedings of the Fourth Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom98), October 1998, pp. 85–97.

This page is intentionally left blank

Global Journal of Computer Science and Technology
Volume 11 Issue 20 Version 1.0 December 2011
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Performance Evaluation of Wireless Sensor Network Routing Protocols for Real Time Application Support

By S.Koteswararao, M.Sailaja, T.Madhu
Department of Electronics and Communication Engineering

Abstract - This paper evaluates the performance of prominent on demand routing protocols, which are Ad Hoc On –Demand Distance vector Routing(AODV), Destination –Sequenced Distance Vector Routing(DSDV), Dynamic Source Routing(DSR)for wireless sensor networks Results obtained from simulations demonstrates that even though DSDV,AODV and DSR share a similar on demand behavior, the differences in protocol mechanics can lead to significant performance differentials. The performance differentials are analyzed using varying network load and network size using PHENOM ATTRIBUTES & NS-2.26 is used as a platform for simulating DSDV, AODV&DSR under various conditions.PHENOM routing protocol is designed especially for wireless sensor networks. Wireless Sensor Networks (WSNs) are characterized by multi-hop wireless connectivity, frequently changing network topology and need for efficient routing protocols.

Keywords : *DSDV,AODV, DSR, WirelessSensoretworks, PHENOM routing protocol,multi-hop wireless links,NS- 2.26*

GJCST Classification : *C.2.2*

Strictly as per the compliance and regulations of:

Performance Evaluation of Wireless Sensor Network Routing Protocols for Real Time Application Support

S.Koteswararao[α], M.Sailaja[Ω], T.Madhu[β]

Abstract - This paper evaluates the performance of prominent on demand routing protocols, which are Ad Hoc On –Demand Distance vector Routing(AODV), Destination –Sequenced Distance Vector Routing(DSDV), Dynamic Source Routing(DSR)for wireless sensor networks Results obtained from simulations demonstrates that even though DSDV,AODV and DSR share a similar on demand behavior, the differences in protocol mechanics can lead to significant performance differentials. The performance differentials are analyzed using varying network load and network size using PHENOM ATTRIBUTES & NS-2.26 is used as a platform for simulating DSDV, AODV&DSR under various conditions.PHENOM routing protocol is designed especially for wireless sensor networks. Wireless Sensor Networks (WSNs) are characterized by multi-hop wireless connectivity, frequently changing network topology and need for efficient routing protocols.

Keywords : DSDV,AODV, DSR, WirelessSensoretworks, PHENOM routing protocol,multi-hop wireless links,NS-2.26

I. Introduction

Wireless sensor networks are defined as an autonomous, adhocsystem consisting of a collection of networked sensor nodes designed to intercommunicate via wireless radio. Theses are of small with sensing, computations, and wireless networking capabilities, and as such these networks represent the convergence of important technologies. Sensor networks have enormous potential for both consumer and military applications. Military mission require sensor and other intelligence gathering mechanisms that can be placed close to their intended targets. the solutions to these constraints lies in large arrays of passive electromagnetic, optical, chemical, and biological sensors[2]. These can be used to identify and track targets, and they serve also as a first line of detection for various types of attacks. Such networks can also support the movement of unmanned robotic vehicles. The design considerations for some industrial applications are quite similar to those for military applications. Most sensors will be deployed with non-rechargeable batteries. The problem of battery life time in such sensors may be surrounded by using ultra small energy-harvesting radios. Research in this area promises radios smaller than one cubic centimeter, weighing less than 100grams, and with a power dissipation level below 100 microwatts [10]. Sensor networks are very different from conventional computer networks.First, because sensors have a limited supply of energy, energy-conserving forms of communication and computation are essential to wireless sensor networks.Second,since sensors have limited computer power, they may not be able to run sophisticated network protocols.Third,since the bandwidth of wireless link connecting Sensor nodes is often limited,inter-sensor communication is further constrained. The goal of this paper is to Carry out a systematic performance study of three dynamic routing protocols for WSN,the Dynamic Source Routing protocol(DSR)[5],the Ad-Hoc On-Demand instance Vector protocol(AODV)[6]&DSDV [1] for wireless sensor networks using NS2.

a) NetworkSimulator2

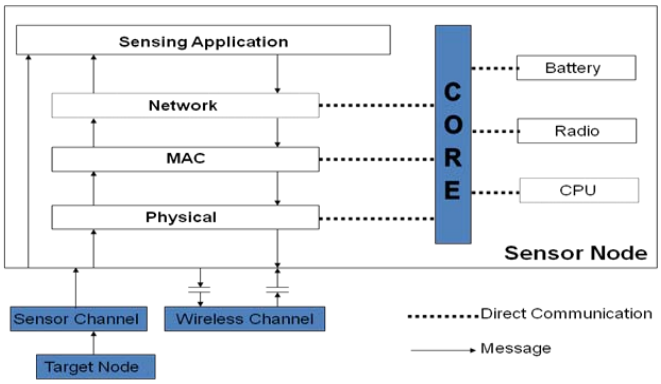
It is Discrete event simulator developed in C++.NS-2[14] is one of the most popular non-specific network simulators, and supports a wide range of protocols in all layers. It uses OTcl[Y]as configuration and script interface.NS-2 is the paradigm of reusability. It provides the most complete support of communication protocol models, among non-commercial packeges.several projects intend to provide WSN support to NS-2 such as Sensor-Sim[5] and NRL[14].Both are extensions of NS-2 to support WSN modeling.NS-2 can comfortably model wired&wireless network topologies up to 1,000 nodes or above with some optimizations. This experiments size can be kept for wireless using some optimizations [11] .A disadvantage of NS-2 is that it provides poor graphical support, via Nam.This application just reproduces a NS-2[12] trace The key motivation behind the design of on-demand protocols is the reduction of the routing load. High routing load usually has a significant performance impact in low bandwidth wireless links. Including this section, this paper has five sections, Section1shows about importance of wireless sensor network Section2 highlights sensor's simulation model.Section3 describes how protocols mechanisms are simulated and enlists simulation model parameters.Section4 discusses results

Author α : Department of Electronics and Communication Engineering, RIT, Yanam,U.T. E-mail : steevan2@gmail.com
Author Ω : Department of Electronics and Communication Engineering, JNTUK,Kakinada, A.P. E-mail : s.maruvada@gmail.com
Author β : Department of Electronics and Communication Engineering, SIET,Narsapur, A.P. E-mail : tennetimadhu@yahoo.com

which are obtained from various cases. Finally in section5 analysis on the basis of results is given.

II. Simulation Model

The goal of simulation is to simulate and closely model the sensor network scenario[14]. The broad outline of any sensor network can be represented by high-level representation as shown in Fig.1.The sensor model can be represented by the sensor node model and the power model.



Sensor node representations in a network

Fig1 : Sensor node representations in a networ

III. Performance Evolution

a) Performance Measures

Several simulations were run both with AODV,DSDV and DSR to compare performance metrics of both versions of the protocol.The performance metrics under considerations are:

- Mean end-to-end packet latency/delay: End-to-end packet latency is defind as the time elapsed from the moment a packet is generated by the data agent at the sending node,to the time the packet is received at the corresponding agent at the receiving node[8]
- Packet delivery ratio/Success rate ratio:

Packet delivery ratio is the ratio of total number of data packets that were deliverd successfully to intended destinations to the total number of data packets generated[10].packets may not be deliverd to the destination mainly because of one of the following reasons:packet collisions,routing loop and queue drop[15].

b) Simulation model

Simulation Area	500*500
Model	Energy
Ininatial energy	12.1J
Transmitting Power	0.660
Receiving Power	0.396
Transmission range	250m to 450m
No.of Mobile nodes	100

Table1 : Node configuration parameters

Radio Propagation model	Two Ray Ground Model
Antenna Model	Omni Antenna
Network Interface Type	Phy/Wireless Phy
MAC Type	802.11
Routing Type	AODV,DSDV,DSR
Interface Queue Type	Queue/DropTail/PriQueue
Buffer Size of IFq	6000

Table2 : energy model

c) Received Signal Power in free Space

The free space propagation model assumes the ideal propagation condition that is only one clear line of sight path between the transmitter and receiver[3]. H.T.Friis presented equational to calculate the received signal power in free space at distance from the transmitter

$$\Pr = (Pt * Gt * Gr * \lambda 2) / (4\pi) 2 * d 2 * L$$

Equation .1 : received signal power in free space

Pt is the transmitted signal power,Pr is the received signal power,Gt, Gr are the antenna gains of the transmitter and the receiver respectively and L is the system loss

d) Implemented Algorithm Explanation

This section explains how AODV[8] is simulated; DSR[9]&DSDV[1] algorithms are simulated in the manner except it has a slight difference in maintaining routing information.

In AODV, each node maintains two separate counters:

1. Sequence number, a monotonically increasing counter used to maintain freshness information about the reverse route to the source.
2. broadcast-ID, which is incremented whenever the source issues a new route request (RREQ) message.

Each node also maintains information about its reachable neighbors with bi-directional connectivity. Whenever a node (router) receives a request to send a message, it checks its routing table to see if a route exists. Each routing table entry consists of the following fields:

a) Destination address
b) next hop address
c) Destination sequence number
d) hop count

e) AODV route discovery algorithm

When a node needs to determine a route to a destination node, it floods the network with a route request (RREQ) message as shown in fig.2. if a route exists, the originating node sends data packet to destination[9]. Otherwise, it saves the messages in a message queue, and then it initiates a route request to

the destination (destination node) it replies with RREP (route reply) message, so that path can be determined/ established by source node and communication can take place.

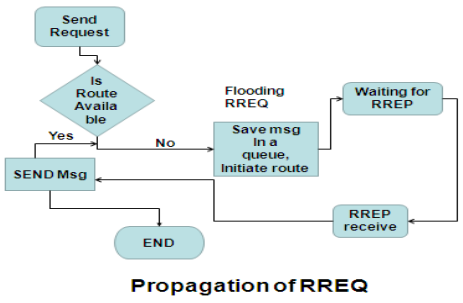


Fig2 : Propagation of RREQ

As these requests spread through the network, intermediate nodes store reverse routes back to the originating node[15]. Since an intermediate node could have many reverse routes, it always picks the route with the smallest hop. Count

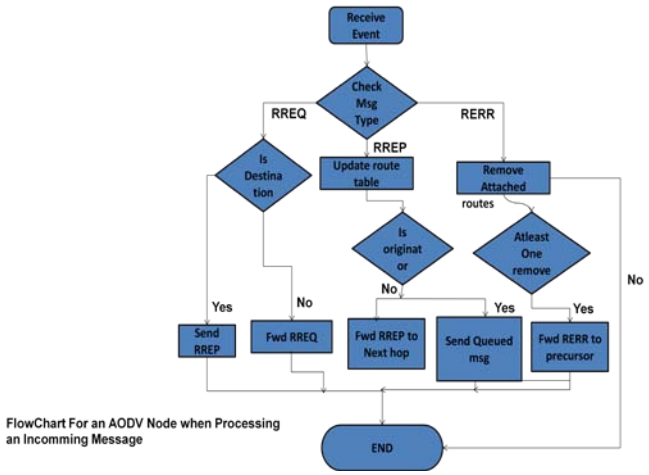


Fig3 : Flowchart for an AODV node when an incoming message

f) Packet Storage

The flow chart in fig.4 explains how packets are serviced inside a node, before node does anything it has to store a packet in a queue[15]. The nodes in simulation stores packets in FIFO manner.

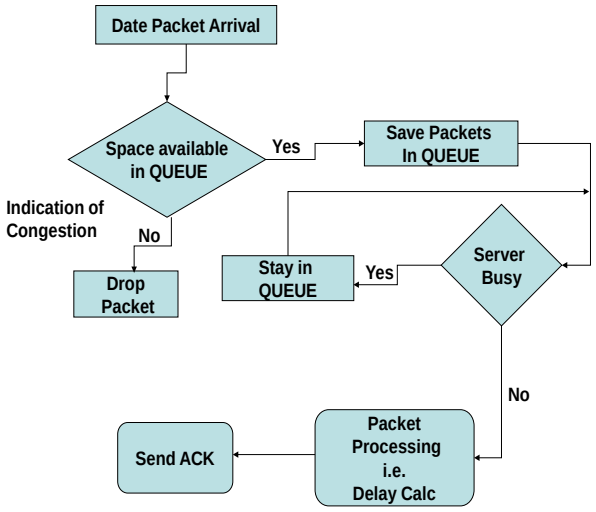


Fig4 : Flow chart of AODV node when storing Packet.

IV. Direct-Secquenced Distance Vector Routing(DSDV)

It is table driven routing protocol based on Bellman-Ford Routing Algorithm with certain improvements. Every mobile station maintains a routing table that lists all available destinations, the number of hops to reach the destination and the sequence number assigned by the destination node[1]. The sequence number is used to distinguish stale routes from new ones and thus avoid the formation of loops. The stations periodically transmit their routing tables to their immediate neighbors. A station also transmits its routing table if a significant change has occurred in its table from the last update sent.So,the update is both time-driven and event drive[10].

V. Dynamic Source Routing

The Dynamic source routing (DSR) is based on source routing, which means that the originator of nodes through which the packet must pass while travelling to the destination. The DSR protocol consists of two basic mechanisms: Route Discovery and Route Maintenance [5]

a) RouteDiscovery

Route discovery is used only when a source node attempts to send a packet to a destination node and does already know a route to it[10] To initiate the Route Discovery, the source node transmits a "Route Request "with a unique ID as a single local broad cast packet. when some intermediate node receives this Route Request, at first it determines whether it has seen the Route Request or not. If the node has already seen the Route Request earlier, it will discard the packet; otherwise it will check its Route Cache whether there is a route to the destination of the packet [5]. If it has the

route to target in its routing cache ,it returns a "Route Reply "to the initiator of the Route Discovery, giving a copy of the accumulated route record from the Route Request; otherwise it transmits the Route Request until the Route Request is received by the target[9]

b) Route Maintenance

DSR Protocol implements the route maintenance mechanism while communicating the packets from source node to destination node. In this scenario DSR protocols uses the route mechanism, to detect any other possible known route towards the destination to transmit data [8]. If the route maintenance fails to find an alternative known route to establish the communication then it will invoke the route discovery to find the new route to destination.

VI. Results & Conclusion

a) Comparison of Delay

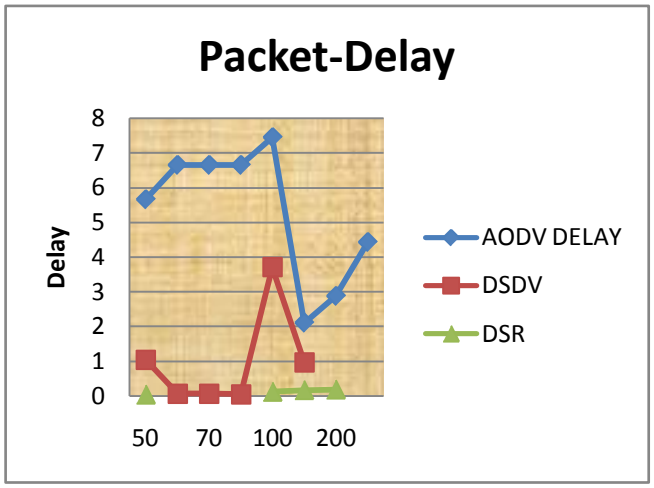


Fig 5 : Packet-Delay Comparisons

Simulations were run for varying number of packets with constant packet size and the result is plotted in fig.5. the result shows that the delay of DSR is slightly less than DSDV& AODV for increasing number of packets, the delay is more for DSDV at lower no. of packets According to above result, it can be said that AODV[outperforms DSR for more number of sources or for more network traffic and DSR performs better even though increasing more number of packets in terms of delay[3].

b) Packet Delivery Ratio (PDR) Comparison with varying no. of packets

The results plotted in fig6 is that delivery ratio is linearly increasing at lesser no. of packets ,PDR decreases at higher no. of packets in the case of DSDV.PDR is constant for all values in the case of AODV.PDR linearly varying at higher no. of loads in DSR[5].AODV outperforms than DSDV&DSR.

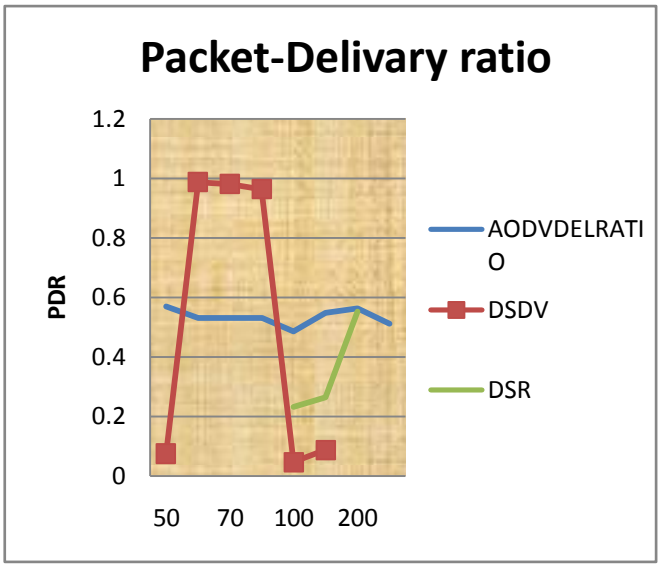


Fig 6 : Packet-Delivary Ratio Comparisons

c) Packet-Drop Comparison with varying no. of Packets

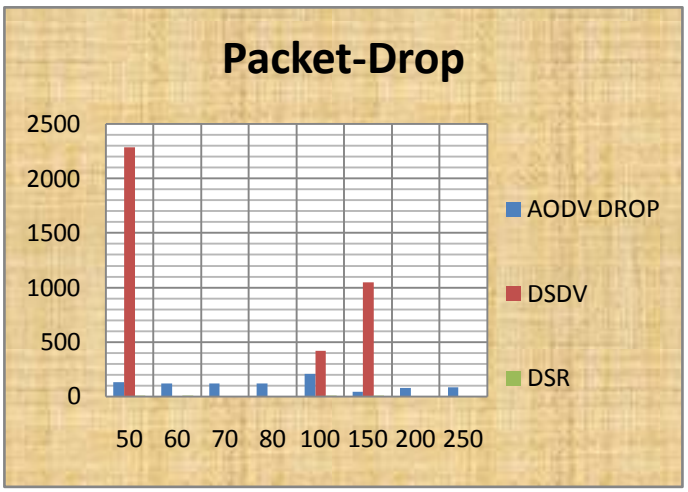


Fig7 : Packet Drop Comparison

DSR packet drop very low when compared to DSDV and AODV.Drop rate is more at less no. of sources in the case of DSDV.Drop rate is almost constant in AODV irrespective of varying load. Hence DSR outperforms DSDV&AODVhere as shown in Fig7.

VII. Analysis

a) Delay Performance

DSR exhibits slower delay than AODV&DSDV. However DSDV's delay performance worsens with large number of sources and gives about twice as much delay than AODV[15].

b) Overall Performance

On the whole shows better performance than DSDV in terms of packet delivery ratio &Drop except Delay performance. DSR, AODV&DSDV use on-demand route discovery, but with different routing

mechanics. In particular, DSR uses source routing and route caches, and does not depend on any periodic or timer-based activities. DSR exploits caching aggressively and maintains multiple routes per destination. AODV, on the other hand, uses routing tables, one route per destination, and destination sequence numbers, a mechanism to prevent loops and to determine freshness of routes.

VIII. Conclusion & Future Work

In this paper we simulated wireless sensor networks routing protocols for DSDV, AODV&DSR using PHENOM attributes and comparing the performance analysis of various parameters like Packet Delivery Ratio(PDR),Delay&Drop usingNS-2.26.

To enhance these protocols by adopting various routing techniques with the help of OTCL linkage with C++ in order to get Energy Efficient Model.

References References Referencias

1. Padmini Misra,*"Routing Protocols for Ad Hoc Mobile Wireless Networks*"[online] http://www.1.cse.wustl.edu/~jain/cis78899/adhoc_routing/index.html
2. I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cyirci. *"Wireless Sensor Networks: A survey".* Computer Networks, 38(4):393-422, 2002.
3. Praveen Namboori, Department of Computer Science, North Dakota State University, *" Energy Efficient Protocols and Schemes for Wireless SensorNetworks",* http://www.cs.ndsu.nodak.edu/~namboori/csci659 .doc
4. Ian F. Akyildiz, Xudong Wang, Weilin Wang *"Wireless mesh networks: a survey",* http://www.ece.gatech.edu/research/labs/bwn/mesh.pdf
5. J.Broch, D.Johnson, and D. Maltz, *"The Dynamic Source Protocol for Ad hoc Networks*", http://www.ietf.org/internetdrafts/draft-ieft-manet-dsr-03.txt, IETF draft, Oct.1999.
6. CHARLES E.PERKINS, ELIZABETH M.BELDING-ROYER AND IAN D.CHAKERES,*"Ad-hoc On-Demand Distance Vector(AODV)Routing*", Internet Request for Comment,RFC3561,July2003.
7. J.Hill, R.Szewczyk, A.Woo, S.Hollar, D.Culler, and K.Pister.*"System architecture directions for networked sensors*". In Proc.APSLOS-IX, Novber 2000.
8. Charles E. Perkins, Elizabeth M. Belding Royer, Samir R.Das, *AdHoc On-demand Distance Vector (AODV) Routing*, http://www.ietf.org/internet-drafts/draft-ietf-manet-aodv.txt, IETF Internet draft, July 2000.
9. Sangeetha Biswal,*"Study of DSR Routing Protocol in Mobile Adhoc Network",* International Conference on Information and Network Technology,IPCSITvol.4(2011).
10. Tarek- Master's Thesis. *Modeling and Simulation of a routing protocol for AD HOC networks combining queuing network analysis and ANT COLONY algorithm*. Http://miless.uniduisburg-essen.de/servlets/DerivatewServlet/Derivate-12937/Tarek-Thesis.pdf
11. V.Naoumoy, T.Gross,*"Simulation of Large Ad Hoc Network*s."In proc.ACM Modeling, Analysis and simulation of Wireless and Mobile Systems (MS WiM2003). San Diego, CA,pp.50-57,2003.
12. Jason Lester Hill, PhD *dissertation "System Architecture for Wireless Sensor Networks",* http://www.jlhlabs.com/jhill_cs/jhill_thesis.pdf
13. Charles E.Perkings, Elizabeth M.Royer and Samir R.Das, *Performance Comparison of Two On-Demand Routing protocols for Ad Hoc Networks, IEEEPersonal* ommunications, Feb2001.
14. K.Fall,and K.Varadhan.*"The network simulator ns-2: Documentation".* http:/www.isi.edu/nsnam/ns/ns~documentation.html.
15. RIZWAN AHMED KHAN,SHOB A KHAN *Performance Evaluation of AODV&DSR for Wireless Sensor Networks"*Preceedings of the 10th WSEAS International Conference on Communications, Vouliagment,Athens,Greece,July 10-12,2006(pp266-271).

This page is intentionally left blank

Global Journal of Computer Science and Technology
Volume 11 Issue 20 Version 1.0 December 2011
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Key Agreement & Authentication Protocol for IEEE 802.11

By A.K.M. Nazmus Sakib, Fauzia Yasmeen, Samiur Rahman, Md.Monjurul Islam , Prof. Dr. Md. Matiur Rahaman Mian, Md. Rashedur Rahman

University of Engineering and Technology

Abstract - WPA and WPA2 (Wi-Fi Protected Access) is a certification program developed by the Wi-Fi Alliance to indicate compliance with the security protocol created by the WiFi alliance to secure wireless networks. The alliance defined the protocol in response to several weaknesses researchers had found in the previous Wired Equivalent Privacy (WEP) system. Many sophisticated authentication and encryption techniques have been embedded into WPA but it is still facing a lot of challenging situations. In this paper we discuss the vulnerability & weakness of WPA. This paper also present solutions or suggestions which will improve Wi-Fi Protected Access (WPA) protocol. We provide a brief description of the different functional entities and we investigate several technical issues including infrastructure and aspects related to the AAA (Authentication, Authorization, and Accounting) procedures for users as well as the system security. Also we suggest different key agreement algorithm & encryption techniques.

Keywords : WiFi, Authentication, Key, Hash function, WPA 2, ECDH, RSA, DH.

GJCST Classification : D.4.6

Strictly as per the compliance and regulations of:

Key Agreement & Authentication Protocol for IEEE 802.11

A.K.M. Nazmus Sakib[α], Fauzia Yasmeen[Ω], Samiur Rahman[β], Md.Monjurul Islam[ψ], Prof. Dr. Md. Matiur Rahaman Mian[¥], Md. Rashedur Rahman[§]

Abstract - WPA and WPA2 (Wi-Fi Protected Access) is a certification program developed by the Wi-Fi Alliance to indicate compliance with the security protocol created by the WiFi alliance to secure wireless networks. The alliance defined the protocol in response to several weaknesses researchers had found in the previous Wired Equivalent Privacy (WEP) system. Many sophisticated authentication and encryption techniques have been embedded into WPA but it is still facing a lot of challenging situations. In this paper we discuss the vulnerability & weakness of WPA. This paper also present solutions or suggestions which will improve Wi-Fi Protected Access (WPA) protocol. We provide a brief description of the different functional entities and we investigate several technical issues including infrastructure and aspects related to the AAA (Authentication, Authorization, and Accounting) procedures for users as well as the system security. Also we suggest different key agreement algorithm & encryption techniques.

Keywords : WiFi, Authentication, Key, Hash function, WPA 2, ECDH, RSA, DH.

I. Introduction

WiFi (Wireless Fidelity) networks based on IEEE 802.11 standard [1] are being widely deployed in different environment due to standardization and ease to use as well as low cost. However, this deployment is limited to hotspots, homes, offices, public zone including airports, etc. due to the limited coverage of Wi-Fi propagation and high cost of installing and maintaining a wired network backhaul connection [17][18]. An extension of the IEEE 802.11 standard known as 802.11s to achieve mesh networking is under specification and not finalized yet represents the proposed architecture and the main functional entities [20]. In section III, we investigate the AAA and security issues and we describe the solution adopted in our architecture to achieve a secure service and protection against attacks. Finally, section IV concludes the paper.

II. User Authentication

User authentication can be based on a variety of authentication mechanisms such as Username/password, Universal SIM (USIM) and removable user identity Module (RUIM), etc. We will describe the authentication procedures for both user type A and user type B.

1. User Type A:

After completing the PMP Network Entry process & capabilities negotiation [6][20], user type A starts the authentication process, based on PKM-EAP recommendations as follows:

- In order to initiate the EAP conversation, a user type A may send PKMv2-EAP-start message (Figure 3).
- The MBS send an EAP-Identity request to the user. The EAP request may be encapsulated into a MAC management PDU (Packet data Unit) in the BS and may be transmitted in format of [PKM-Request (PKMv2-EAP-transfer)] [22]. User receives EAP-Request, forwards it to the local EAP method for processing, and transmits EAP-Response (PKM-Response/PKMv2 EAP-transfer) [20]. From now, the BSs (MBS and CBS) forward all users' messages to the AAA server.
- After one or more EAP-Request/Response exchanges, the AAA server connected remotely via Radius protocol, determines whether or not the authentication is successful [7]. The shared session keys are established at user type A and at the AAA server [22]. The AAA server then transfers the generated keys to the MBS. As specified in 802.16e [3][6], both user type A and MBS generate a PMK. Then, the AAA Server and user type A generate AK from shared session keys[22]. The key distribution entity in MBS delivers AK and its context to key receiver entity (in MBS) which is responsible of generating subsequent subordinate keys from AK and its context[7].
- To mutually prove possession of valid security association based on AK, the MBS sends the Security Association Traffic Encryption Key (SA-TEK) challenges message, the user type A

Author α : BSc in Computer Science & Engineering from Chittagong University of Engineering and Technology.
Telephone: +880-1730079790, E-mail : sakib425@yahoo.com
Author Ω : Lecturer of IBAIS University. Her research area is image processing & wireless network security. Telephone: 01912581501
Author β : BSc in Computer Science and Engineering from Chittagong University of Engineering and Technology.
Telephone: +880-1720085936, E-mail : sami_mania@ymail.com
Author ψ : BSc in Computer Science and Engineering from Chittagong University of Engineering and Technology. Telephone: 01719547887
Author ¥ : Dean, Faculty of Science & Engineering, IBAIS University. Telephone: 01912024740
Author § : Senior System Engineer,Grameen Phone. Complete B.Sc Engineering from Ahsanullah University of Science and Technology. Telephone: 01711504294), E-mail : rashedur@hotmail.com

responds by sending the SA-TEK request, and the MBS perform the procedure by sending the SA-TEK response. The SA-TEK proves liveliness of the security association in the user type A and its possession of the valid AK [22].

- For each SA, the user requests from BS two TEKs which are randomly created by the MBS and transferred to the user [20].
- Service flow Addition MAC management messages are used to create a new service flow [22].

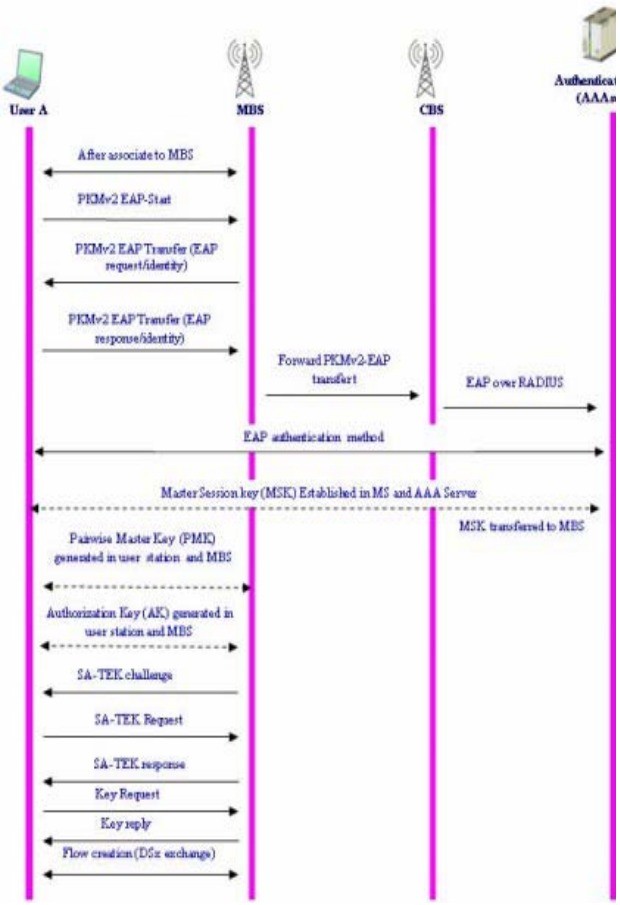


Fig3 : User type A Authentication procedure

2. User Type B:

To obtain Internet access, a user first completes the network discovery process & sends an associate request to an AP. After the reception of an associate response, user type B starts the authentication process, based on WPA2 recommendations, by sending user authentication information (ex: user name & password), in order to be allowed to use network resources. To get a better idea of how the authentication will operate, the interactions between elements are illustrated in the diagram of Figure 4:

- The user type B send an EAP-start message.
- The AP replies with an EAP-request identity message.
- The user type B sends an EAP-response packet containing the identity to be sent to the authentication server[22]. In a secure environment, the AP, MBS and CBS forward this information to the authentication server[20].

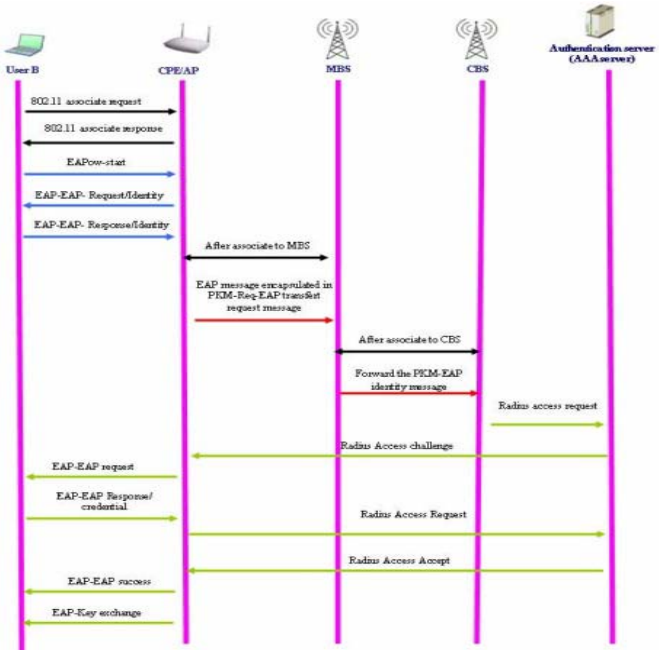


Fig4 : User type A Authentication procedure

- The authentication server using a specific authentication algorithm verifies the user's identity[7]. This could be through the use of digital certificates or other EAP authentication type[7].
- The authentication server will either send an acceptation (or reject) message to the AP. Then the AP sends an EAP-success packet (or fail) message to the user type B [7].
- If the authentication server accepts the user type B, the AP will transit the user type B's port to an authorized state & forward additional traffic. This is similar to the AP automatically opening the gate to let in only people belonging to the group cleared for entry. In this procedure for user type B, all BS's are merely a secure conduit for the AAA messages & does not play a significant role in the AAA process.

III. Secure Authentication Process by Using Hash Function

The security steps are as follows:

Step 1: Client request for communication & send out a string as a challenge to A.P.

Step 2: A.P also sends out a string as a challenge to the Client.

Step 3: Client & AP both calculate their corresponding string. and send the message digest value to the 2nd Hash function.

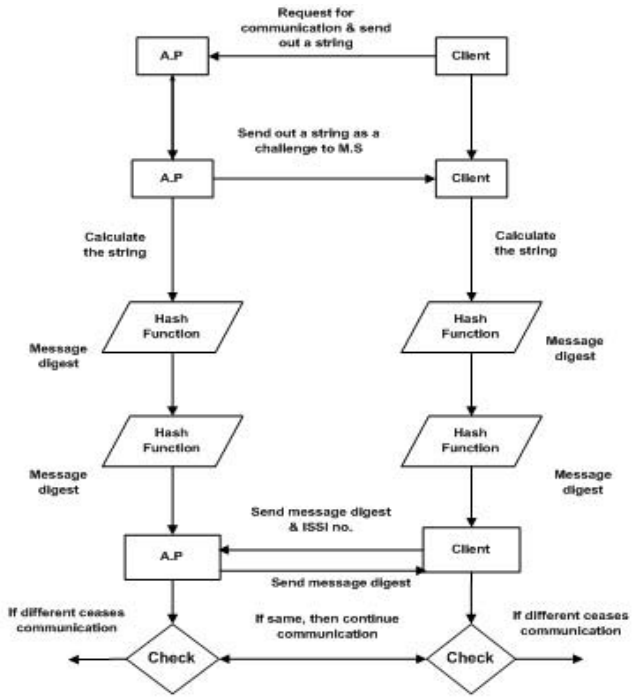


Fig5 : Authentication in secure way using Hash Function

Step 4: Both calculates the message digest for the corresponding string & send to each other. Only the legitimate A.P And Client knows the hash algorithm. But the evil M.S is not able to produce correct value for the given string.

Step 5: A.P & Client compare the corresponding message digest value. If it match then continue further communication. Otherwise, ceases the communication immediately (Fig 5).

IV. Secure Authentication Process by Using Math Function

The security steps are as follows:

Step 1: Client request for communication & send out a number as a challenge to A.P.
Step 2: A.P also sends out a number as a challenge to Client.
Step 3: Client calculates the value of the number by applying Math function And sends the challenging value and its ISSI number to A.P.

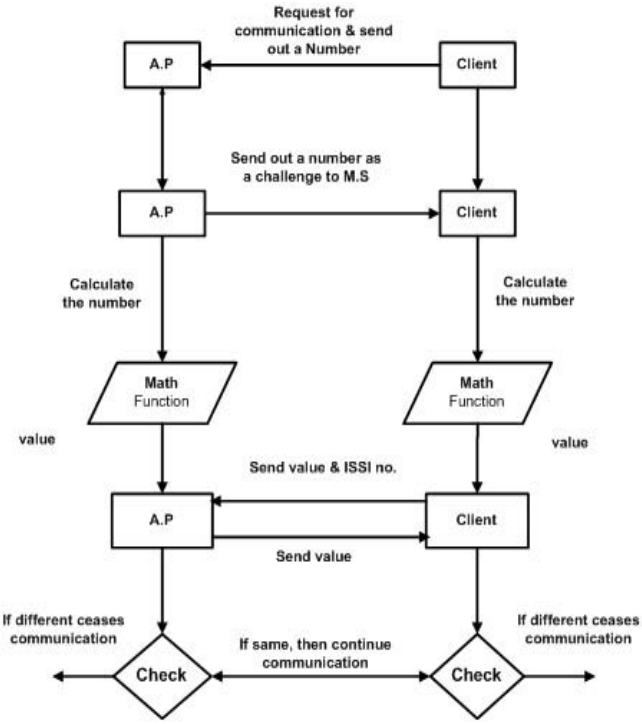


Fig6 : Authentication in secure way using Math Function

Step 4: A.P also calculates the value for the corresponding number & send to the Client. Only the legitimate A.P & Client knows the Math function. But the evil M.S is not able to produce correct value for the given number.

A.P & Client compare the corresponding value of the number. If it matches then continue further communication, Otherwise, ceases the communication immediately (Fig 6).

V. Function Library

Table 1 : Function Table

Polynomial Function	Log Function	Trigonometric Function	Exponential Function
$X^{12}+3X$	Log2X-33X	Cos5X/2	e^{5X+44}
$190X+1/X$	$2X^{11}+LogX$	Sin2X -21X	$e^{X}+e^{1/X}$
$X^{3}/5X$	$X^{3}/123Log2$	Tan33X- X^{2}	$e^{44X+177}$
$44/X^{12}$	Log4X-230	2SinX+33TanX	$1/e^{x}$
X^{2}-1X+55X	$3+LogX^{2}$	CotX –Sec2X	$e^{\sqrt{X}}$

VI. WPA2 Key Generation

Key generation is accomplished by means of two handshakes: a 4-Way Handshake for PTK (Pair wise Transient Key) & GTK (Group Transient Key) derivation & a Group Key Handshake or GTK renewal. The 4-Way

Handshake is accomplished by four EAPoL-Key messages between the client & the AP is initiated by the access point & performs the following tasks:

- Confirm the client's knowledge of the PMK. The PMK derivation, required to generate the PTK, is rely on the authentication method used. In WPA2 Personal mode, the PMK is derived from the authentication PSK & for WPA2 Enterprise mode the PMK is derived from the authentication MK [1] (key hierarchy in Fig. 7).
- Derive a fresh PTK, which is comprised of three types of keys: KCK (Key Confirmation Key – 128 bits) used to check the integrity of EAPoL-Key frames, Key Encryption Key (KEK – 128 bits) used to encrypt the GTK & the Temporal Keys (TK – 128 bits) used to secure data traffic[1][7].
- Install encryption & integrity keys.
- Encrypt transport of the GTK which is calculated by the AP from a random Group Master Key (GMK) [6].
- Confirm the cipher suite selection.

VII. Key Hierarchy

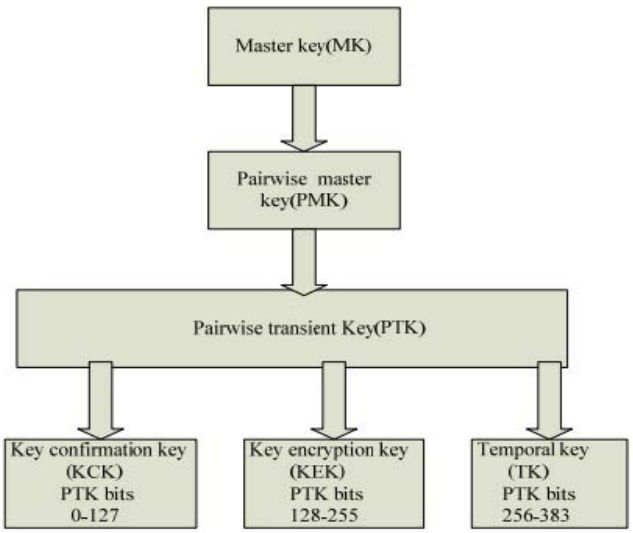


Fig7 : Pair wise key hierarchy

VIII. WPA2 Encryption and Decryption

The encryption process by using this symmetric key is described in the following flow chart (fig 8). Here for both encryption & decryption use two ways of permutation and performed Exclusive-OR operation with the symmetric key generated from previous process[22][6].

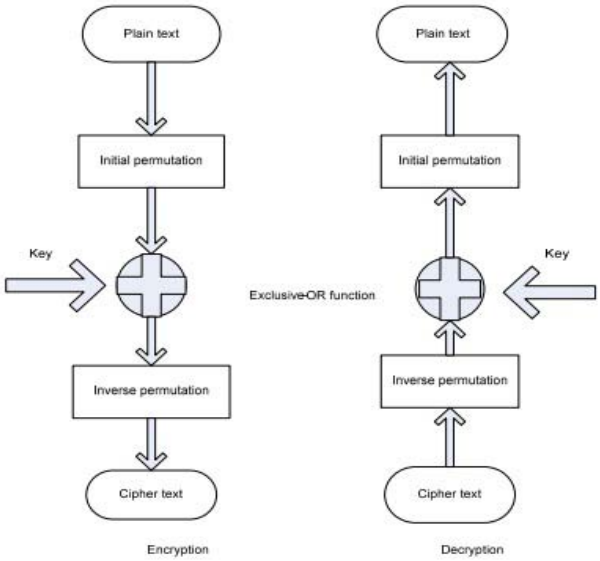


Fig8 : Encryption and Decryption Process

IX. Key Agreement Algorithm

To establishing shared secret between M.S & B.S, both must agrees on public constants p & g. where p is a prime number & g is the generator less than p [17].

Step 1: Let x and y be the private keys of M.S & B.S respectively. Private keys are random number, less than p.
Step 2: Let gx mod p and gy mod p be the public keys of devices M.S & B.S respectively
Step 3: M.S and B.S exchanged their public keys.
Step 4: The end M.S computes (gy mod p)x mod p, which is equal to gyx mod p.
Step 5: The end B.S computes (gx mod p) y mod p, which is equal to gxy mod p.
Step 6: Since, K = gyx mod p=gxy mod p, shared secret = K.

a) Mathematical Explanation- Dh

From the properties of modular arithmetic,

$$x \bmod n * y \bmod n \equiv x * y \ (\bmod n) .$$

We can write: $(x_1 \bmod n)*(x_2 \bmod n)*\ldots *(x_k \bmod n) \equiv x_1 * x_2 * \ldots * x_k \ (\bmod n)$,

if $x_i=x$, where $i = 1, 2, 3\ldots k$ $(x \bmod n)k \equiv x_k \bmod n$, $(gx \bmod p)y \bmod p = gxy \bmod p$ & $(gy \bmod p)x \bmod p = gyx \bmod p$, For all integers gxy=gyx, Therefore shared secret K=gxy mod p=gyx mod p [17]. Since, it is practically impossible to find the private key x or y from the public key [17] gx mod p or gy mod p, it is impossible to obtain the shared secret K for a attacker [17].

b) One-way function in DH

For M.S, Let x be the private key and a = gx mod p is the public key, Here, a = gx mod p is one-way function[17]. The public key a is obtained easily in the

forward operation, but finding _x' given a, g and p is the reverse operation & it will take exponentially longer time and is practically impossible. This is called discrete logarithm problem [17].

i. *ECDH – elliptic curve diffie-hellman*

ECDH: a variant of DH, is a key agreement algorithm. To generate a shared secret between M.S and B.S using ECDH [14] [17], both have to agree up on Elliptic Curve domain parameters. An overview of ECDH is given below.

c) Key Agreement Algorithm

Establishing a shared secret between M.S & B.S

Step 1: Let dX & dY be the private key of M.S & B.S respectively, Private keys are random number which is less than n, where n is a domain parameter.
Step 2: Let QX = dX*G & QY = dY*G be the public key of M.S & B.S respectively, G is a domain parameter
Step 3: M.S & B.S exchanged their public keys
Step 4: The end M.S computes K = (aK, bK) = dX*QY
Step 5: The end B.S computes L = (aL, bL) = dY*QX
Step 6: Since, K=L, shared secret is aK

d) Mathematical Explanation (ECDH)

To prove the agreed shared secret K & L at M.S & B.S

$$K = dX*QY = dX*(dY*G) = (dY*dX)*G = dY*(dX*G) = dY*QX = L,$$

Hence, K = L, therefore aK = aL Since it is practically not possible to find the private key dX or dY from the public key QX or QY, it is impossible to obtain the shared secret for a third party [17] [16].

ii. *RSA*

It is a public key algorithm, which is used for Encryption, Signature and Key Agreement. It (RSA) typically uses keys of size 1024 to 2048 [17]. The RSA standard is specified as RFC 3447, RSA cryptography Specifications Version 2.1 [17]. Overviews of RSA algorithms are given below.

e) Parameter generation

Step 1: Consider two prime numbers a & b.
Step 2: Find n=a*b, Where n is the modulus which is made public. The length of n is considered as the RSA key length [17].
Step 3: Choose a random number _e' as a public key in the range 0<e<(a-1)(b-1) such that gcd(e,(a-1)(b-1))=1 [17]
Step 4: Find private key d such that ed ≡ 1(mod (a-1)(b-1)) [17].

iii. *Encryption*

Consider, B.S needs to send a message to M.S securely.

Step 5: Let e be M.S's public key, Since e is public, B.S has access to e.
Step 6: To encrypt the message M, represent the message as an integer in the range 0<M<n [17].
Step 7: Cipher text C = Me mod n, where n is the modulus [17].

iv. *Decryption*

Step 8: Let C be the cipher text received from B.S.
Step 9: Calculate Message M = Cd mod n, where d is M.S's private key & n is the modulus.

f) Key Agreement (RSA)

Public key cryptography involves mathematical operation on large numbers and these algorithms are considerably slow compared to the symmetric key algorithm [17]. They are too slow that it is unable to encrypt large amount of data. Public key encryption algorithm such as RSA can be used to encrypt small data such as keys which used in private key algorithm [17]. RSA is thus used as key agreement algorithm.

g) Key agreement algorithm

Establishing shared secret between B.S and M.S

Step 10: Generate a random number, key to B.S.
Step 11: Encrypt by RSA encryption algorithm using M.S's public key & pass the cipher text to M.S [17].
Step 12: M.S decrypt the cipher text using M.S's private key to obtain the key[17].

h) One-Way function in RSA

Consider key generation equation Step 4, ed≡1 (mod(a-1)(b-1)) & n=a*b ,Where e is the public key d is the private key. a & b are kept private but n is made public. Since e is public, anybody who has access to a & b could easily generate the private key d using the above equation in Step 4. The security of RSA depends on the difficulty to factorize n to obtain the prime numbers a & b [17]. n is easily obtained by multiplying a & b but the reverse operation of factorizing n to obtain prime numbers a & b is practically impossible if a & b are large numbers. This encryption will be symmetric key encryption process & and it is suggested to use 'Vernam Cipher'encryption process rather than DES or AES to encrypt initial management communication[17]. Where key will be used as a random number for encryption .Because of the use of symmetric key encryption as well as Vernam Cipher which required only to performed bitwise Exclusive-OR operation, it will not introduce any traffic overhead in the network [17]. Encryption process is described in figure.

X. Conclusion

In this paper, an overview of security scheme in WiFi is presented. Attacks on authentication can be described as the ways by which a network can be intruded & the privacy of the users is compromised; if the user authorization & authentication stage is compromised. Therefore, the ways to breach the authentication frameworks are termed as attacks on privacy & key management protocols. But the hash based & function based authentication protocol will protect this type of interception. We also proposed

secure symmetric key agreement algorithm for secure key generation. This will prevent a key misuse & save band width in the multicast and broadcast services.

References References Referencias

1. "Benefits and Vulnerabilities of Wi-Fi Protected Access 2 (WPA2)", Paul Arana, INFS 612 – Fall 2006.
2. "IEEE 802.11i." Wikipedia, The Free Encyclopedia. 11 Nov 2006, 10:22 UTC. Wikimedia Foundation, Inc. Nov. 25 2006.
3. "Wi-Fi Protected Access 2 Data Encryption and Integrity." Microsoft TechNet. The Cable Guy. July 29 2005.
4. "Understanding the updated WPA and WPA2 standards".ZDNet Blogs. Posted by George Ou. June 2 2005.
5. "Deploying Wi-Fi Protected Access (WPAtm) and WPA2tm in the Enterprise." Wi-Fi Alliance, Feb. 27 2005.
6. Lehembre, Guillaume. "Wi-Fi security –WEP, WPA and WPA2". Article published in number 1/2006 (14) of hakin9, Jan.2006.
7. Ou, George. "Wireless LAN security guide"Revision 2.0 Jan 3 2005.
8. Bulk Frank. "Learn the basics of WPA2 Wi-Fi security". Network Computing Jan. 27 2006.
9. "Extensible Authentication Protocol." Wikipedia, Free Encyclopedia. Nov. 26 2006, 15:39 UTC. Wikimedia Foundation, Inc. Nov27 2006.
10. Gupta Ashok and Buthmann, Theresa. "The Bell Labs Security Framework: Making the case for End-to-End Wi-Fi Security". LucentTechnologies Sep. 11 2006.
11. Epstein Joe. "802.11w fills wireless security holes". Network World Apr 3, 2006.
12. Wright Joshua. "How 802.11w will improve wireless security". Network World May 29, 2006.
13. Wright Joshua. "802.11w security won't block DoS attacks". Tech World Jun 14, 2006.
14. Sood Kapil and Eszenyi Mathew. "Secure Management of IEEE 802.11 Wireless LANs". Intel Software Network.
15. Strand Lars. "802.1X Port-Based Authentication HowTo". The Linux Documentation Project Oct 18, 2004.
16. Bellardo John and Savage Stefan. "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions" USENIX 2003 Nov 7, 2003.
17. "IEEE 802.16e Security Vulnerability: Analysis & Solution",A.K.M. Nazmus Sakib, Dr. Muhammad Ibrahim Khan, Mir Md. Saki Kowsar, GJCST, October 2010, Volume 10, Issue 13, Version 1 A.K.M. Nazmus Sakib et al. / International Journal of Engineering Science and Technology (IJEST).
18. "Security Enhancement & Solution for Authentication Frame work in IEEE 802.16"- A.K.M. NAZMUS SAKIB[1], Academic & Industrial Colleboration Centre [International Journal of Computer Science & Information Technology] Vol2, No 6, 2010.
19. "Security Improvement of IEEE 802.11i (Wi-Fi Protected Access 2)"- A.K.M. NAZMUS SAKIB[1], Fariha Tasmin Jaigirdar, Muntasim Munim, Armin Akter, International Journal of Engineering Science & Technology.
20. "Secure Key Exchange & Authentication Protocol For Multicast & Broad cast Service in IEEE 802.16e"- A.K.M. NAZMUS SAKIB[1], Mir Md Saki Kawsor, AP Journal Special Issue.
21. "Security Improvement of Multi & Broadcast services in IEEE 802.16e by removing Forward Secrecy"- A.K.M. NAZMUS SAKIB[1] , Global Journal of Computer Science & Technology, Volume 11 Issue 16 Version 1.0 August/September 2011.
22. "Secure Authentication & Key Exchange Technique for IEEE 802.16e by using Cryptographic Properties", A.K.M. Nazmus Sakib[1], Vol 1 Issue 3, 2011.

Global Journal of Computer Science and Technology
Volume 11 Issue 20 Version 1.0 December 2011
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Concept Set Modeling Approach to Conceptualise Multilingual Digital Linguistic Database

By Ahmad Hweishel AL-Farjat, Ibrahim Mahmoud Ibrahim Alturani, Marwan Hweishel Al-Farajat, Tareq Ahmad Ali Alzayyat

AlBalqa Applied University, Jordan, Aqaba

Abstract - In this paper, we report the work on developing a multilingual digital linguistic database that aims to provide overall information a linguistic item carries in a language, and its cross-linguistic morphemic equivalent in other languages. It is conceptualised as a model of human knowledge of a language, and its description and architecture is an effort towards modeling such linguistic knowledge. From computational and programming aspects it throws an enormous challenge as it has many-to-many relations across languages, scripts, orthography, fields and entries. To accomplish such linkages among languages and between different types and kinds of information related to the linguistic item, an idea of a 'Concept Set Model' is discussed.

Keywords : *Language, Database, Electronic.*

GJCST Classification : *H.2.1*

Strictly as per the compliance and regulations of:

Concept Set Modeling Approach to Conceptualise Multilingual Digital Linguistic Database

Ahmad Hweishel AL-Farjat[α], Ibrahim Mahmoud Ibrahim Alturani[Ω], Marwan Hweishel Al-Farajat[β], Tareq Ahmad Ali Alzayyat[ψ]

Abstract - In this paper, we report the work on developing a multilingual digital linguistic database that aims to provide overall information a linguistic item carries in a language, and its cross-linguistic morphemic equivalent in other languages. It is conceptualised as a model of human knowledge of a language, and its description and architecture is an effort towards modeling such linguistic knowledge. From computational and programming aspects it throws an enormous challenge as it has many-to-many relations across languages, scripts, orthography, fields and entries. To accomplish such linkages among languages and between different types and kinds of information related to the linguistic item, an idea of a 'Concept Set Model' is discussed.

Keywords : *Language, Database, Electronic.*

I. Introduction

For more than 2000 years, paper dictionaries are compiled with a view to provide specific information that it aims to provide. Hence, there are several types of dictionaries providing specific information depending upon the type of dictionary. Similarly, an electronic dictionary, though primarily designed to provide basic information such as grammatical category, meaning, usage, frequency, etc., has also got its usage in various other ancillary tasks in the newer domains of language use. Such electronic dictionary, however, has a major shortcoming as it provides specific information considering the scope, usage, and storage for which it is developed [1].

With the gaining in weight of regional and foreign languages in India from the 11th century onwards, a novel type of lexicon came into being: bilingual and multilingual dictionaries. Amara simhāna Amarakośa emba Nāmalingānuśāsana (ಅಮರ ಸಿಂಹನ ಅಮರಕೊಶಎಂಬ ನಾಮಲಿಂಗಾನು ಶಾಸನ) published in 1970, By Prasaranga of University of Mysore, is an example of multilingual thesaurus having Sanskrit as source and English and Kannada as target languages. Thus, even in multilingual dictionaries the correspondence between the working languages is mostly established through an intermediate language – an interlingua – very much in the same way as it is done when connecting two languages by means of a couple of bilingual dictionaries.

Electronic Dictionaries: The expression Electronic dictionary started life in the last quarter of the 20th century as a term for specialised device - a handheld computer dedicated to storing a lexical database and performing lookup in it. As classical lexicography is in a complex relationship with linguistic theory, so is electronic lexicography with computational linguistics, of which electronic dictionaries are a product whilst also serving as tools and feedstock for creating other products.

An electronic bilingual or multilingual dictionary may be a digitaised edition of a conventional reference work, perhaps augmented by types of information specific of this medium (recorded pronunciations, hyperlinks, full text search, etc). Alternatively, it may be a system of monolingual dictionaries of different languages interlinked at the level of entries. [2]

Multilingual Lexical database is a great help if one often needs to translate similar documents into different languages (a reasonably common situation and bound to become more and more frequent in this age of global communication, especially in massively multilingual societies such as India, European Union). Also adding one more language to a multilingual dictionary tends to be less labour-intensive than creating a new bilingual dictionary thus economically more viable for languages with relatively few speakers and learners.

Some of the Advantages of Electronic Lexical Database is enlisted below;

1. Flexibility in Growth: Potential for Infinite growth in Lexical Entries and can be integrated with voluminous corpus.
2. Multi Purpose: Serve as explanatory dictionary, grammatical dictionary, Dictionary of Synonyms, Antonyms, phraseology, etymology, pictorial including Embedded Audio-Video which is not possible in printed dictionary.

Author α : Applied Science Department, AlBalqa Applied University, Jordan, Aqaba. E-mail : Ahmed_alfarajat@hotmail.com
Author Ω : Applied Science Department AlBalqa Applied University, Jordan, Aqaba. E-mail : Traini110@yahoo.com
Author β : Asycuda Technical Consultant, United Nation Conference on Trade and Development (UNCTAD) DTL - Asycuda Programme. E-mail : Marwan_alfa@hotmail.com
Author ψ : Department Of Management Information System, University Of Petra, Jordan, Amman. E-mail : tareq_alzayyat@hotmail.com

3. User Friendly: Easy look up is possible, since easy to use GUI is provided by which the word to be looked up can be typed directly or by just selecting the word in the text by invoking dictionary by keyboard or mouse events (as in WordWeb) from any word editors.
4. Digital grammatical dictionaries can also extract inflections at least partly and work as morphological analysers and generators upon demand.
5. Easy update facility can be provided under the guidance of a moderator

The major issue which comes into picture at the time of developing a multilingual digital Linguistic database is, interlinking the Lexical entries of different languages in database.

The major issue in Linking Lexical entries across language is the complexity of many-to-many relationship of words. One word of a language may have more than one meaning, but the word corresponding to the same word in a different language may not represent all the meanings of a source language term. At the same time Target word may be representing some more meanings other than the source language term. In multilingual scenario, those other meanings may get linked with a lexical item of some other third language of which there may not be any corresponding term available in first language.

To cite an example, a linguistic item in Kannada 'ke-sa-ri' (ಕೇಸರಿ) represents three concepts.

A shade of yellow tinged with orange- saffron.

A flavouring agent - saffron.

A large tawny flesh-eating wild cat of Africa and South Asia- lion.

When the Kannada word 'ke-sa-ri' maps with its Arabic counter part 'za'farān' (زعفران), which provides the first two sense but the third sense 'lion' is not provided by Arabic 'za'farān', instead Arabic word 'al'asad' (الأسد) is used.

There are situations when a term used in one meaning in a language may exist in the second language but with a different meaning. Thus, linking them is not possible.

e.g.: The Linguistic item 'u-pa-nya-sa' (ಉಪನ್ಯಾಸ) in Kannada means 'A speech that is open to the public - Lecture' in Hindi same 'u-pa-nya-sa' (उपन्यास) means, 'An extended fictional work in prose; usually in the form of a story - Novel'. 'Novel' in Kannada means 'Ka-dam-ba-ri' (ಕಾದಂಬರಿ), but same 'Ka-dam-ba-ri' (कादंबरि) means 'Cluster-of-Clouds' in Hindi.

A Language might have borrowed a word with a meaning or a few meanings from some Classical Language instead of borrowing all the meanings, and may have a word homographic in its own language with different meaning or lexical category

For e.g. Linguistic item 'hari' (ಹರಿ) in Kannada which was borrowed from Sanskrit as noun means 'The sustainer; a Hindu divinity worshipped as the preserver of worlds - Lord Vishnu', but in Sanskrit it is used in 36 senses including 'Lord Vishnu', few of them are given below.

'The destroyer; one of the three major divinities in the later Hindu pantheon -Shiva' (noun)

'Solid-hoofed herbivorous quadruped domesticated since prehistoric times - Horse', (noun)

'Any of various long-tailed primates (excluding the prosimians) - Monkey', (noun)

'Limbless scaly elongate reptile; some are venomous - Snake' (noun)

'The process of combustion of inflammable materials producing heat and light and (often) smoke - Fire' (noun)

Kannada borrowed only the meaning of 'Lord Vishnu' so in developing multilingual dictionary it cannot be linked with all the concepts of Sanskrit. More over in Kannada the same lexical item 'hari' is homograph representing different meanings as follows.

'The motion characteristic of fluids – flowing' (verb)

'Move smoothly and sinuously, like a snake – snake' (verb)

'To separate or be separated by force – tear' (verb)

The above meaning of the Kannada lexical entry 'hari' is not shared by the 'hari' of Sanskrit. So these meanings also cannot be linked in database.

By the above given examples it's clear that Word-to-Word mapping is impossible. Multilingual dictionaries usually select one language as the leading one (or vedette). Data in all other working languages are translated into this one and in this way are connected to each other [3]. If exact word is not available in the target language the user should at least get the descriptive meaning of Source Language word.

As it is evident that word to word mapping is not possible, and in multilingual scenario no language can be set as Interlingua. There is no natural language exists which can provide all the corresponding words for all the languages used in a multilingual dictionary. But there is no better choice than having an Interlingua for linking multiple languages lexicon entries.

In this approach rather than following the equivalent items across languages, the descriptive meaning of the item in question is followed. In other words, based on equivalent meaning, items are interrelated, and iterated over different languages. Under such approach, however, it is a known fact that lexical underspecification across languages are encountered. To account this issue, an Interlingua language is taken. Even though it may not have corresponding lexical item for a source word, its descriptive meaning will enable the language lexicographer of a different language to give suitable lexical item in one's language.

The Proposed 'concept set model' i.e. a Lexical Item is entered along with its Semantic Meaning and synonyms and spelling variants linked with 'descriptive meaning in Interlingua' to database. Other lexical semantic relations are entered manually. Based on the 'descriptive meaning', the process is iterated in other languages. In other words, we are following indexation of 'descriptive meaning'.

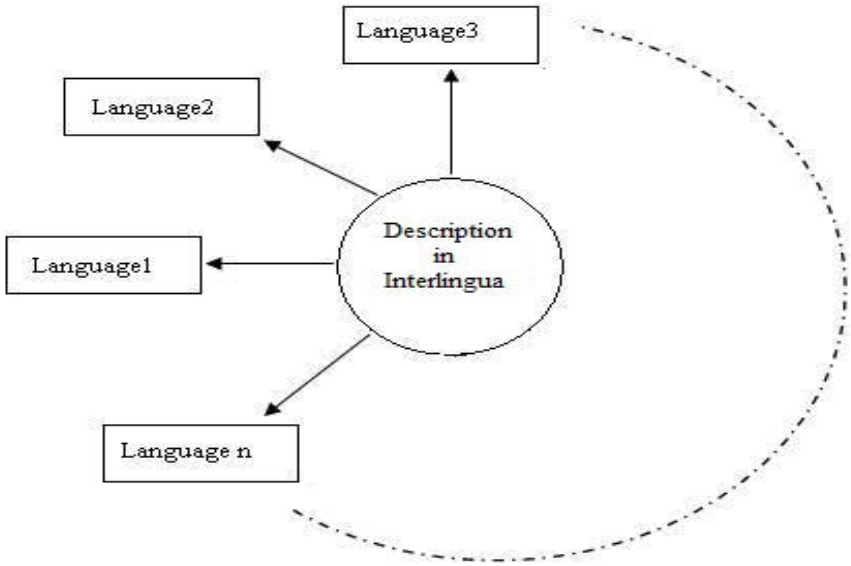
Concept Set can be represented as follows.

{

(Description in Interlingua + Lexical Item in Interlingua + Grammatical Category),
(Semantic Meaning + Words along with their Spelling Variations sharing Semantic Meaning) in Language-1,
(Semantic Meaning + Words along with their Spelling Variations sharing Semantic Meaning) in Language-2,
---

(Semantic Meaning + Words along with their Spelling Variations sharing Semantic Meaning) in Language-n

}



Conceptual Representation of Linking Languages

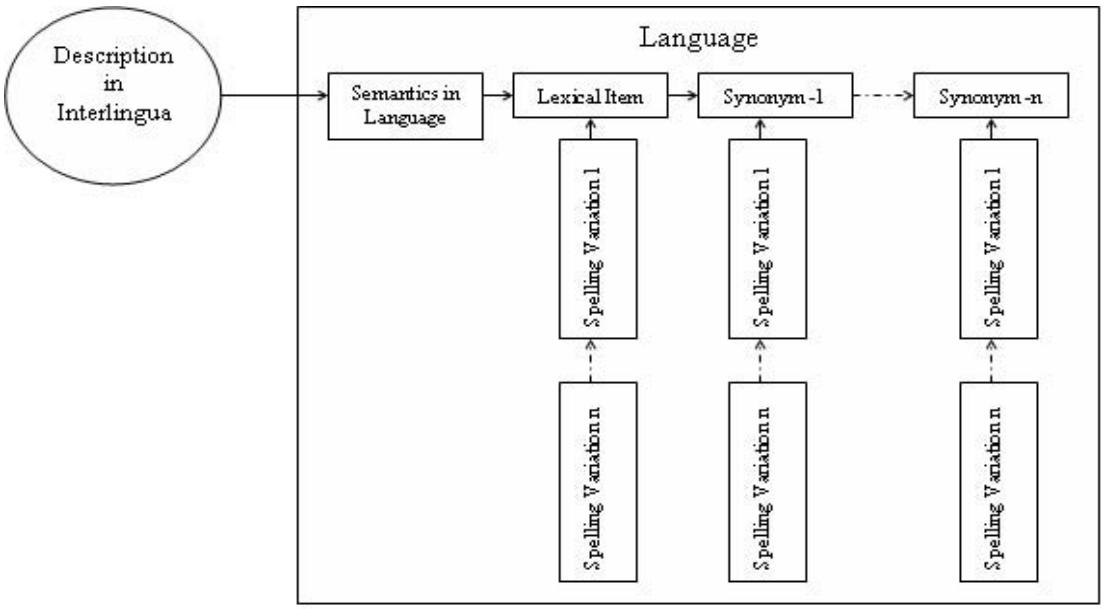
IPA, pronunciation, and transliteration can be embedded in the system. To expedite the data entry, a graphical user interface (GUI) can be provided, which automatically picks 'concept set model's synset along with their spelling variations as an entry. Other fields are provided manually.

As Interlingua is also a Natural Language, Many a times it may give a word which has more than one sense to a linking word. That's why 'description-along-with-lexical-item-and-its-grammatical-category' should be represented in Interlingua with a specific index. The Secondary Languages which are getting linked in Multilingual Dictionary can be able to give their Lexical Items to that Concept-Set.

Many a times the Interlingua may not be able to provide any lexical item for a multilingual language's lexical item. In such cases a detailed description has to be given in Interlingua in concept set.

For e.g. : If there exists a word like 'Abhisarika' (ಅಭಿಸಾರಿಕಾ) in Kannada, meaning 'The lady who goes rendezvous with her significant-other', if English used as an Interlingua which may not have a corresponding lexical item for it then the whole Description of 'Abhisarika' in English (interlingua) can be used. Other languages of the multilingual dictionary will give corresponding lexical entry (or description in case no corresponding lexical entry exists).

In this proposed model Interlingua can be any Language, but as it is used only for linking, and has only description, the Interlingua by itself cannot be one among the Multilingual Dictionary Language. The language used for the Interlingua also has to be represented like any other language and has to use the Concept Set as any other Language.



Graphical Representation of Linking of Interlingua-Description with a Lexical Entry of a Language

The major advantage in this approach is; all language of the multilingual dictionaries can enjoy primary language status. A methodology can be devised for a particular period of time, where one language will have primary language status and goes on adding lexical items to Interlingua description, and other languages (Secondary Languages) will give their corresponding lexical items for each Interlingua description added by the primary language. After the time period is over some other language will take over as primary language.

II. Summary

Multilingual Electronic Dictionaries attempt to provide wide ranging information, and cater the needs of a user to know about a specific linguistic item in a language and its morphemic equivalent across languages. It also provides information at different levels from graphemic to idiomatic expressions and beyond. Its architecture is modular; hence, it can be customised according to the needs of the specific applications/ users.

In its conceptualisation and design, specific information of an item is provided at the strata which are called levels that can be customised according to the requirements. Each level provides specific information. The multilingual digital linguistic database can be enriched with more and more languages, drawing cross-linguistic morphemic similarities and differences between languages. On the other hand, it is conceptualised as a model of what a native speaker of a language knows about an item in his/her language synchronically/diachronically.

References References Referencias

1. Rajesha N, Ramya M, Samar Sinha, 2010, Lexipedia: A Multilingual Digital Linguistic Database, published by"LANGUAGE IN INDIA" Volume-11: 5-May-2011 ISSN 1930 - 2940 http://languageinindia.com/may2011/rajesharamyasamar.pdf.
2. Ivan A DERHANSKI, 2009, Bi-and Multilingual Electronic Dictionaires: Their Design and Application to Low- and Middle-Density Languages, Language engineering for lesser-studied languages, IOS Press, PP-123.
3. Igor Boguslavsky, Jesús Cardeñosa, Carolina Gallardo 2009, "A Novel Approach to Creating Disambiguated Multilingual Dictionaries", Applied Linguistics (2009) 30 (1): pp 70-92.
4. Kavi Narayana Murthy. 2006. Natural Language Processing : An Information Access Perspective . New Delhi: Ess Ess Publications.
5. Samar Sinha 2011. - (A causerie on churning of speech sounds), NEILS 6 Conference, Tezpur University, Tezpur, Assam 31 Jan - 2 Feb, 2011.
6. Ammar Merhbi 2009. Corpus Linguistics, Concordance and Data-Driven Learning: An innovative Language Teaching Approach!.

Global Journal of Computer Science and Technology
Volume 11 Issue 20 Version 1.0 December 2011
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

The Impact of Spatial Masking in Image Quality Meters

By M.T. Qadri, K.T. Tan, M. Ghanbari
University of Essex, UK

Abstract - Compression of digital image and video leads to block-based visible distortions like blockiness. The PSNR quality metric doesn't correlate well with the subjective metric as it doesn't take into consideration the impact of human visual system. In this work, we study the impact of human visual system in masking the coding distortions and its effect on the accuracy of the quality meter. We have chosen blockiness which is the most common coding distortion in DCT-based JPEG or intra- coded video. We have studied the role of spatial masking by applying different masking techniques on full, reduced and no reference meters. As the visibility of distortion is content dependent, the distortion needs to be masked according to the spatial activity of the image. The results show that the complexity of spatial masking may be reduced by using the reference information efficiently. For full and reduced reference meters the spatial masking hasn't much importance, if the blockiness detection is accurate, while for the no reference meter spatial masking is required to compensate the absence of any required reference information.

Keywords : *Image Quality Assessment, Spatial Masking, Blockiness Measurement, Frequency Domian Analysis.*

GJCST Classification : *I.4.8, I.4.7*

Strictly as per the compliance and regulations of:

The Impact of Spatial Masking in Image Quality Meters

M.T. Qadri[α], K.T. Tan[Ω], M. Ghanbari[β]

Abstract - Compression of digital image and video leads to block-based visible distortions like blockiness. The PSNR quality metric doesn't correlate well with the subjective metric as it doesn't take into consideration the impact of human visual system. In this work, we study the impact of human visual system in masking the coding distortions and its effect on the accuracy of the quality meter. We have chosen blockiness which is the most common coding distortion in DCT-based JPEG or intra- coded video. We have studied the role of spatial masking by applying different masking techniques on full, reduced and no reference meters. As the visibility of distortion is content dependent, the distortion needs to be masked according to the spatial activity of the image. The results show that the complexity of spatial masking may be reduced by using the reference information efficiently. For full and reduced reference meters the spatial masking hasn't much importance, if the blockiness detection is accurate, while for the no reference meter spatial masking is required to compensate the absence of any required reference information.

Keywords : *Image Quality Assessment, Spatial Masking, Blockiness Measurement, Frequency Domian Analysis.*

I. Introduction

The coding of images and video introduces artefacts like blockiness, blurriness, ringing etc. Blockiness is the most common artefact in block based compression techniques. For fixed size DCT blocks, in high compressions, luminance changes do appear as regular patterns at the DCT block boundaries. Many researchers [1-11] have designed objective quality meters which use engineering approaches to determine the image quality. They are divided into full reference (FR), reduced reference (RR) and no reference (NR) meters. Full reference requires the entire reference image to be available at user end while reduced reference requires some features of the reference image. No reference meters don't require any information of reference image to be available at user side.

In literature various kinds of spatial maskings are used by the researchers ranging from very simple tools to the very complex psychological models. Many of them have studied the non-linear behavior of human visual system and its sensitivity with frequency variations. The aim of this paper is to investigate how important is the sophistication of a spatial masking in the accuracy of a quality meter and whether it is or is not equally effective for all types of the reference models. Our experiments show that if the blockiness detection is accurate then by using the reference information the role of spatial masking is reduced. However, in no reference mode the spatial masking is required to compensate the absence of any reference information.

For the full and reduced reference meters, different masking techniques are applied which improve the quality of meter but improvement is not much significant in weight if compared with the complexity and processing time consumed for masking.

The simplest masking includes edge cancellation between reference and coded images but it is only applicable for FR and RR modes only. Edge cancellation process helps to distinguish between natural edges of the image and sharp edges due to blockiness artifact. The edge cancelled image which contains edges only due to blockiness is then processed for frequency domain analysis to estimate the distortion.

For NR meter, more complex masking technique is required to mimic the behavior of human visual system. Edge cancellation process is not possible in no reference mode therefore a more reliable blockiness detector is required to discriminate natural edges from artificial edges appeared due to blockiness. Fortunately we have shown that through Fourier analysis one can easily separate the periodic pattern resulting from the regular blockiness edges from the irregular natural edges [12]. For the effective spatial masking, one can use Fiorentini and Zoli [13] masking technique after the edge detection process to mask the distortion before quantifying the blockiness in frequency domain. They calculate the masking function for each pixel by using the adjacent pixel values in order to compensate the distortion locally to apply the property of human visual system. The perception is that the humans observe less distortion in detailed areas because the distortion is masked by the details present in adjacent pixels. This technique of course has no masking effect on the regular edges resulting from the blockiness. This masking technique can be very useful in the no reference meter but it requires more processing time as discussed in section V.

We have tested various masking functions with the three FR, RR and NR models on LIVE image

Author α β : School of Computer Science and Electronic Engineering, Fellow IEEE, University of Essex, UK.
E-mail : mtqadr@essex.ac.uk, ghan@essex.ac.uk
Author Ω : School of Electrical and Electronic Engineering Singapore Polytechnic, Singapore. E-mail : kttan@sp.edu.sg

database [14]. There are 233 images in this database, where they are DCT coded and compressed at various quality. There is a mean opinion score (MOS) assigned to each compressed image, where we can test the accuracy of our meters against these scores.

The rest of the paper is organized as follows: Section II gives an overview of blockiness measurement in frequency domain and the details of blockiness detection for each model is given in its own section. Section III explains blockiness detection and the role of spatial masking in Full Reference model. These for the Reduced Reference model are given in section IV and those for No Reference model are given in section V. Finally the concluding remarks are given in section VI.

II. Overview of Blockiness Measurement

Since, the Blockiness artifact is due to the discontinuities in pixel intensity across DCT block boundaries, for a fixed DCT block size i.e. 8x8, this discontinuity appears as a periodic pattern. Transforming the pattern into a frequency domain, it will appear as harmonics at certain frequencies. The periodicity of the pattern makes it easy to discriminate blockiness edges from the natural ones. The strength of these harmonics are proportional to the amount of blockiness in the coded picture. The sum of energy concentrated in these harmonics is therefore used for blockiness estimation [12]. Figure below illustrates the concept of blockiness measurement through harmonic analysis in the frequency domain.

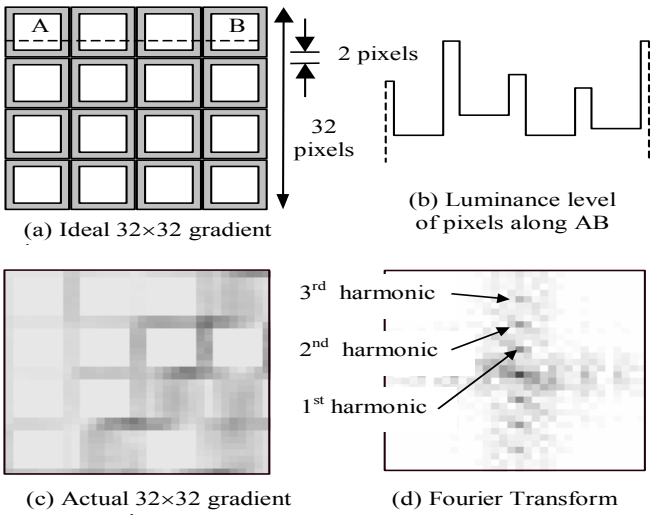


Fig 1 : Basic concept of Harmonic Amplitude Analysis

Figure 1(a) shows the gradient of block of 8x8 pixels within a 32x32 pixel image. Scanning of the gradient image results in a rectangular waveform as shown in figure 1(b). Fourier transform of this waveform generates harmonics at the spatial frequencies of multiple of 8/32. For real images, figure 1(c) shows the gradient of a real blocky image at block dimensions of 8x8 pixels. The two dimensional harmonics of the image with a 2D Fourier transform is shown in figure 1(d). Naturally if the image didn't have such a regular pattern, then the image energy in these harmonics will be nonexistent. Comparing the image energy at these harmonics with those of whole block energy at the ac coefficients can give an indication of blockiness [12].

III. Full Reference Blockiness Meter

In full reference meter, the complete reference image is used with the coded image to determine the quality. Initially the distortion meter is designed using the frequency domain approach without using any spatial masking technique. Section A of this part discusses the blockiness estimation in full reference mode using harmonics analysis in frequency domain and in section B the impact of different spatial masking is discovered to improve the quality of distortion meter.

a) Overview of Blockiness Estimation in FR Mode

The block diagram of the simplest full reference meter without using any spatial masking is given in figure below.

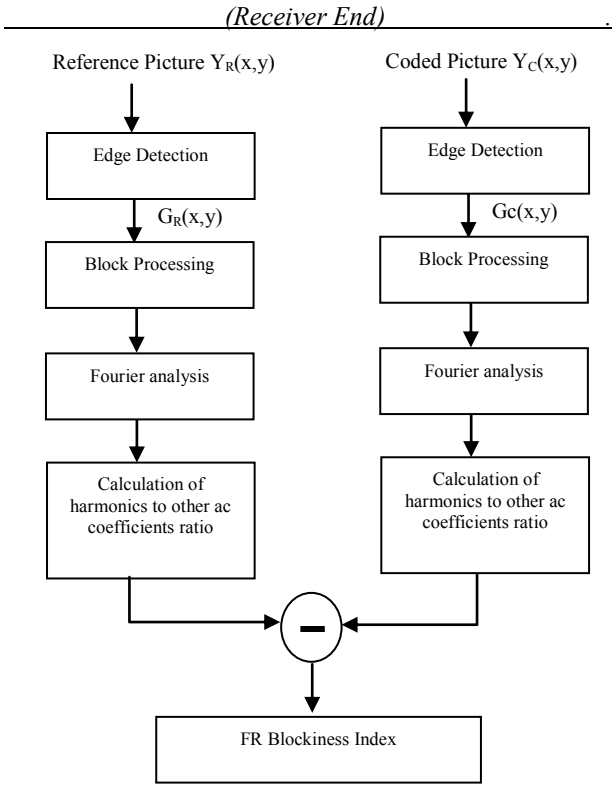


Fig 2 : Block diagram of full reference blockiness meter

Due to the availability of complete reference image at user end, the first step is to apply the edge detection process on both reference and coded images. It is used to determine the sharp luminance edges which

might be because of the details present in the image or because of the blockiness artifact, as blockiness results in sharp luminance discontinuities at DCT block boundaries. The edge detection process is performed in horizontal and vertical directions on both images separately. The chances of misreading textual details to be treated as blockiness artifact are reduced by using gradient versions of both images.

Since, the blockiness distortion is not likely to be the same in all parts of the image, therefore both of the resulted edge detected gradient images are then divided into blocks in spatial domain to determine the blockiness locally for each block. The block size must be any multiple of 8x8 (DCT block size). Here 32x32 block size is selected to keep the appropriate distance between harmonics. After block processing, each block is transformed into frequency domain and harmonics are calculated for each block for both gradient images. Each block of 32x32 will have a DC coefficient and two repetitive groups of 15 ac components in horizontal and vertical directions denoted by H1-H15 and V1-V15 respectively. Of these ac components, the particular frequency components are extracted which have same spatial frequency as the blockiness pattern (i.e. 8 pixels/cycle) and its multiples, called harmonics. These harmonics can be determined using the following equation.

$$f_k = k * \left(\frac{w}{8}\right), \quad \text{for k} = 1,2,\ldots,\left(\frac{w}{8} - 1\right) \tag{1}$$

where, f_k is the frequency of harmonics in cycles per window (cpw), and w is the width of the FFT window. For 32×32 FFT window, the interested harmonic frequencies are 4 cpw, 8 cpw, and 12 cpw, which are in fact the H4, H8 and H12 for the horizontal direction, and V4, V8 and V12 for the vertical direction. The equations for the horizontal and vertical blockiness parameter are given below:

$$Rh = \frac{\sum(H_4+H_8+H_{12})}{\sum_{n=1}^{16} H_n} \tag{2}$$

and

$$Rv = \frac{\sum(V_4+V_8+V_{12})}{\sum_{n=1}^{16} V_n} \tag{3}$$

The above ratio is calculated for each 32x32 pixels block of reference and coded images and then compared to determine the amount of blockiness locally for every block of the coded image. The blockier an image is, the higher will be the harmonics to AC components ratio. Finally, the blockiness of each block is accumulated at the end for a single quality metric.

The objective results are compared with the mean opinion scores of images from LIVE image database. The Pearson's correlation coefficient of 95.75% is obtained by using the above full reference frequency domain analysis without using any complex spatial masking technique.

b) Effect of Spatial Masking in Full Reference Mode

The spatial masking helps to compensate the distortion according to the local spatial activity of the image. In this section, different spatial maskings techniques are applied with the above full reference meter to compare its effect and highlight the importance of spatial masking in quality estimation.

The simplest spatial masking is implemented by cancelling the textual edges between gradient versions of reference and coded images. For blockiness estimation, the detection of sharp luminance edges at DCT block boundaries are needed whereas simply edge detection process may treat natural edges and textual details as blockiness distortion. To avoid misinterpreting textual edges as blockiness, Edge Cancellation process is included which cancels the natural edges and leaves only edges because of blockiness artifact. It improves the efficiency of distortion meter.

The edge cancelled image is obtained by taking the difference of reference and coded gradient images. To determine the blockiness locally, the edge cancelled gradient image is divided into blocks and then each block is transformed into frequency domain. If the coded image is affected by blockiness then the edge cancelled gradient image must have harmonics at spatial frequencies and by comparing the harmonics with other ac coefficients, the blockiness can be estimated accurately. The Pearson's correlation coefficient of 96.12% is obtained by including the edge cancellation process which improves the above results by 0.3%. The block diagram of the full reference meter with edge cancellation process is given below.

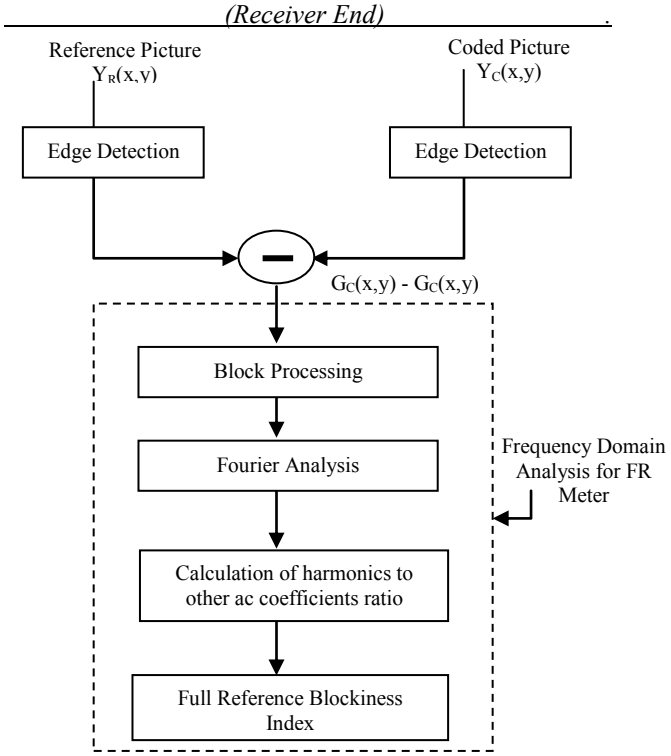


Fig 3 : Block diagram of FR blockiness meter with edge cancellation process

As the human visual system is non-linear and sensitive to different frequency variations this means that users observe different amount of distortion depending upon the adjacent details. The distortion will be masked by the nearby details and be less visible to human observers. Applying more sophisticated masking technique includes the features of human visual. This property is implemented by using the masking technique by Fiorentini and Zoli [13]. For this purpose, the local masking function is calculated for each pixel using the adjacent pixel values to implement the property of human visual system. For each pixel in gradient reference image, the adjacent horizontal and vertical pixels (5 adjacent pixels) are compared and the minimum value is chosen which represents the maximum masking effect for that pixel. The process is applied for each pixel of gradient reference image and the final masking function is determined which contains the spatial activity of the reference image.

The masking function is then convolved with the edge cancelled coded gradient image to mask the distortion. Then the block processing is applied on masked coded image and each block is transformed into frequency domain analysis. For each block, the harmonics to other ac coefficients ratio is calculated to determine the blockiness distortion locally. Finally, the distortion of each block is accumulated in the end for single value. The Pearson's correlation coefficient is improved to 96.25% by using this masking technique. The block diagram including above masking technique is given below.

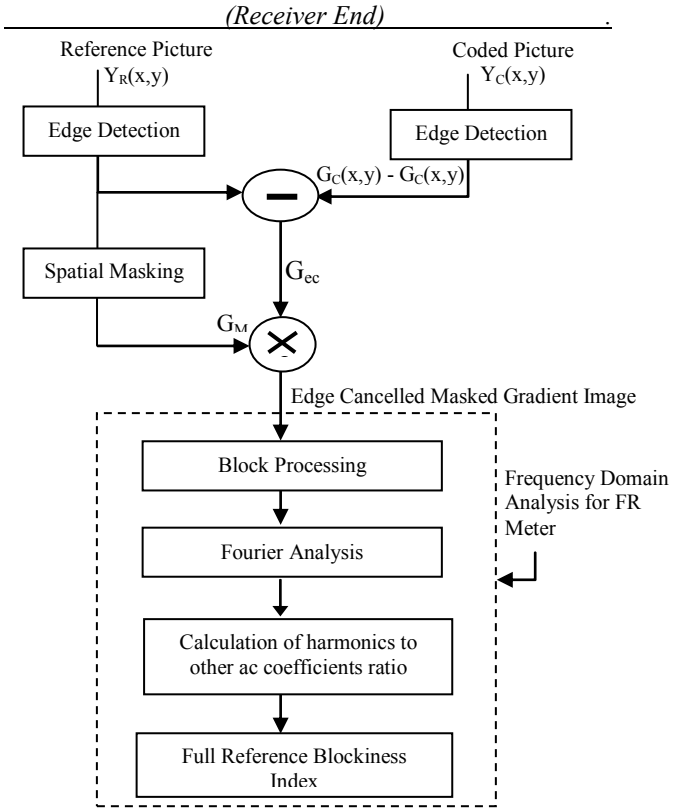


Fig 4 : Block diagram of FR blockiness meter with spatial maskings

To conclude the discussion for full reference distortion meter, the table below summarizes the effect of spatial masking on full reference meter.

Table 1 : Effect of different maskings on FR blockiness meter

FR Blockiness Meter	Processing Time	Correlation Coefficient
Without Any Masking	1 Unit	95.75%
Edge Cancellation	1.33 Units	96.12%
Fiorentini and Zoli Masking	4.18 Units	96.25%

Due to the availability of the complete reference image at user end in full reference mode, the spatial masking has not much importance in full reference mode. However, it helps to improve the accuracy of the meter but it increases the complexity and processing time of the system. Since masking also increases some processing burden to the quality meter, the table also shows how much this is increased due to the calculation of masking function.

IV. Reduced Reference Blockiness Meter

The availability of some reference features at user end in reduced reference mode helps to reduce the complexity of spatial masking. Part A of this section discusses the blockiness estimation in RR mode without using any spatial masking technique while part B examines the role of spatial masking in reduced reference meter.

a) Overview of Blockiness Estimation in RR Mode

Since, blockiness has periodic patterns which are represented by harmonics in frequency domain, therefore the strength of ac coefficients at harmonics frequency i.e. 4th, 8th and 12th ac coefficient of each block in frequency domain are used as reduced reference parameter. The block diagram of the simplest reduced reference blockiness meter without using any spatial masking is given below.

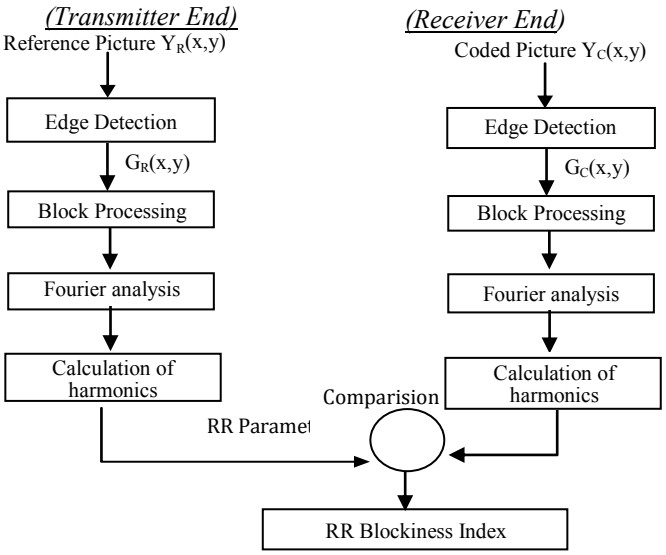


Fig 5 : Block diagram of reduced reference meter without any masking

For RR meter, a similar approach to FR is used except that, instead of using complete reference image, some of its features are used which reduces the quality of RR meter. The procedures include edge detection, block processing (of 32x32 pixels in spatial domain) and then frequency domain analysis of each block to determine the strength of harmonics of reference image. For each block, vertical and horizontal harmonics of the reference and coded images are compared to calculate the amount of distortion locally. The equations of vertical and horizontal harmonics of reference and coded images are given below.

$$R_{ref} = \sum(H_4 + H_8 + H_{12} + V_4 + V_8 + V_{12})_{reference} \quad (4)$$

and

$$R_{coded} = \sum(H_4 + H_8 + H_{12} + V_4 + V_8 + V_{12})_{coded} \quad (5)$$

Finally, the average of blockiness distortion is calculated at the end for a single quality metric. The RR meter is tested on LIVE image database and the Pearson's correlation coefficient of 88.2% is obtained with no spatial masking used.

b) Effect of Spatial Masking in Reduced Reference Mode

In the above RR distortion meter, natural edges in the reference picture located at DCT block boundaries may be treated as blockiness which may be mistakenly considered as harmonics in frequency domain. To improve the quality of RR meter, the sharp edges at DCT block boundaries must be distinguished with edges due to blockiness artifact. For this purpose, edge cancellation process is applied to cancel natural edges of reference image. However, edge cancellation in RR mode is not as effective as in FR mode because it only cancels edges at block boundaries and leaves the remaining natural edges within the block. For edge cancellation in RR mode, the check is applied on each block to determine that weather the corresponding block is affected by blockiness or contains natural edges. Due to the fact that the blockiness increases the harmonics amplitude therefore if the strength of harmonics of coded image is greater than the harmonics of reference image i.e. $R_{coded} > R_{ref}$, then consider that block as blocky and determine the amount of blockiness by the difference in harmonics amplitudes. Using the edge cancellation process the correlation coefficient is improved by 5.39% which becomes as 93.59%.

The quality of distortion meter may be improved by including the spatial masking of Fiorentini and Zoli [13] as performed in FR mode. This technique is discussed in detail in section III. Here the masking is performed separately on reference and coded images in spatial domain before block processing. The harmonics of masked reference image are used as reduced reference parameter and compared with the harmonics of masked coded image to determine the amount of blockiness in coded image. The block diagram of the meter after including Fiorentini and Zoli is given below.

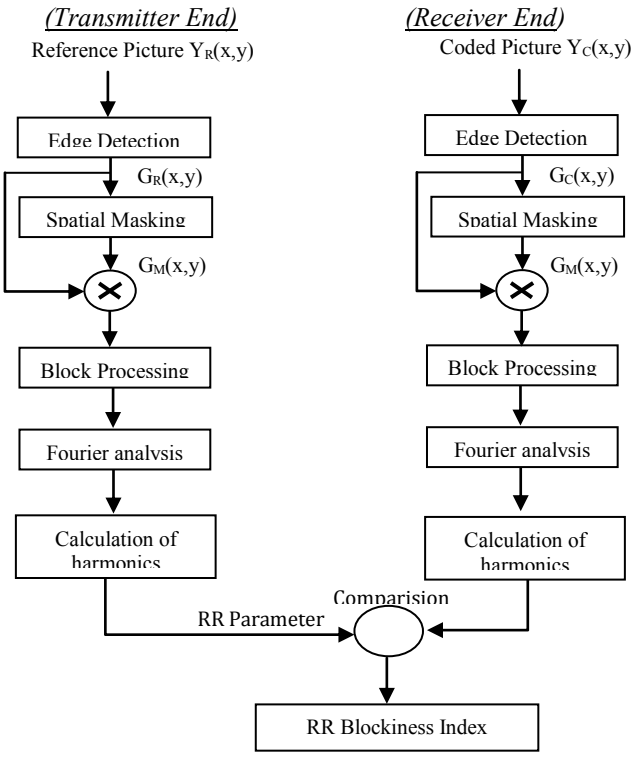


Fig 6 : Block diagram of RR meter with spatial masking

By using this masking technique the correlation coefficient is increased to 94.89% but it increases the complexity and processing time of the system. The table below summarizes the effect of spatial masking on reduced reference meter.

Table 2 : Effect of different maskings on RR blockiness meter

RR Blockiness Meter	Processing Time	Correlation Coefficient
Without any Masking	1 Unit	88.2%
Edge Cancellation	1.2 Units	93.59%
Fiorentini and Zoli Masking	6.7 Units	94.89%

Due to unavailability of full reference image at user end in RR mode, the edge cancellation process helps to discriminate between natural edges and edges due to blockiness. But using complex masking techniques may improve the results but they require more processing time as shown in table 2 above.

V. No Reference Blockiness Meter

The spatial masking has more importance in no reference mode to compensate the absence of any reference information. The basic idea of blockiness estimation is the same as used for FR and RR techniques above. Part A explains the method for

measuring blockiness distortion in no reference mode and in part B, the role of spatial masking is discussed using different masking techniques.

a) Overview of Blockiness Estimation in NR Mode

There is only coded image available to determine the quality therefore all processes which includes edge detection, block processing and frequency domain analysis must be applied on the coded image itself. The block diagram of the NR meter without using any masking is given below.

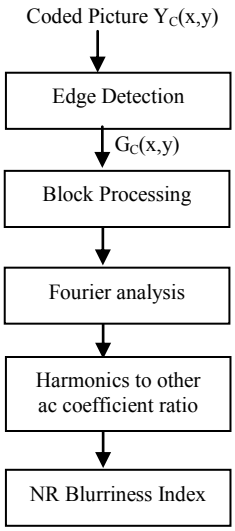


Fig 7 : Block diagram of NR meter without any masking

After the edge detection and block processing in spatial domain, the blockiness is estimated in frequency domain by comparing the amplitude of harmonics to other ac coefficients as blockiness results in harmonics in frequency domain due to their periodic patterns at DCT block boundaries. Due to absence of any reference, the accuracy of NR meter is not as good as FR and RR approaches because there are chances of interpreting natural edges as blockiness as the their cancellation is not possible without any reference information. The Pearson's correlation coefficient of 83.72% is achieved for no reference blockiness meter without using any masking.

b) Effect of Spatial Masking in No Reference Mode

The absence of reference information reduces the quality of NR meter as there is no other way to distinguish between natural and blockiness edges except the distortion must be masked before frequency domain analysis. For this purpose, the spatial masking from Fiorentini and Zoli [13], discussed in section III, is applied on edge detected version of the coded image itself to mask the distortion according to the local spatial activity. Here, the same coded image is used to determine the spatial activity because the overall spatial activity of the coded image would roughly be same as of reference picture. The rest of the procedures are same as used for above techniques. The block diagram of the NR meter with spatial masking is given below.

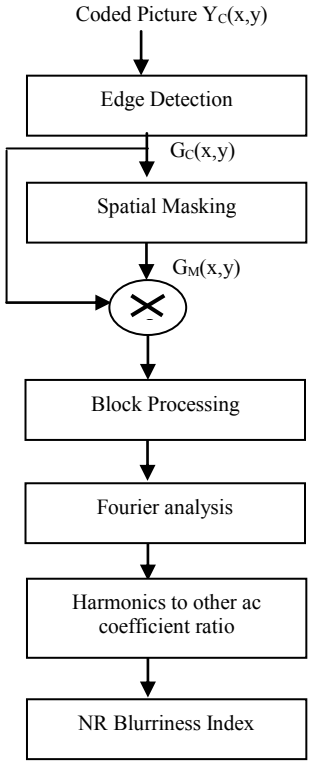


Fig 8 : Block diagram of NR meter with masking

The correlation coefficient of 90.30% is obtained by including the spatial masking from Fiorentini and Zoli. The table below summarizes the effect of spatial masking on no reference meter.

Table 3 : Effect of different maskings on NR blockiness meter

NR Blockiness Meter	Processing Time	Correlation Coefficient
Without any Masking	1 Unit	83.72%
Edge Cancellation	Not Possible due to absence of any reference	
Fiorentini and Zoli Masking	3.6 Units	90.30%

The above results show that the spatial masking is essential in NR mode as natural edges of the image may be treated as blockiness edges because of the absence of any reference information.

VI. Conclusion

The aim of the work is to determine the importance of spatial masking in FR, RR and NR modes. Different masking techniques, from simple to complex, are applied on all three types of meters. The algorithm is tested on LIVE image database of blocky images compressed at different compression rates. The

database consists of 233 images with their mean opinion scores. The results show that the complexity of spatial masking can be reduced by using the reference information. For FR meter, in table 1, due to availability of complete reference image, there is virtually no need of using any masking techniques. The accurate blockiness detection is possible using the gradient versions of reference and coded images. However, in RR mode, in table 2, the features of reference image can be used to distinguish natural and blockiness edges to improve the quality of distortion meter. Simple cancellation of natural edges at DCT block boundaries helps to develop a reliable distortion meter and there is no need for any sophisticated spatial masking.

Finally, in NR mode, as in table 3, complex masking techniques are required to compensate the absence of any required information, this is because some part of natural edges may be miscalculated as blockiness and the masking will reduce this miscalculation. However, the accuracy is not as good as for FR and RR meters. It shows that the spatial masking is necessary to compensate the reference information but if the reference information is available, the role of spatial masking is not vital.

References Références Referencias

1. K. Seshadrinathan, R. Soundararajan, A. C. Bovik and L. K. Cormack, "Study of Subjective and Objective Quality Assessment of Video", IEEE Transactions on Image Processing, vol.19, no.6, pp.1427-1441, June 2010.
2. K. Seshadrinathan, R. Soundararajan, A. C. Bovik and L. K. Cormack, "A Subjective Study to Evaluate Video Quality Assessment Algorithms", SPIE Proceedings Human Vision and Electronic Imaging, Jan. 2010.
3. A.A. Webster, C.T. Jones, M.H. Pinson, S.D. Voran, S. Wolf, "An objective video quality assessment system based on human perception," SPIE Human Vision, Visual Processing, and Digital Display IV, San Jose, CA, February 1993, pp. 15–26.
4. Z. Wang, A. C. Bovik, and B. L. Evans, "Blind measurement of blocking artefacts in images," in IEEE Int. Conf. Image Processing, September 2000, vol. 3, p. 981-984, IEEE.
5. H. R. Wu and M. Yuen, "A generalized block-edge impairment metric for video coding," IEEE Signal Processing Letters, Vol. 4, Nov. 1997, pp. 317-320.
6. L. Meesters and J. B. Martens, "A single-ended blockiness measure for JPEG-coded images", Signal Process., Vol. 82, pp. 369-387, 2002.
7. Z. M. Parvez Sazzad, Y. Kawayoke, and Y. Horita, "No-reference image quality assessment for jpeg2000 based on spatial features," Signal Processing: Image Communication, vol. 23, no. 4, pp. 257–268, April 2008.
8. Zhu and P. Milanfar, "A no-reference sharpness metric sensitive to blur and noise", QoMEX, 2009. July 29–31, 2009, San Diego, California, U.S.A.
9. M. G. Choi, J. H. Jung, and J. W. Jeon, "No-Reference Image Quality Assessment using Blur and Noise," in International Journal of Computer Science and Engineering 3:2 2009, pp. 76–80.
10. R. Barland and A. Saadane, "A new reference free approach for the quality assessment of mpeg coded videos," in 7th Int. Conf. Advanced Concepts for Intelligent Vision Systems, Sep. 2005, vol. 3708, pp. 364–371.
11. H. R. Wu and M. Yuen, "A generalized block-edge impairment metric for video coding," IEEE Signal Processing Letters, Vol. 4, Nov. 1997, pp. 317-320.
12. K. T. Tan, M. Ghanbari, "Frequency domain measurement of blockiness in MPEG-2 coded video," Proceedings of ICIP 2000, Vol. 3, pp.977 – 980.
13. Fiorentini, A. and Zoli, M. T., "Detection of a Target Superimposed to a Step Pattern of Illumination. II. Effects of a Just-Perceptible Illumination Step", Atti. Fond. G. Ronchi, Vol. 22, pp. 207-217,1967.
14. Live website for subjective scores MOS., http://live.ece.utexas.edu/research/quality/

This page is intentionally left blank

Global Journal of Computer Science and Technology
Volume 11 Issue 20 Version 1.0 December 2011
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

A Handoff using Guard Channels Scheme (HGCS) for Cognitive Radio Networks

By Madeeha Aman, Dr. Saeed Mahfooz, and Waheed Ur Rehman
University of Peshawar, Khyber Pakhtunkhwa, Pakistan

Abstract - Spectrum handoff is a very important phenomenon in Cognitive Radio (CR) networks. It provides flawless transmission upon the arrival of primary user (PU) while the channel is in use by the secondary user (SU). Spectrum handoff process provides the SUs with the opportunity to continue their communication on other unoccupied channels as soon as the PU repossesses its channel. FCC (Federal Communications Commission) has released new White Space rules in September 2010 which eliminate the requirement of spectrum sensing, making CRs more flexible. In addition, the CR is to be equipped with TV channel database. Taking these new rules into account, this paper suggests a new handoff scheme, HGCS (Handoff using Guard Channels Scheme), which makes effective use of the guard channels for communication. A preemptive resume priority (PRP) M/G/1 queuing network model is proposed to assess total service time for the suggested HGCS and comparing it to the existing random proactive-decision handoff scheme. Simulation and numerical results verify that HGCS can minimize the handoff delay, hence reduces the total service time compared to the random proactive approach.

Keywords : *Spectrum Handoff, Handoff Delay, Handoff using guard channels, Cognitive Radio.*

GJCST Classification : *C.2.1*

Strictly as per the compliance and regulations of:

A Handoff using Guard Channels Scheme (HGCS) for Cognitive Radio Networks

Madeeha Aman[α], Dr. Saeed Mahfooz[Ω], and Waheed Ur Rehman[β]

Abstract - Spectrum handoff is a very important phenomenon in Cognitive Radio (CR) networks. It provides flawless transmission upon the arrival of primary user (PU) while the channel is in use by the secondary user (SU). Spectrum handoff process provides the SUs with the opportunity to continue their communication on other unoccupied channels as soon as the PU repossesses its channel. FCC (Federal Communications Commission) has released new White Space rules in September 2010 which eliminate the requirement of spectrum sensing, making CRs more flexible. In addition, the CR is to be equipped with TV channel database. Taking these new rules into account, this paper suggests a new handoff scheme, HGCS (Handoff using Guard Channels Scheme), which makes effective use of the guard channels for communication. A preemptive resume priority (PRP) M/G/1 queuing network model is proposed to assess total service time for the suggested HGCS and comparing it to the existing random proactive-decision handoff scheme. Simulation and numerical results verify that HGCS can minimize the handoff delay, hence reduces the total service time compared to the random proactive approach.

Keywords : Spectrum Handoff, Handoff Delay, Handoff using guard channels, Cognitive Radio.

I. Introduction

The concept of software defined radio and CR was introduced to enhance the efficiency of frequency spectrum usage [1]. The Notice of Proposed Rule Making (NPRM) of the Federal Communications Commission (FCC) found the licensed band allocated to TV channels highly underutilized. To improve spectrum efficiency, they permitted secondary systems to function in the frequency band allocated to the television services [2] [3] [4]. Considering this, the IEEE 802.22 Working Group (WG) developed WRAN (Wireless Regional Area Network), a secondary system that will be operating in the licensed TV channels [5] [6].

The WRAN system was developed to provide wireless broadband access to the rural areas where broadband services have not yet reached due to certain physical limitations. To achieve this purpose, CR is seen as the solution, allowing capable and reliable use of spectrum by adjusting to the radio's environment accordingly [1] [7]. CR has emerged as a potential technology in order to increase the usage of the limited radio bandwidth in addition with accommodating the growing number of wireless services, devices and networks. A CR transceiver is an intelligent device that adjusts itself to the radio environment consequently increasing the utilization of the limited radio resources while providing flexibility in wireless access [8]. Although the requirement of spectrum sensing has been eliminated recently by FCC [18] as CR will now be equipped with TV channel database, the traditional CRs could perform following important functions [9]: (1) Sense the spectrum to find out the available portions and detects the presence of licensed users in a licensed band. (2) Choose the best suited vacant channel. (3) Sharing this channel with other users; and (4) Vacate the channel at the arrival of the licensed user.

Spectrum handoff is a very important aspect in CR networks. It manages flawless communication in case of PU arrival while the channel is being used by the SU. Spectrum mobility allows the SU to resume its transmission on another vacant channel when the PU reclaims its channel. In order to continue its transmission SU will have to look for an idle channel first, and then decide whether to switch to another channel or stay on the current channel to wait for it to become available again. In all this process there will be a notable amount of handoff delay.

This paper focuses on the issue of handoff delay caused during spectrum mobility under the new FCC September 2010 release. Radio frequency spectrum is a very precious and valuable resource. According to [9], TV channels and their guard channels are to be used for communication in IEEE 802.22, which is the first standard implementing CR technology. This concludes that guard channels can be used for communication. During handoff process we can make wise use of guard channels through intelligent hardware devices and by communication protocols. This concept was first floated in [24], this paper implements this concept and proposes a handoff to a guard channel scheme (HGCS) in order to reduce the handoff delay compared to the existing handoff schemes. The guard channels are vacant channels; SU will easily search and access them without any difficulty.

The rest of the paper is organized as follows: In section II and III related work and spectrum handoff

Author α : Research Scholar, Department of Computer Science, University of Peshawar, Khyber Pakhtunkhwa, Pakistan.
E-mail : madeeha_08@yahoo.com
Author Ω : Chairman, Department of Computer Science, University of Peshawar, Khyber Pakhtunkhwa, Pakistan.
E-mail : saeedmahfooz@upesh.edu.pk
Author β : Assistant Professor, Department of Computer Science, University of Peshawar, Khyber Pakhtunkhwa, Pakistan.
E-mail : wahrehman@upesh.edu.pk

mechanism is discussed. Followed by section IV and V which presents the proposed handoff to the guard channel scheme (HGCS) and numerical and simulation results. Finally section VI concludes the paper.

II. Related Work

Spectrum handoff varies from traditional handoff in wireless networks. Spectrum handoff takes place upon PU arrival whereas the handoff in wireless networks takes place due to signal degradation and user mobility. In nearly all of the existing spectrum handoff schemes [10]–[17], the handoff performance has been examined using numerous methods, taking into account different aspects discussed as follows:

In [10], authors explored spectrum handoff for link maintenance of three types, i.e., non-spectrum handoff, the proactive spectrum handoff, and the spectrum handoff depending on sensing mechanism. The authors have observed the performance based on the probability of link maintenance as well as the effective data rate of the SU's transmission. However their results reveal that there could be chances of erroneous and incorrect channel selection hence affecting the performance of SU. The authors in [11] have measured the handoff performance in opportunistic1 and negotiated2 situations. They have generalized the key tele-traffic parameters in both the primary system and the secondary system. Although the results show that opportunistic access provides higher SU service completion, nevertheless there will be an increase in handoff operations leading to noticeable amount of handoff delay. Whereas in [12] the authors have evaluated reactive-sensing spectrum handoff in comparison with proactive-sensing spectrum handoff. The authors have shown that proactive sensing minimizes transmission latency, although certain handoff delay still exists there. Moreover, [13] discusses a greedy approach to minimize total service time by selecting the target channels. Except that since there will be multiple spectrum handoffs, it will increase the number of interruptions resulting in a lot of channel switching overhead in resuming the transmission. In the study by [14], the authors propose a new scheme for spectrum handoff i.e. —Spectrum handoff to a backup channel‖ to reduce the consecutive spectrum handoffs. Even so the scheme is for wireless ad hoc networks only. The authors in [15] have proposed a post-sensing spectrum handoff scheme which is based on Markov decision process. This scheme tries to minimize the waiting time for packet transmission. However the delay involved for sensing process persists. In [16], the authors have introduced a voluntary spectrum handoff method that reduces forced handoffs for secondary users, making the secondary users have longer uninterrupted connection times. Except that since it is dependent on primary user estimation, there are chances of erroneous estimates. In addition, there will be an added complexity for the estimation process. In [17] the SU selects its operating channel based on the expected remaining idle period. Nonetheless it is dependent on past channel usage statistics for which the estimates could seldom be inaccurate.

All the spectrum handoff schemes discussed above have different shortcomings and the major one that is common in all of them is delay due to spectrum handoff. Other drawbacks include wastage of time, transmission latency, increase in transmission time for a SU caused by consecutive spectrum handoffs, chances of collision in case of proactive handoffs and increased complexity by estimating the PU arrival beforehand.

III. Spectrum Handoff

The spectrum handoff procedure has been discussed widely in many papers. Spectrum handoff takes place when a SU is operating on a licensed channel; meanwhile the PU gets activated and reclaims its channel. To continue its transmission, SU will search for an idle channel using different handoff schemes.

The traditional handoff procedure involves the sensing phase. FCC adopted and released new rules for White Space in September 2010 [18]. According to the new rules, the requirement for TV band devices to be capable of spectrum sensing has been eliminated, as the geo location and database access method are enough to provide reliable protection to TV channels. According to the new rules, the SU should have access to the TV channel database and it should be equipped with geo-location capability as well. The SU will then know if the channel is empty or taken up by PU, it does not need to sense the spectrum for idle channels anymore.

a) The traditional spectrum handoff procedure

- The SU has sensed the spectrum to find available channel for transmission.
- When the channel is available, the SU hops onto the channel and starts using it for transmission.

[1] No centralized spectrum agency managing the spectral band [11].
[2] A spectrum server centrally managing the whole spectrum [11].

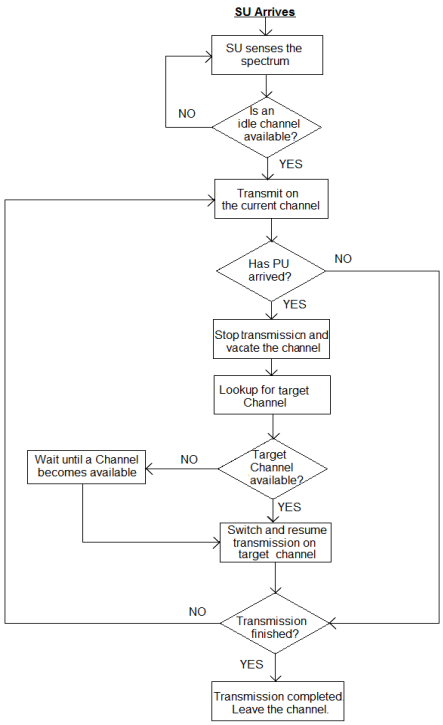


Fig.1 : Flow chart for traditional spectrum handoff

- When the SU detects the arrival of PU, it stops its transmission.
- The SU then vacates the channel, and resumes its transmission on the selected target channel.
- This process is repeated for as many times the interrupt occurs.

The flow chart of the traditional handoff procedure is shown in figure 1.

b) Handoff delay for traditional spectrum handoffs

The amount of delay caused during a handoff procedure relies on the handoff scheme used. These spectrum handoff schemes can be categorized as:

- Non spectrum handoff.
- Handoff based on radio sensing; which is further classified into Proactive sensing spectrum handoff and Reactive sensing spectrum handoff.

Handoff delay is termed as the time period from the moment of suspending frame transmission until the moment of resuming the transmission [12]. In case of non-spectrum handoff, the secondary user will wait for the same channel it had previously transmitted on before interrupt to become available again. In this case, the total handoff delay will be the waiting time on the channel for it to become idle again after each interrupt. [13] Calculates the handoff delay for non-spectrum handoff as,

$$E[D] = Y_o \qquad (1)$$

Where E[D] denotes the handoff delay and Y_o is the average busy period resulted from the PU of the channel.

In case of reactive approach, the delay will be the time required to find another channel on the spot, and wide band sensing will be needed. [12] Calculates the delay due to reactive approach as,

$$E[D_{reactive}] = t_p \qquad (2)$$

Where *tp* denotes the processing time which is the sum of channel switching time ts and channel sensing time *tf*.

In case of proactive approach, a backup channel is ready before transmission, the delay comprises of waiting time in queue as well as the waiting time on channel. [12] Calculates the delay due to proactive approach as,

$$E[D_{proactive}] = \min\{E[D_{stay}], E[D_{change}]\} \qquad (3)$$

Where $E[D_{stay}]$ is the delay if the SU chooses to stay on the channel and wait for it to become available and $E[D_{change}]$ is the delay if the SU chooses not to wait for the current channel and hops onto to an available backup channel.

Proactive decision spectrum handoff reduces handoff delay as compared to reactive handoff since sensing all over again is not required [19]. This paper proposes a HGCS scheme that will minimize the handoff delay and total service time even more than the proactive strategy.

c) The Spectrum Handoff Procedure under new FCC rules

With these new rules, a typical TV band CR device mechanism now becomes:

- SU is connected to a fixed device that has access to TV channel database and is equipped with geo-location facility.
- SU obtains a list of idle channels from the fixed device.
- The SU selects a channel from the list and starts using it for transmission.
- The SU will already be aware of the arrival of PU. It will stop transmission and vacate the channel upon the arrival of PU.
- The SU will use a spectrum handoff mechanism to vacate the channel upon the arrival of PU.
- According to the spectrum handoff mechanism used, the SU will have already looked up or will then look up the available TV channel list for another idle channel for transmission.
- If another idle channel is available in the TV channel list, the SU will hop on to it and resume its transmission on the new idle channel.
- Else the SU then stays on the current channel and will wait for it to become available again.
- For the number of times the SU is interrupted, the above handoff procedure is repeated for each time.

d) Handoff Delay under new FCC rules

The handoff delay depends on two major aspects, one is due to the handoff scheme applied and secondly due to the time needed in spectrum sensing phase. The major difference between traditional and new procedure handoff is that the new procedure eliminates spectrum sensing phase. Its delay will only depend on the handoff scheme used, where as in traditional approach both aspects need to be considered.

IV. Handoff to the Guard Channel Scheme (HGCS)

This paper reduces the handoff delay and hence the total service time for 802.22 networks using CR technology using the concept introduced in [24]. IEEE 802.22 is the first wireless standard based on CRs [5]. A slotted-based CR network is considered as in [13], with essential modifications made to it. Since the sensing requirement has been eliminated by FCC [18], each slot now consists of available TV channels list lookup phase and transmission phase. SU must obtain a list of available channels from TV Channel database before data transmission. The proposed handoff solution is a combination of proactive handoff strategy and HGCS strategy.

a) The proposed HGCS Scheme

This section gives an overview of the proposed HGCS scheme. The assumptions are summarized as follows,

- All the SU nodes are equipped with CR technology.
- The spectrum to be used for unlicensed communication by SU is the licensed spectrum of the PU (i.e. the TV channels).
- The SUs are mode I personal/ portable TVBDs (TV Band Devices) connected to a fixed mode II TVBD which is capable of determining the available channels at its location using geo-location and database access [23]. Figure 2 shows the scenario.
- SU can use the licensed channel for unlicensed use with the condition that the PU can preempt the SU when it arrives.
- The SUs are served on first come first serve (FCFS) basis.
- The PRP M/G/13 queuing network model proposed in [12] and [13] is followed with essential modifications made to it.
- There are guard channels that exist between the transmission channels. We assume that guard channels can be used for communication [9].
- Further we assume, as in [20] that while communicating on the guard channels the integrity of the system will be preserved. It will not interfere with the transmission of other channels. This has been made possible by superimposing the information signals in the guard frequency bands. [20] Proves that guard bands can be used for communication and that a proper method as well as an apparatus exists for it.

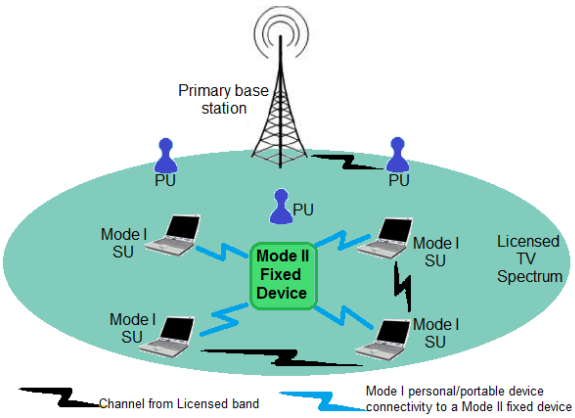


Fig.2 : Assumed CR Network Scenario

- It is assumed that SUs will communicate with each other by accessing their base station [22], which will be the fixed mode II TVBD they are connected to. Further, the base station maintains a database of all the channels and guard channels being used by the SUs.
- The proposed scheme is for IEEE 802.22 scenario, where RF channel bandwidth as well as the guard channel bandwidth is 6 MHz [9] [21], so the quality of the transmission will not be affected.

The steps of the proposed scheme HGCS are described as follows:

1. The SU obtains a list of available channels from the TV channel database of fixed Mode II device it is connected to.
2. SU selects a channel for transmission from the provided list.
3. SU starts using the selected channel for its transmission.
4. The SU will know from the TV channel list when to expect the PU back on the channel. It will vacate the channel as soon as the PU is back.
5. The SU will now look up the TV channel list for another channel. If available, it hops onto it and resumes its transmission.
6. If no other channel is available in the TV channel list, the SU will access its base station (the fixed mode II device) to look up the database of guard channels being used by other SUs.

[3] PRP M/G/1 queuing network model is a Preemptive Resume Priority queuing network model with Markovian (exponential) distribution inter arrival time of PU and SU. It has a General distribution service time with 1 or more channels. The model is used to characterize the spectrum handoff for random proactive approach and proposed HGCS approach.

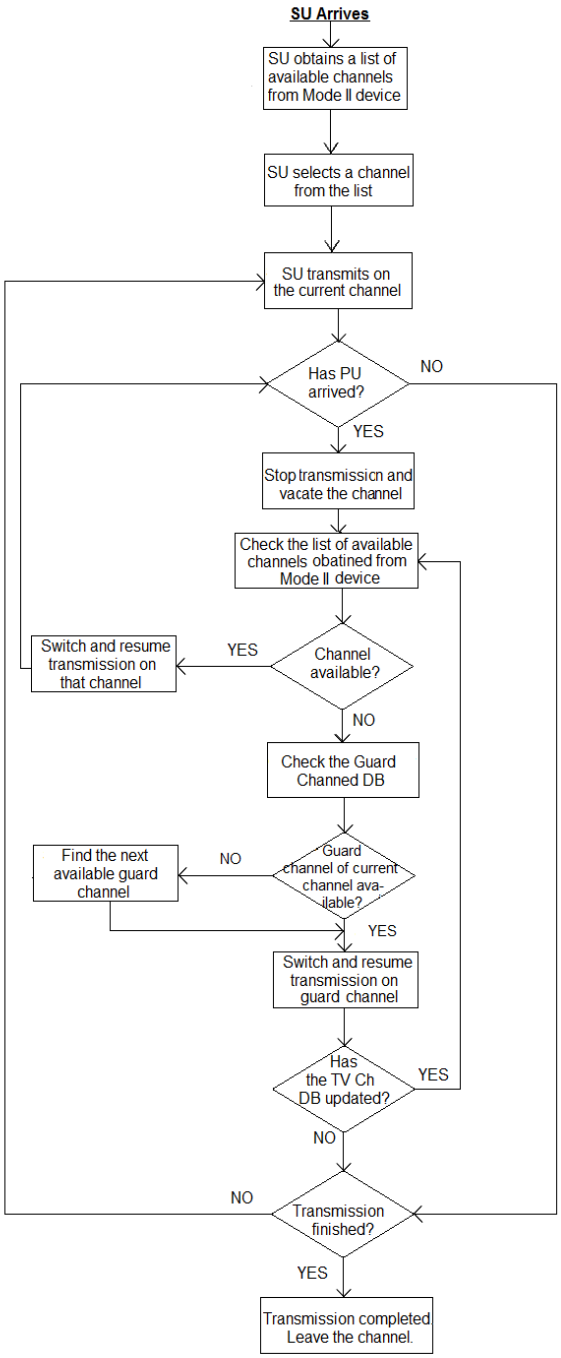


Fig.3 : Flow chart for the proposed HGCS Scheme

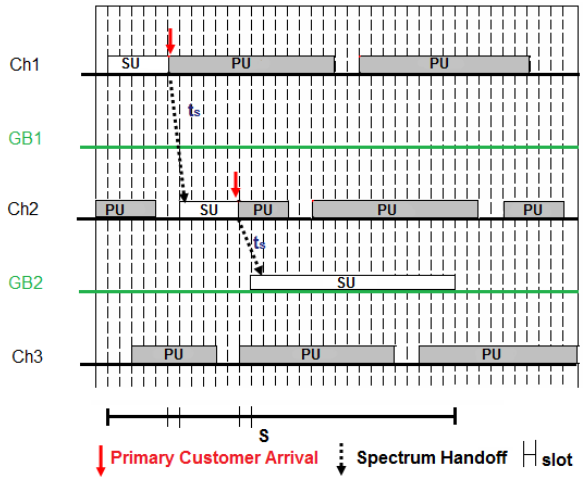


Fig.4 : An example of packet transmission process following HGCS scheme with two interruptions, where ts is the channel switch time.

7. If in the database, the SU finds the guard channel of the channel it last used empty, it will switch to the guard channel and resume its transmission on the guard channel.
8. If the guard channel of the last channel used by SU is unavailable, it will switch to the next available guard channel and resume its transmission on it.
9. While communicating on guard channel, the SU will recheck its database for another idle channel if it is updated.
10. If it finds another idle channel in the updated database, it will switch to it and resume its transmission there.
11. Else it stays on the guard channel to complete its transmission.

The flow chart of the proposed scheme is shown in figure 3. The diagrammatic illustration used in [14] is modified it to the proposed HGCS scheme as shown in figure 4. In this figure, PU and SU stand for primary user and secondary user respectively. The default channel of SU is Ch 1. Finding its default channel Ch1 available; SU starts transmission on Ch1. After 5 time slots, the SU stops transmission and vacates the channel for the PU. The SU looks up its TV channel list and finds Ch2 idle. It switches to Ch2 to resume its transmission. After 5 time slots the SU needs to vacate the channel again for the PU. The SU looks up the TV channel list again for another idle channel. Finding no idle channel even in the list, the SU then checks the guard channel database. It finds the guard channel (GB2) of its last used channel (Ch2) available. The SU switches to GB2 to resume its transmission.

Finally the transmission of SU finishes on GB2. The total service time (denoted by S) is termed as the period from the moment of beginning transmitting packets until the completion of transmission. In this case

the SU needed total 27 time slots to complete its transmission.

b) PRP M/G/1 Queueing Network Model

A preemptive resume priority (PRP) M/G/1 queuing network proposed in [12] [13] is followed with considerable modifications made to the traditional PRP M/G/1 Theory as well as the proposed model in [13].

The guard channel between the channels is utilized for transmission in order to reduce the transmission delay for SU. A HGCS scheme is proposed to reduce the handoff delay, consequently minimizing the Total Service Time (S).

The proposed PRP M/G/1 queuing network is shown in figure 5. The model demonstrates a PRP M/G/1 queuing network having 2 channels, where PUs are placed in high priority queue and SUs are placed in low priority queue. The (bs(x)) indicate the transmission packets. λ_o denotes the arrival rate of PUs and λn denotes the arrival rate of SUs.

When SUs are interrupted by PUs, two cases can arise:

Case 1: After interruption, the SU checks the backup channels and the available TV channels list respectively for another vacant channel, if available; the unfinished transmission is put into the low priority queue of that channel.

Case 2: Else, instead of waiting in queue for a channel to become available, the unfinished transmission is then resumed on the guard channel of the last used channel.

If the guard channel of the last used channel is not available, the SU finds another available guard channel in the guard channel database.

The secondary user will be in 'always-change' state, since it will never have to stay on a channel and wait for it to become available.

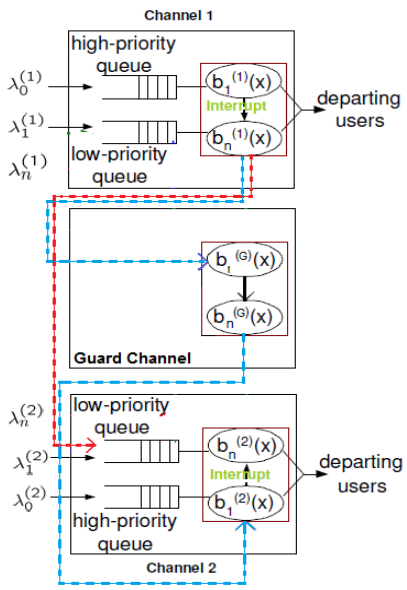


Fig 5 : PRP M/G/1 Queuing Network Model for the proposed scheme

c) Handoff delay and Total Service Time of secondary customers

Let S denote the total service time and E[D] denote the handoff delay. [13] Calculates the total service time as,

$$S = E[X_s] + E[N]E[D] \quad (4)$$

where, E[Xs] = The mean transmission length beginning with the packet transmission or resumption until packet interruption.

E[N] = The average number of interruptions. Calculated by,

$$E[N] = \lambda_o E[X_s] \quad (5)$$

where, λ_o is the arrival rate of PUs with Poisson processes.

E[D] = hand off delay.

For always-stay strategy, [13] calculates,

$$E[D_{stay}] = Y_o \quad (6)$$

For always-change strategy, [13] calculates,

$$E[D_{change}] = W_s + t_s \quad (7)$$

where Ws is the waiting time of SUs and ts is the channel switching time.

Considering both cases, [12] calculates Total Service Time for random proactive decision spectrum handoff as,

$$E[S_{random}] = E[X_s] + \frac{E[N]}{2} Y_o + \frac{E[N]}{2}(W_s + t_s) \quad (8)$$

According to the proposed HGCS method, the SU will always be in always-change case, i.e., either handoff to another vacant channel, or handoff to the guard channel. So, when calculating the total service time (S) for proposed HGCS scheme, the situation concerning the always-change case only will be faced, therefore the new Total Service Time (S) can now be calculated as:

$$S = E[X_s] + \frac{E[N]}{2}(W_s + t_s) \quad (9)$$

V. Numerical and Simulation Results

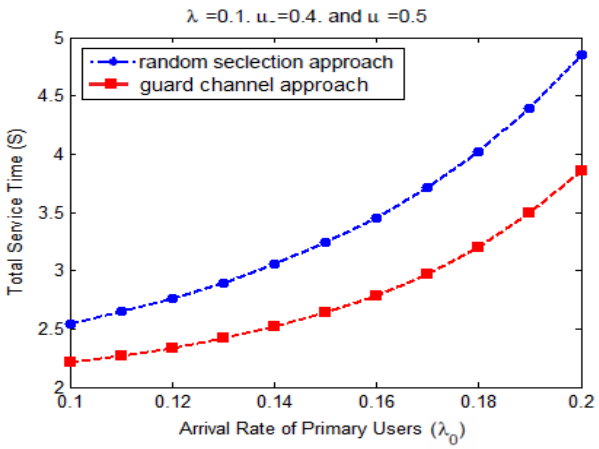


Fig.6 : Comparison of total service time for random and guard channel strategies. The value of ts is assumed to be zero.

a) Simulation Setup

For simulation MATLAB software is used. In order to compare our results with the random proactive decision spectrum handoff, the scenario assumed in [13] is followed. A system with 2 channels is considered. Both channels will entertain PUs and SUs. The arrival rate for both types of users is generated with the Poisson process. SUs can be interrupted by PUs. First_ comefirst-serve scheduling discipline is assumed.

b) Performance Evaluation

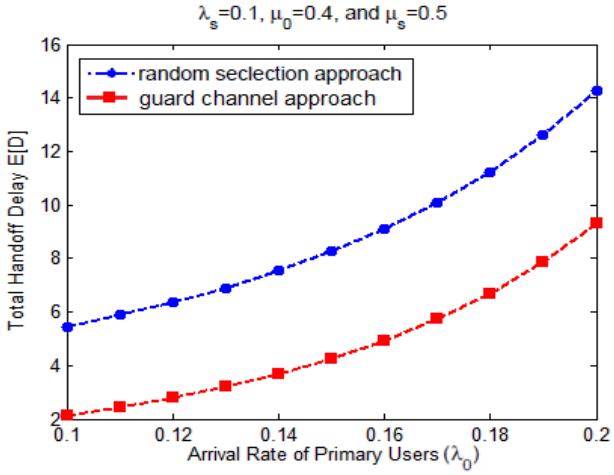


Fig.7 : Comparison of total handoff delay for random and guard channel strategies. The value of ts is assumed to be zero.

Figure 6 compares the total service time using two different handoff schemes: 1) the random proactive decision channel selection strategy and 2) the proposed HGCS strategy. For $\lambda_{\circ} \leq 0.2$, the figure shows that the total service time can be reduced to more than 20% from the random channel selection approach. For larger $\lambda_{\circ}$, it can be anticipated that the proposed HGCS strategy can notably improve total service time.

Figure 7 compares the handoff delay for the two approaches mentioned above. For $\lambda_{\circ} \leq 0.2$, the figure shows that the total handoff delay can be reduced significantly using the propd HGCS approach as compared to the random channel selection approach.

For larger $\lambda_{\circ}$, it is shown in Table1 that the proposed HGCS strategy can considerably minimize the total handoff delay.

Figure 8 shows the effect of μs on the total service time of the HGCS. The SU has exponentially distributed packet length (bs(x)) defined in [13] as,

$$b_s(x) = \mu_s e^{-\mu_s x} \quad (10)$$

where μs is the packet inter arrival time of SU. $\mu_{\circ}$ is the packet inter-arrival time of PU. The figure shows that with greater μs, the total service time is considerably less.

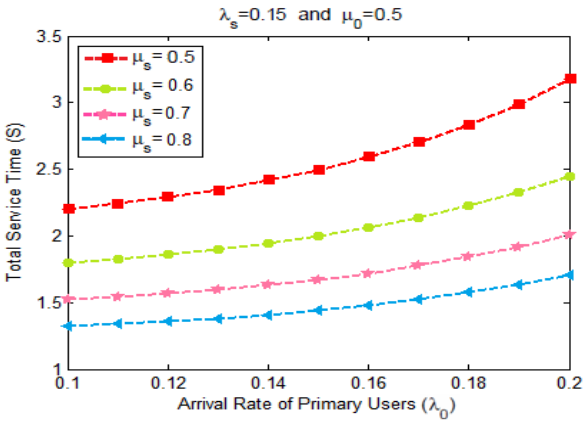


Fig.8 : Effect of μs on the total service time of HGCS. The value of ts is assumed to be 0.

Table 1 compares the values of total service time and delay for different PU arrival rates. With the increase in arrival rate of PU, the service time significantly improves as compared to the random approach from 15 % to 20 % as shown in Table 1. For larger values of $\lambda_{\circ}$, the improvement will be even greater than 20%.

There is a noteworthy improvement in the delay values as well. HGCS shows better results as it eliminates the need of on channel wait as in random proactive approach. Secondly, it eliminates the blocking probability of SU transmission as well, as SU is going to have a channel available for it throughout the transmission. In addition the time needed for finding a new channel for completing the transmission is also minimized, as can be seen in the Table 1.

Table I : Comparison of Random Approach and HGCS Approach

λs= 0.1 , μs = 0.5 and μo = 0.5						
		Random Proactive Approach		HGCS Approach		Improvement in S with HGCS
	$\lambda_{\circ}$	S	E[D]	S	E[D]	% Increase
1.	0.12	2.76	6.35	2.33	2.78	15.5%
2.	0.14	3.05	7.53	2.51	3.68	17.7%
3.	0.16	3.45	9.09	2.78	4.92	19.4%
4.	0.18	4.02	11.22	3.20	6.68	20.3%
5.	0.2	4.85	14.28	3.85	9.28	20.6%

VI. Conclusion

In this paper a HGCS is suggested that makes effective use of the guard channels for communication in CR networks. By using guard channels, a major improvement can be seen in the total service time as HGCS successfully minimizes the handoff delay with an improvement of approximately 20%. HGCS is then compared to the random proactive decision handoff scheme using a preemptive resume priority (PRP) M/G/1

queuing network model to analyze the total service time and handoff delay in each case. Numerical and simulation results show significant improvement from 15% to 20% with the increase in the PU arrival rate for HGCS as it guarantees faster service time for SUs. In future work, HGCS will be tested in the BRS (Business Radio Service) scenario formerly known as MMDS (Multi channel Multipoint Distribution Service).

Refrences Refrences Refrencias

1. S. Haykin, "Cognitive Radio: Brain-Empowered Wireless Communication", IEEE JSAC, Feb 2005.
2. Federal Communications Commission (FCC), "Notice of Proposed Rule Making," ET Docket no. 04-113, May 25, 2004.
3. Federal Communications Commission (FCC), "Notice of Proposed Rule Making," ET Docket no. 06-156, October, 2006.
4. Federal Communications Commission (FCC), "Notice of Proposed Rule Making," ET Docket no. 03-322, December, 2003.
5. Carlos Cordeiro, Kiran Challapali, Dagnachew Birru and Sai Shankar N, "IEEE 802.22: An Introduction to the First Wireless Standard based on Cognitive Radios", Journal of Communications, April 2006.
6. IEEE 802.22 Working Group on Wireless Regional Area Network, http://www.ieee802.org/22/.
7. J. Mitola, "Cognitive radio: Making software radio more personal" IEEE Pers. Comm. 2005, August 1999.
8. E. Hossain , V. Bhargava., "Cognitive Wireless Communication Networks", Springer Science+Business Media, 2007, LLC, ISBN 978-0-387-68830-5, e-ISBN 978-0-387-68832-9.
9. I. F. Akyildiz, W. Y. Lee, M. C. Vuran, and S. Mohanty, "NeXt Generation/Dynamic Spectrum Access/Cognitive Radio Wireless Networks: A Survey," Computer Networks Journal (Elsevier), vol. 50, pp. 2127–2159, September 2006.
10. L-C. Wang and A. Chen, "On the Performance of Spectrum Handoff for Link Maintenance in Cognitive Radio", Wireless Pervasive Computing, 3rd International Symposium, 7 – 9 May 2008.
11. Y. Zhang, "Spectrum Handoff in Cognitive Radio Networks: "Opportunistic and Negotiated Situations", IEEE International Conference on Communications, 2009.
12. L-C. Wang and C-W. Wang, "Spectrum Handoff for Cognitive Radio Networks: Reactive-Sensing or Proactive-Sensing?", IEEE Performance, Computing and Communications Conference, December 2008.
13. C-W. Wang and L-C. Wang, "Modeling and Analysis for Proactive-decision Spectrum Handoff in Cognitive Radio Networks", IEEE International Conference on Communications, June 2009.
14. M. A. Kalil, F. Liers, T. Volkert and A. M- Thie; "A Novel Opportunistic Spectrum Sharing Scheme for Cognitive AdHoc Networks", Journal Springer Verlag, 2009.
15. R.-T. Ma, Y.-P. Hsu, and K.-T. Feng, "A POMDP-based Spectrum Handoff Protocol for Partially Observable Cognitive Radio Networks," IEEE Wireless Communications and Networking Conference (WCNC), April 2009.
16. S.-U. Yoon and E. Ekici, "Voluntary Spectrum Handoff: A Novel Approach to Spectrum Management in CRNs," IEEE International Conference on Communications (ICC), May 2010.
17. Y. Song and J. Xie, "Common Hopping Based Proactive Spectrum Handoff in Cognitive Radio Ad Hoc Networks," IEEE Global Communications Conference (GLOBECOM), Dec. 2010.
18. Federal Communications Commission(FCC), "Notice of Proposed Rule Making," ET Docket No. 04-186, 23 September 2010.
19. Q. Zhao, L. Tong, A. Swami, and Y. Chen, "Decentralized Cognitive MAC for Opportunistic Spectrum Access in Ad Hoc Networks: A POMDP Framework," IEEE Journal on Selected Areas in Communications, vol. 25, no. 3, pp. 589–600, April 2007.
20. Mitsuru Uesugi and Yokosuka, "OFDM Guard Band Communication Apparatus And Method," U.S. Patent 7 012 949 B2, Mar. 14, 2006.
21. Sung-Hyun Hwang, "Fractional BW Usage for WRAN Systems," IEEE P802.22 Wireless RANs, .: IEEE 802.22-06-0117-00-0000, 17 July 2006.
22. Kwang-Cheng Chen, Ramjee Prasad, "Cognitive Radio Networks", John Wiley and Sons, 2009, ISBN 978-0-470—69689-7.
23. Federal Communications Commission(FCC), "Small Entity Compliance Guide," ET Docket No. 04-186, 14 November 2008.
24. Madeeha Aman, Saeed Mahfooz and Waheed Ur Rehman, "Handoff delay in Cogntive Radios – A concept paper on utilization of guard channels IEEE 1st International Conference on Computer Networks and Information Technology (IEEE ICCNIT'11), 11 – 13 July, 2011, pp. 211 – 215, ISBN: 978-1-61284-941-6, ISSN: 2223-6317.

Global Journal of Computer Science and Technology
Volume 11 Issue 20 Version 1.0 December 2011
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Visual Pixel Expansion of Secret Image

By Velmurugan.N, Vijayaraj.A
Saveetha Engineering College, Thandalam

Abstract - Two common drawbacks of the visual cryptography scheme (VCS) are the large pixel expansion of each share image and the small contrast of the recovered secret image. In this paper, we propose a step construction to construct VCSOR and VCSXOR for general access structure by applying (2,2)-VCS recursively, where a participant may receive multiple share images. The proposed step construction generates VCSOR and VCSXOR which have optimal pixel expansion and contrast for each qualified set in the general access structure in most cases. Our scheme applies a technique to simplify the access structure, which can reduce the average pixel expansion (APE) in most cases compared with many of the results in the literature. Finally, we give some experimental results and comparisons to show the effectiveness of the proposed scheme.

Keywords : *Average pixel expansion (APE), VCSOR, VCSXOR, Visual Cryptography Scheme (VCS), Share image, Secret image.*

GJCST Classification : *I.4.6*

Strictly as per the compliance and regulations of:

Visual Pixel Expansion of Secret Image

Velmurugan.N [α], Vijayaraj.A [Ω]

Abstract - Two common drawbacks of the visual cryptography scheme (VCS) are the large pixel expansion of each share image and the small contrast of the recovered secret image. In this paper, we propose a step construction to construct VCSOR and VCSXOR for general access structure by applying (2,2)-VCS recursively, where a participant may receive multiple share images. The proposed step construction generates VCSOR and VCSXOR which have optimal pixel expansion and contrast for each qualified set in the general access structure in most cases. Our scheme applies a technique to simplify the access structure, which can reduce the average pixel expansion (APE) in most cases compared with many of the results in the literature. Finally, we give some experimental results and comparisons to show the effectiveness of the proposed scheme.

Keywords : Average pixel expansion (APE), VCSOR, VCSXOR, Visual Cryptography Scheme (VCS), Share image, Secret image.

I. Overview of the Paper

In this project, there is a secret image which is encrypted into some share images. The secret image is called the original secret image for clarity, and the share images are the encrypted images. When a qualified set of share images are stacked together properly, it gives a visual image which is almost the same as the original secret image or recovered secret image. In the case of black and white images, the original secret image is represented as a pattern of black and white pixels. Each of these pixels is divided into subpixels which themselves are encoded as black and white to produce the share images. The recovered secret image is also a pattern of black and white subpixels which should visually reveal the original secret image if a qualified set of share images is stacked. This paper will focus on the black and white images, where a white pixel is denoted by the number 0 and a black pixel is denoted by the number 1. Using these 0's and 1's the XOR and OR operation takes place to recover the original secret image.In a traditional VCS, each participant takes one share image and all the share images have the same pixel expansion. However, in proposed construction of this paper, each of the participants may take multiple share images with different pixel expansions. So, in the following part, list the pixel expansions of all the share images for each participant. We compute the average pixel expansion (APE) as well, where the APE is defined as the average value of the total pixel expansions of the share images that each participant holds. Quantum key distribution protocol which works on network security by the use of key agreement. Secret Key is used by each user in the network. Each user has unique Secret Key and will be shared by each user to Trusted Center. In Trusted Center we have to generate a Key for network Security with the Help of Algorithms and Quantum Mechanics. Through that we have to prove how secure the data has been transmitted over network to receiver.

Author α : Assistant Professor, Department of MCA, Saveetha Engineering College, Thandalam, Chennai-602 105.
E-mail : velmurugann@yahoo.com
Author Ω : Associate Professor, Department of IT, Saveetha Engineering College, Thandalam,Chennai-602 105.
E-mail : satturvijay@yahoo.com

II. Existing System

In 2008 an algorithm for visual cryptography has been developed by Chetana Hegde, Manu S, P Deepa Shenoy, Venugopal K R, and L. M. Patnaik for Banking Applications. The aim of the algorithm was to design an efficient technique for checking authenticity of the customer in corebanking and internet banking applications. In 2008 Avishek Adhikari and Bimal Roy have proposed On some Constructions of Monochrome Visual Cryptographic Schemes, which is a (2, n) visual cryptographic scheme.Data hiding in halftone images using conjugate ordered dithering (DHCOD) algorithm is an existing algorithm which is used for visual cryptography scheme. In this algorithm let X is the cover image and H is the image to be hidden i.e. secret image.

1. Add some noise to the secret image i.e. H. Let us call it as H1.It introduces some stochastic factors between the original multi-tone images and final share. This step is very important to break the direct correlation between multi-tone and share images.
2. Convert the noisy secret image i.e. H1 into binary image. Let us call it as H2.
3. Generate the first share X1: X1 will be nothing but a dithered halftone image generated by the cover image X. We can use dithering technique to generate the halftone image.The error diffusion technique spreads the quantized error in neighboring pixels which can affect in halftoning of that pixel and we might get wrong value for e.g. a pixel which should be a black one can turn to a white pixel. While in ordered dithering we deals with individual pixels and it is takes less computation to generate the halftone image. Since this work is completely based on pixel by pixel manner so it is better to use ordered dithering with respect to error diffusion. We have also made a small change in the

revealing operation of DHCOD algorithm which shows a dramatically good result in the revealed image. If we change the revealing operation from "AND" to "XOR" then we get a very clear secret image without any cover image. But we cannot use this for visual cryptography since we are performing XOR operation and it does not work for stacking of shares. But it may be very useful in copyright protection and other cryptographic scheme.

Merits and Demerits of this Scheme

Proposed scheme provides a high-level security. First phase i.e. visual cryptographic encryption adds the advantages and security of basic schemes. Then phase two adds the advantage and security DHCOD algorithm. Here we get the shares with some information as some image can be shown in the shares with respect to completely black and white pixels in basic scheme. Since it provides better security so it is most useful in transmission of financial documents. More applications can also be developed which require a high level security. As we know no scheme can be perfect in all aspects. This scheme also has drawbacks as the quality of the revealed image is not rich. Since it uses second phase takes the input as the result of first phase i.e. visual cryptographic encryption so definitely it will have the low contrast and high pixel expansion.

III. Proposed System

To overcome the drawbacks of visual cryptography schemes we propose a step construction to construct VCS_{OR} and VCS_{XOR} for general access structure by applying (2,2)-VCS recursively, where a participant may receive multiple share images. The proposed step construction generates VCS_{OR} and VCS_{XOR} which have optimal pixel expansion and contrast for each qualified set in the general access structure in most cases. Our scheme applies a technique to simplify the access structure, which can reduce the average pixel expansion (APE) in most cases compared with many of the results in the literature. Finally, we give some experimental results and comparisons to show the effectiveness of the proposed scheme.

In a traditional VCS, each participant takes one share image and all the share images have the same pixel expansion. However, in proposed construction of this paper, each of the participants may take multiple share images with different pixel expansions. So, in the following part, list the pixel expansions of all the share images for each participant. We compute the average pixel expansion (APE) as well, where the APE is defined as the average value of the total pixel expansions of the share images that each participant holds.Particularly, for a set of participants A, we define the pixel expansion of A as the largest pixel expansion of the share images of A. If A is a qualified set, then define the contrast of A as the contrast of the recovered secret image after adjusting stacking.The participants may have multiple share images, and different qualified sets of share images may result in different contrasts. So, in this paper will focus pixel expansion as well as contrast of the secret image.

Data Flow Diagram

A data flow diagram (DFD) is a graphical representation of the "flow" of data through an information system. A data flow diagram can also be used for the visualization of data processing (structured design). It is common practice for a designer to draw a context-level DFD first which shows the interaction between the system and outside entities. This context-level DFD is then "exploded" to show more detail of the system being modelled.

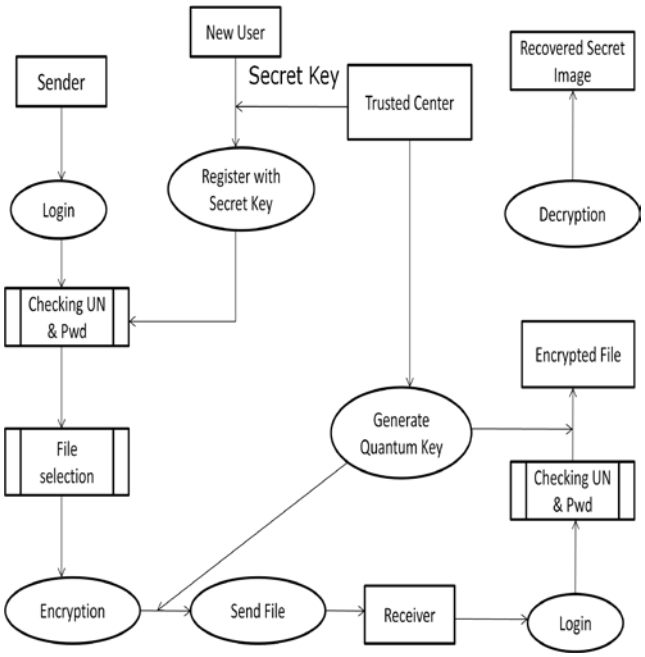


Fig : Data Flow Diagram

IV. Module Description

This includes three basic modules. They are

- Sender
- Trusted Center
- Receiver

SENDER

Getting Authorization is the first stage in sending phase. If a user wants to send a text to Destination user, he wants unique Identification. By using that Identification System knows that the person is an authorized person. This phase or Sender Module has Sub Modules. They are as:

- Registration

- Login
- Send Data

Registration is the Initial state for getting Authentication. By Providing username and Password user sets their Authentication. And System provides one more credentials that is Secret key which is generated by the system for each user. By using username, Password and Secret key system will identify the Authorized person. These credentials are provided to user for the login purpose. These values are stored in the Database. The Database access will be through the registration form in the project. A user wants to send a file means, he/she must log in by using his/her authentication credentials. In this module we have to give username, password and Secret key which was generated by the system.If the user does not provide proper information or the given information is mismatched with database then our system shows Exception message immediately.If the user's details are verified and matched with the existing database then our system allows the person to transmit the file.

TRUSTED CENTER

This module provides the path for the data transfer from the sender to the receiver. This will also generates and verifies the generated key simultaneously.

Verify the secret key received from the user and authenticate the corresponding user for secure transmission. It is shared secret key which is used to for encryption and decryption. The size of session key is 8 bits. This session key is generated from pseudo random prime number and exponential value of random number.

RECEIVER

Getting Authorization is the first stage in receive phase. If a user wants to receive a text from source user, he wants unique Identification. By using that Identification System knows that the person is an authorized person. Verifying the credentials provided, it will allow the user to receive the data. The data given are stored in the database. Similarly there will be secret key generation. In the receiver there will be decryption module. This phase or Receiver Module has Sub Modules. They are as:

1. Registration
2. Login
3. Receive Data

Registration is the Initial state for getting Authentication. By Providing username and Password user sets their Authentication. System provides one more credentials that is Secret key which is generated by the system for each user. By using username, Password and Secret key system will identify the Authorized person. These values are stored in the Database. A user wants to send a file means, he/she must log in by using his/her authentication credentials. In this module we have to give username, password and Secret key which was generated by the system.If the user does not provide proper information or the given information is mismatched with database then our system shows Exception message immediately.After login the TCP program calls i.e. our Trusted Center program starts listen the client or sender. Through Login we send the sender's secret key for Identification. If the given credentials provided matches the data in the database then it allows the transaction. If improper it declines the transaction and identifies that it is an unauthorized user. Here, the receiver waits for the sender request to send the data.

The main aim of this module is to decrypt a file. Decryption will happen only if the system gets a key from Trusted Center (TC). So after verification of user identification system will send the current user's name and his/her secret key to Trusted Center (TC).

V. Implementation

Implementation is the most crucial stage in achieving a successful system and giving the user's confidence that the new system is workable and effective. Implementation of a modified application to replace an existing one. This type of conversation is relatively easy to handle, provide there are no major changes in the system. Each program is tested individually at the time of development using the data and has verified that this program linked together in the way specified in the programs specification, the computer system and its environment is tested to the satisfaction of the user. The system that has been developed is accepted and proved to be satisfactory for the user. And so the system is going to be implemented very soon. A simple operating procedure is included so that the user can understand the different functions clearly and quickly.

MAINTENANCE

The software will definitely undergo change once it is deliver to the customer. There can be many reasons for this change to occur. Change could happen because of some unexpected input values into the system. In addition, the changes in the system could directly affect the software operation. The software should be developed to accommodate changes that could happen during the post implementation period.

VI. Conclusion

In this paper, the step construction of VCS for general access structure which improves the pixel expansion and contrast properties compared with many of the known results in the literature. According to the step construction proposed in this paper, the VCS with general access structure can be constructed by only applying (2, 2)-VCS recursively, regardless of whether the underlying operation is OR or XOR, where a participant may receive multiple share images. This result is most interesting, because the construction of

XOR for general access structure has never been claimed to be possible before. Using Cryptography scheme, image is transferred in a secure mode through the trusted center. Simultaneously, the quantum key is generated in the trusted center and it is distributed to the sender and the receiver. By, this authentication the third party cannot interfere in the middle during the data transfer. The proposed construction can generate optimal OR and XOR for each qualified set and our schemes can also reduce the APE in the most cases compared with the known results in the literature.

References References Referencias

1. M. Naor and A. Shamir, "Visual Cryptography," in EUROCRYPT'94, Berlin, 1995, vol LNCS 950, pp. 1-12, Springer-Verlag.
2. E. Bihman and A. Itzkovitz, "Visual Cryptography with polarization," in RUMP Session of CRYPTO'98, 1997.
3. S. Droste, "New results on visual cryptography," in CRYPTO'96, 1996, vol. 1109, pp. 401-415,Springer-VerlagLNCS.
4. C. Blundo, A. De Santis, and D. R. Stinson, "On the Contrast in visual cryptography schemes," J. Crypotology, vol. 12, no. 4, pp. 261-289, 1999.
5. C. N. Yang, "New visual secret sharing schemes using probabilistic method," Pattern Recognit. Lett., vol. 25, pp. 481-494, 2004.
6. S. Cimato, R. De Prisco, and A. De Santis, "Probablistic visual cryptography schemes," Computer J., vol. 49, No. 1, pp. 97-107, 2006.
7. X. M. Chen, "On the simplification of the acces: structure secret sharing schemes(in Chinese), "China Sci. Bulletin, vol. 15, pp. 1599-1603,1999.
8. C. N. Yang and T. S. Chen, "Size –adjustable visual secret sharing schemes," in ASIA CRYPT'2002, 2002, vol. 2501, pp. 328-345, Springer-VerlagLNCS.

Global Journals Inc. (US) Guidelines Handbook 2011

www.GlobalJournals.org

FELLOW OF ASSOCIATION OF RESEARCH SOCIETY IN COMPUTING (FARSC)

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

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

MEMBER OF ASSOCIATION OF RESEARCH SOCIETY IN COMPUTING (MARSC)

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

AUXILIARY MEMBERSHIPS

ANNUAL MEMBER

- Annual Member will be authorized to receive e-Journal GJMBR for one year (subscription for one year).
- The member will be allotted free 1 GB Web-space along with subDomain to contribute and participate in our activities.
- A professional email address will be allotted free 500 MB email space.

PAPER PUBLICATION

- The members can publish paper once. The paper will be sent to two-peer reviewer. The paper will be published after the acceptance of peer reviewers and Editorial Board.

Process of submission of Research Paper

The Area or field of specialization may or may not be of any category as mentioned in 'Scope of Journal' menu of the GlobalJournals.org website. There are 37 Research Journal categorized with Six parental Journals GJCST, GJMR, GJRE, GJMBR, GJSFR, GJHSS. For Authors should prefer the mentioned categories. There are three widely used systems UDC, DDC and LCC. The details are available as 'Knowledge Abstract' at Home page. The major advantage of this coding is that, the research work will be exposed to and shared with all over the world as we are being abstracted and indexed worldwide.

The paper should be in proper format. The format can be downloaded from first page of 'Author Guideline' Menu. The Author is expected to follow the general rules as mentioned in this menu. The paper should be written in MS-Word Format (*.DOC,*.DOCX).

The Author can submit the paper either online or offline. The authors should prefer online submission.Online Submission: There are three ways to submit your paper:

(A) (I) First, register yourself using top right corner of Home page then Login. If you are already registered, then login using your username and password.

(II) Choose corresponding Journal.

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

(B) If you are using Internet Explorer, then Direct Submission through Homepage is also available.

(C) If these two are not convenient, and then email the paper directly to dean@globaljournals.org.

Offline Submission: Author can send the typed form of paper by Post. However, online submission should be preferred.

Preferred Author Guidelines

MANUSCRIPT STYLE INSTRUCTION (Must be strictly followed)

Page Size: 8.27" X 11'"

- Left Margin: 0.65
- Right Margin: 0.65
- Top Margin: 0.75
- Bottom Margin: 0.75
- Font type of all text should be Swis 721 Lt BT.
- Paper Title should be of Font Size 24 with one Column section.
- Author Name in Font Size of 11 with one column as of Title.
- Abstract Font size of 9 Bold, "Abstract" word in Italic Bold.
- Main Text: Font size 10 with justified two columns section
- Two Column with Equal Column with of 3.38 and Gaping of .2
- First Character must be three lines Drop capped.
- Paragraph before Spacing of 1 pt and After of 0 pt.
- Line Spacing of 1 pt
- Large Images must be in One Column
- Numbering of First Main Headings (Heading 1) must be in Roman Letters, Capital Letter, and Font Size of 10.
- Numbering of Second Main Headings (Heading 2) must be in Alphabets, Italic, and Font Size of 10.

You can use your own standard format also.
Author Guidelines:

1. General,

2. Ethical Guidelines,

3. Submission of Manuscripts,

4. Manuscript's Category,

5. Structure and Format of Manuscript,

6. After Acceptance.

1. GENERAL

Before submitting your research paper, one is advised to go through the details as mentioned in following heads. It will be beneficial, while peer reviewer justify your paper for publication.

Scope

The Global Journals Inc. (US) welcome the submission of original paper, review paper, survey article relevant to the all the streams of Philosophy and knowledge. The Global Journals Inc. (US) is parental platform for Global Journal of Computer Science and Technology, Researches in Engineering, Medical Research, Science Frontier Research, Human Social Science, Management, and Business organization. The choice of specific field can be done otherwise as following in Abstracting and Indexing Page on this Website. As the all Global

Journals Inc. (US) are being abstracted and indexed (in process) by most of the reputed organizations. Topics of only narrow interest will not be accepted unless they have wider potential or consequences.

2. ETHICAL GUIDELINES

Authors should follow the ethical guidelines as mentioned below for publication of research paper and research activities.

Papers are accepted on strict understanding that the material in whole or in part has not been, nor is being, considered for publication elsewhere. If the paper once accepted by Global Journals Inc. (US) and Editorial Board, will become the copyright of the Global Journals Inc. (US).

Authorship: The authors and coauthors should have active contribution to conception design, analysis and interpretation of findings. They should critically review the contents and drafting of the paper. All should approve the final version of the paper before submission

The Global Journals Inc. (US) follows the definition of authorship set up by the Global Academy of Research and Development. According to the Global Academy of R&D authorship, criteria must be based on:

1) Substantial contributions to conception and acquisition of data, analysis and interpretation of the findings.

2) Drafting the paper and revising it critically regarding important academic content.

3) Final approval of the version of the paper to be published.

All authors should have been credited according to their appropriate contribution in research activity and preparing paper. Contributors who do not match the criteria as authors may be mentioned under Acknowledgement.

Acknowledgements: Contributors to the research other than authors credited should be mentioned under acknowledgement. The specifications of the source of funding for the research if appropriate can be included. Suppliers of resources may be mentioned along with address.

Appeal of Decision: The Editorial Board's decision on publication of the paper is final and cannot be appealed elsewhere.

Permissions: It is the author's responsibility to have prior permission if all or parts of earlier published illustrations are used in this paper.

Please mention proper reference and appropriate acknowledgements wherever expected.

If all or parts of previously published illustrations are used, permission must be taken from the copyright holder concerned. It is the author's responsibility to take these in writing.

Approval for reproduction/modification of any information (including figures and tables) published elsewhere must be obtained by the authors/copyright holders before submission of the manuscript. Contributors (Authors) are responsible for any copyright fee involved.

3. SUBMISSION OF MANUSCRIPTS

Manuscripts should be uploaded via this online submission page. The online submission is most efficient method for submission of papers, as it enables rapid distribution of manuscripts and consequently speeds up the review procedure. It also enables authors to know the status of their own manuscripts by emailing us. Complete instructions for submitting a paper is available below.

Manuscript submission is a systematic procedure and little preparation is required beyond having all parts of your manuscript in a given format and a computer with an Internet connection and a Web browser. Full help and instructions are provided on-screen. As an author, you will be prompted for login and manuscript details as Field of Paper and then to upload your manuscript file(s) according to the instructions.

To avoid postal delays, all transaction is preferred by e-mail. A finished manuscript submission is confirmed by e-mail immediately and your paper enters the editorial process with no postal delays. When a conclusion is made about the publication of your paper by our Editorial Board, revisions can be submitted online with the same procedure, with an occasion to view and respond to all comments.

Complete support for both authors and co-author is provided.

4. MANUSCRIPT'S CATEGORY

Based on potential and nature, the manuscript can be categorized under the following heads:

Original research paper: Such papers are reports of high-level significant original research work.

Review papers: These are concise, significant but helpful and decisive topics for young researchers.

Research articles: These are handled with small investigation and applications

Research letters: The letters are small and concise comments on previously published matters.

5.STRUCTURE AND FORMAT OF MANUSCRIPT

The recommended size of original research paper is less than seven thousand words, review papers fewer than seven thousands words also.Preparation of research paper or how to write research paper, are major hurdle, while writing manuscript. The research articles and research letters should be fewer than three thousand words, the structure original research paper; sometime review paper should be as follows:

Papers: These are reports of significant research (typically less than 7000 words equivalent, including tables, figures, references), and comprise:

(a)Title should be relevant and commensurate with the theme of the paper.

(b) A brief Summary, "Abstract" (less than 150 words) containing the major results and conclusions.

(c) Up to ten keywords, that precisely identifies the paper's subject, purpose, and focus.

(d) An Introduction, giving necessary background excluding subheadings; objectives must be clearly declared.

(e) Resources and techniques with sufficient complete experimental details (wherever possible by reference) to permit repetition; sources of information must be given and numerical methods must be specified by reference, unless non-standard.

(f) Results should be presented concisely, by well-designed tables and/or figures; the same data may not be used in both; suitable statistical data should be given. All data must be obtained with attention to numerical detail in the planning stage. As reproduced design has been recognized to be important to experiments for a considerable time, the Editor has decided that any paper that appears not to have adequate numerical treatments of the data will be returned un-refereed;

(g) Discussion should cover the implications and consequences, not just recapitulating the results; conclusions should be summarizing.

(h) Brief Acknowledgements.

(i) References in the proper form.

Authors should very cautiously consider the preparation of papers to ensure that they communicate efficiently. Papers are much more likely to be accepted, if they are cautiously designed and laid out, contain few or no errors, are summarizing, and be conventional to the approach and instructions. They will in addition, be published with much less delays than those that require much technical and editorial correction.

The Editorial Board reserves the right to make literary corrections and to make suggestions to improve briefness.

It is vital, that authors take care in submitting a manuscript that is written in simple language and adheres to published guidelines.

Format

Language: The language of publication is UK English. Authors, for whom English is a second language, must have their manuscript efficiently edited by an English-speaking person before submission to make sure that, the English is of high excellence. It is preferable, that manuscripts should be professionally edited.

Standard Usage, Abbreviations, and Units: Spelling and hyphenation should be conventional to The Concise Oxford English Dictionary. Statistics and measurements should at all times be given in figures, e.g. 16 min, except for when the number begins a sentence. When the number does not refer to a unit of measurement it should be spelt in full unless, it is 160 or greater.

Abbreviations supposed to be used carefully. The abbreviated name or expression is supposed to be cited in full at first usage, followed by the conventional abbreviation in parentheses.

Metric SI units are supposed to generally be used excluding where they conflict with current practice or are confusing. For illustration, 1.4 l rather than 1.4 × 10-3 m3, or 4 mm somewhat than 4 × 10-3 m. Chemical formula and solutions must identify the form used, e.g. anhydrous or hydrated, and the concentration must be in clearly defined units. Common species names should be followed by underlines at the first mention. For following use the generic name should be constricted to a single letter, if it is clear.

Structure

All manuscripts submitted to Global Journals Inc. (US), ought to include:

Title: The title page must carry an instructive title that reflects the content, a running title (less than 45 characters together with spaces), names of the authors and co-authors, and the place(s) wherever the work was carried out. The full postal address in addition with the e-mail address of related author must be given. Up to eleven keywords or very brief phrases have to be given to help data retrieval, mining and indexing.

Abstract, used in Original Papers and Reviews:

Optimizing Abstract for Search Engines

Many researchers searching for information online will use search engines such as Google, Yahoo or similar. By optimizing your paper for search engines, you will amplify the chance of someone finding it. This in turn will make it more likely to be viewed and/or cited in a further work. Global Journals Inc. (US) have compiled these guidelines to facilitate you to maximize the web-friendliness of the most public part of your paper.

Key Words

A major linchpin in research work for the writing research paper is the keyword search, which one will employ to find both library and Internet resources.

One must be persistent and creative in using keywords. An effective keyword search requires a strategy and planning a list of possible keywords and phrases to try.

Search engines for most searches, use Boolean searching, which is somewhat different from Internet searches. The Boolean search uses "operators," words (and, or, not, and near) that enable you to expand or narrow your affords. Tips for research paper while preparing research paper are very helpful guideline of research paper.

Choice of key words is first tool of tips to write research paper. Research paper writing is an art.A few tips for deciding as strategically as possible about keyword search:

- One should start brainstorming lists of possible keywords before even begin searching. Think about the most important concepts related to research work. Ask, "What words would a source have to include to be truly valuable in research paper?" Then consider synonyms for the important words.
- It may take the discovery of only one relevant paper to let steer in the right keyword direction because in most databases, the keywords under which a research paper is abstracted are listed with the paper.
- One should avoid outdated words.

Keywords are the key that opens a door to research work sources. Keyword searching is an art in which researcher's skills are bound to improve with experience and time.

Numerical Methods: Numerical methods used should be clear and, where appropriate, supported by references.

Acknowledgements: Please make these as concise as possible.

References

References follow the Harvard scheme of referencing. References in the text should cite the authors' names followed by the time of their publication, unless there are three or more authors when simply the first author's name is quoted followed by et al. unpublished work has to only be cited where necessary, and only in the text. Copies of references in press in other journals have to be supplied with submitted typescripts. It is necessary that all citations and references be carefully checked before submission, as mistakes or omissions will cause delays.

References to information on the World Wide Web can be given, but only if the information is available without charge to readers on an official site. Wikipedia and Similar websites are not allowed where anyone can change the information. Authors will be asked to make available electronic copies of the cited information for inclusion on the Global Journals Inc. (US) homepage at the judgment of the Editorial Board.

The Editorial Board and Global Journals Inc. (US) recommend that, citation of online-published papers and other material should be done via a DOI (digital object identifier). If an author cites anything, which does not have a DOI, they run the risk of the cited material not being noticeable.

The Editorial Board and Global Journals Inc. (US) recommend the use of a tool such as Reference Manager for reference management and formatting.

Tables, Figures and Figure Legends

Tables: Tables should be few in number, cautiously designed, uncrowned, and include only essential data. Each must have an Arabic number, e.g. Table 4, a self-explanatory caption and be on a separate sheet. Vertical lines should not be used.

Figures: Figures are supposed to be submitted as separate files. Always take in a citation in the text for each figure using Arabic numbers, e.g. Fig. 4. Artwork must be submitted online in electronic form by e-mailing them.

Preparation of Electronic Figures for Publication

Even though low quality images are sufficient for review purposes, print publication requires high quality images to prevent the final product being blurred or fuzzy. Submit (or e-mail) EPS (line art) or TIFF (halftone/photographs) files only. MS PowerPoint and Word Graphics are unsuitable for printed pictures. Do not use pixel-oriented software. Scans (TIFF only) should have a resolution of at least 350 dpi (halftone) or 700 to 1100 dpi (line drawings) in relation to the imitation size. Please give the data for figures in black and white or submit a Color Work Agreement Form. EPS files must be saved with fonts embedded (and with a TIFF preview, if possible).

For scanned images, the scanning resolution (at final image size) ought to be as follows to ensure good reproduction: line art: >650 dpi; halftones (including gel photographs) : >350 dpi; figures containing both halftone and line images: >650 dpi.

Color Charges: It is the rule of the Global Journals Inc. (US) for authors to pay the full cost for the reproduction of their color artwork. Hence, please note that, if there is color artwork in your manuscript when it is accepted for publication, we would require you to complete and return a color work agreement form before your paper can be published.

Figure Legends: Self-explanatory legends of all figures should be incorporated separately under the heading 'Legends to Figures'. In the full-text online edition of the journal, figure legends may possibly be truncated in abbreviated links to the full screen version. Therefore, the first 100 characters of any legend should notify the reader, about the key aspects of the figure.

6. AFTER ACCEPTANCE

Upon approval of a paper for publication, the manuscript will be forwarded to the dean, who is responsible for the publication of the Global Journals Inc. (US).

6.1 Proof Corrections

The corresponding author will receive an e-mail alert containing a link to a website or will be attached. A working e-mail address must therefore be provided for the related author.

Acrobat Reader will be required in order to read this file. This software can be downloaded

(Free of charge) from the following website:

www.adobe.com/products/acrobat/readstep2.html. This will facilitate the file to be opened, read on screen, and printed out in order for any corrections to be added. Further instructions will be sent with the proof.

Proofs must be returned to the dean at dean@globaljournals.org within three days of receipt.

As changes to proofs are costly, we inquire that you only correct typesetting errors. All illustrations are retained by the publisher. Please note that the authors are responsible for all statements made in their work, including changes made by the copy editor.

6.2 Early View of Global Journals Inc. (US) (Publication Prior to Print)

The Global Journals Inc. (US) are enclosed by our publishing's Early View service. Early View articles are complete full-text articles sent in advance of their publication. Early View articles are absolute and final. They have been completely reviewed, revised and edited for publication, and the authors' final corrections have been incorporated. Because they are in final form, no changes can be made after sending them. The nature of Early View articles means that they do not yet have volume, issue or page numbers, so Early View articles cannot be cited in the conventional way.

6.3 Author Services

Online production tracking is available for your article through Author Services. Author Services enables authors to track their article - once it has been accepted - through the production process to publication online and in print. Authors can check the status of their articles online and choose to receive automated e-mails at key stages of production. The authors will receive an e-mail with a unique link that enables them to register and have their article automatically added to the system. Please ensure that a complete e-mail address is provided when submitting the manuscript.

6.4 Author Material Archive Policy

Please note that if not specifically requested, publisher will dispose off hardcopy & electronic information submitted, after the two months of publication. If you require the return of any information submitted, please inform the Editorial Board or dean as soon as possible.

6.5 Offprint and Extra Copies

A PDF offprint of the online-published article will be provided free of charge to the related author, and may be distributed according to the Publisher's terms and conditions. Additional paper offprint may be ordered by emailing us at: editor@globaljournals.org .

the search? Will I be able to find all information in this field area? If the answer of these types of questions will be "Yes" then you can choose that topic. In most of the cases, you may have to conduct the surveys and have to visit several places because this field is related to Computer Science and Information Technology. Also, you may have to do a lot of work to find all rise and falls regarding the various data of that subject. Sometimes, detailed information plays a vital role, instead of short information.

2. Evaluators are human: First thing to remember that evaluators are also human being. They are not only meant for rejecting a paper. They are here to evaluate your paper. So, present your Best.

3. Think Like Evaluators: If you are in a confusion or getting demotivated that your paper will be accepted by evaluators or not, then think and try to evaluate your paper like an Evaluator. Try to understand that what an evaluator wants in your research paper and automatically you will have your answer.

4. Make blueprints of paper: The outline is the plan or framework that will help you to arrange your thoughts. It will make your paper logical. But remember that all points of your outline must be related to the topic you have chosen.

5. Ask your Guides: If you are having any difficulty in your research, then do not hesitate to share your difficulty to your guide (if you have any). They will surely help you out and resolve your doubts. If you can't clarify what exactly you require for your work then ask the supervisor to help you with the alternative. He might also provide you the list of essential readings.

6. Use of computer is recommended: As you are doing research in the field of Computer Science, then this point is quite obvious.

7. Use right software: Always use good quality software packages. If you are not capable to judge good software then you can lose quality of your paper unknowingly. There are various software programs available to help you, which you can get through Internet.

8. Use the Internet for help: An excellent start for your paper can be by using the Google. It is an excellent search engine, where you can have your doubts resolved. You may also read some answers for the frequent question how to write my research paper or find model research paper. From the internet library you can download books. If you have all required books make important reading selecting and analyzing the specified information. Then put together research paper sketch out.

9. Use and get big pictures: Always use encyclopedias, Wikipedia to get pictures so that you can go into the depth.

10. Bookmarks are useful: When you read any book or magazine, you generally use bookmarks, right! It is a good habit, which helps to not to lose your continuity. You should always use bookmarks while searching on Internet also, which will make your search easier.

11. Revise what you wrote: When you write anything, always read it, summarize it and then finalize it.

12. Make all efforts: Make all efforts to mention what you are going to write in your paper. That means always have a good start. Try to mention everything in introduction, that what is the need of a particular research paper. Polish your work by good skill of writing and always give an evaluator, what he wants.

13. Have backups: When you are going to do any important thing like making research paper, you should always have backup copies of it either in your computer or in paper. This will help you to not to lose any of your important.

14. Produce good diagrams of your own: Always try to include good charts or diagrams in your paper to improve quality. Using several and unnecessary diagrams will degrade the quality of your paper by creating "hotchpotch." So always, try to make and include those diagrams, which are made by your own to improve readability and understandability of your paper.

15. Use of direct quotes: When you do research relevant to literature, history or current affairs then use of quotes become essential but if study is relevant to science then use of quotes is not preferable.

16. Use proper verb tense: Use proper verb tenses in your paper. Use past tense, to present those events that happened. Use present tense to indicate events that are going on. Use future tense to indicate future happening events. Use of improper and wrong tenses will confuse the evaluator. Avoid the sentences that are incomplete.

17. Never use online paper: If you are getting any paper on Internet, then never use it as your research paper because it might be possible that evaluator has already seen it or maybe it is outdated version.

18. **Pick a good study spot:** To do your research studies always try to pick a spot, which is quiet. Every spot is not for studies. Spot that suits you choose it and proceed further.

19. Know what you know: Always try to know, what you know by making objectives. Else, you will be confused and cannot achieve your target.

20. Use good quality grammar: Always use a good quality grammar and use words that will throw positive impact on evaluator. Use of good quality grammar does not mean to use tough words, that for each word the evaluator has to go through dictionary. Do not start sentence with a conjunction. Do not fragment sentences. Eliminate one-word sentences. Ignore passive voice. Do not ever use a big word when a diminutive one would suffice. Verbs have to be in agreement with their subjects. Prepositions are not expressions to finish sentences with. It is incorrect to ever divide an infinitive. Avoid clichés like the disease. Also, always shun irritating alliteration. Use language that is simple and straight forward. put together a neat summary.

21. Arrangement of information: Each section of the main body should start with an opening sentence and there should be a changeover at the end of the section. Give only valid and powerful arguments to your topic. You may also maintain your arguments with records.

22. Never start in last minute: Always start at right time and give enough time to research work. Leaving everything to the last minute will degrade your paper and spoil your work.

23. Multitasking in research is not good: Doing several things at the same time proves bad habit in case of research activity. Research is an area, where everything has a particular time slot. Divide your research work in parts and do particular part in particular time slot.

24. Never copy others' work: Never copy others' work and give it your name because if evaluator has seen it anywhere you will be in trouble.

25. Take proper rest and food: No matter how many hours you spend for your research activity, if you are not taking care of your health then all your efforts will be in vain. For a quality research, study is must, and this can be done by taking proper rest and food.

26. Go for seminars: Attend seminars if the topic is relevant to your research area. Utilize all your resources.

27. Refresh your mind after intervals: Try to give rest to your mind by listening to soft music or by sleeping in intervals. This will also improve your memory.

28. Make colleagues: Always try to make colleagues. No matter how sharper or intelligent you are, if you make colleagues you can have several ideas, which will be helpful for your research.

29. **Think technically:** Always think technically. If anything happens, then search its reasons, its benefits, and demerits.

30. Think and then print: When you will go to print your paper, notice that tables are not be split, headings are not detached from their descriptions, and page sequence is maintained.

31. Adding unnecessary information: Do not add unnecessary information, like, I have used MS Excel to draw graph. Do not add irrelevant and inappropriate material. These all will create superfluous. Foreign terminology and phrases are not apropos. One should NEVER take a broad view. Analogy in script is like feathers on a snake. Not at all use a large word when a very small one would be

sufficient. Use words properly, regardless of how others use them. Remove quotations. Puns are for kids, not grunt readers. Amplification is a billion times of inferior quality than sarcasm.

32. Never oversimplify everything: To add material in your research paper, never go for oversimplification. This will definitely irritate the evaluator. Be more or less specific. Also too, by no means, ever use rhythmic redundancies. Contractions aren't essential and shouldn't be there used. Comparisons are as terrible as clichés. Give up ampersands and abbreviations, and so on. Remove commas, that are, not necessary. Parenthetical words however should be together with this in commas. Understatement is all the time the complete best way to put onward earth-shaking thoughts. Give a detailed literary review.

33. Report concluded results: Use concluded results. From raw data, filter the results and then conclude your studies based on measurements and observations taken. Significant figures and appropriate number of decimal places should be used. Parenthetical remarks are prohibitive. Proofread carefully at final stage. In the end give outline to your arguments. Spot out perspectives of further study of this subject. Justify your conclusion by at the bottom of them with sufficient justifications and examples.

34. After conclusion: Once you have concluded your research, the next most important step is to present your findings. Presentation is extremely important as it is the definite medium though which your research is going to be in print to the rest of the crowd. Care should be taken to categorize your thoughts well and present them in a logical and neat manner. A good quality research paper format is essential because it serves to highlight your research paper and bring to light all necessary aspects in your research.

Informal Guidelines of Research Paper Writing

Key points to remember:

- Submit all work in its final form.
- Write your paper in the form, which is presented in the guidelines using the template.
- Please note the criterion for grading the final paper by peer-reviewers.

Final Points:

A purpose of organizing a research paper is to let people to interpret your effort selectively. The journal requires the following sections, submitted in the order listed, each section to start on a new page.

The introduction will be compiled from reference matter and will reflect the design processes or outline of basis that direct you to make study. As you will carry out the process of study, the method and process section will be constructed as like that. The result segment will show related statistics in nearly sequential order and will direct the reviewers next to the similar intellectual paths throughout the data that you took to carry out your study. The discussion section will provide understanding of the data and projections as to the implication of the results. The use of good quality references all through the paper will give the effort trustworthiness by representing an alertness of prior workings.

Writing a research paper is not an easy job no matter how trouble-free the actual research or concept. Practice, excellent preparation, and controlled record keeping are the only means to make straightforward the progression.

General style:

Specific editorial column necessities for compliance of a manuscript will always take over from directions in these general guidelines.

To make a paper clear

· Adhere to recommended page limits

Mistakes to evade

- Insertion a title at the foot of a page with the subsequent text on the next page

- Separating a table/chart or figure - impound each figure/table to a single page
- Submitting a manuscript with pages out of sequence

In every sections of your document

· Use standard writing style including articles ("a", "the," etc.)

· Keep on paying attention on the research topic of the paper

· Use paragraphs to split each significant point (excluding for the abstract)

· Align the primary line of each section

· Present your points in sound order

· Use present tense to report well accepted

· Use past tense to describe specific results

· Shun familiar wording, don't address the reviewer directly, and don't use slang, slang language, or superlatives

· Shun use of extra pictures - include only those figures essential to presenting results

Title Page:

Choose a revealing title. It should be short. It should not have non-standard acronyms or abbreviations. It should not exceed two printed lines. It should include the name(s) and address (es) of all authors.

Abstract:

The summary should be two hundred words or less. It should briefly and clearly explain the key findings reported in the manuscript--must have precise statistics. It should not have abnormal acronyms or abbreviations. It should be logical in itself. Shun citing references at this point.

An abstract is a brief distinct paragraph summary of finished work or work in development. In a minute or less a reviewer can be taught the foundation behind the study, common approach to the problem, relevant results, and significant conclusions or new questions.

Write your summary when your paper is completed because how can you write the summary of anything which is not yet written? Wealth of terminology is very essential in abstract. Yet, use comprehensive sentences and do not let go readability for briefness. You can maintain it succinct by phrasing sentences so that they provide more than lone rationale. The author can at this moment go straight to

shortening the outcome. Sum up the study, with the subsequent elements in any summary. Try to maintain the initial two items to no more than one ruling each.

- Reason of the study - theory, overall issue, purpose
- Fundamental goal
- To the point depiction of the research
- Consequences, including definite statistics - if the consequences are quantitative in nature, account quantitative data; results of any numerical analysis should be reported
- Significant conclusions or questions that track from the research(es)

Approach:

- Single section, and succinct
- As a outline of job done, it is always written in past tense
- A conceptual should situate on its own, and not submit to any other part of the paper such as a form or table
- Center on shortening results - bound background information to a verdict or two, if completely necessary
- What you account in an conceptual must be regular with what you reported in the manuscript
- Exact spelling, clearness of sentences and phrases, and appropriate reporting of quantities (proper units, important statistics) are just as significant in an abstract as they are anywhere else

Introduction:

The **Introduction** should "introduce" the manuscript. The reviewer should be presented with sufficient background information to be capable to comprehend and calculate the purpose of your study without having to submit to other works. The basis for the study should be offered. Give most important references but shun difficult to make a comprehensive appraisal of the topic. In the introduction, describe the problem visibly. If the problem is not acknowledged in a logical, reasonable way, the reviewer will have no attention in your result. Speak in common terms about techniques used to explain the problem, if needed, but do not present any particulars about the protocols here. Following approach can create a valuable beginning:

- Explain the value (significance) of the study
- Shield the model - why did you employ this particular system or method? What is its compensation? You strength remark on its appropriateness from a abstract point of vision as well as point out sensible reasons for using it.
- Present a justification. Status your particular theory (es) or aim(s), and describe the logic that led you to choose them.
- Very for a short time explain the tentative propose and how it skilled the declared objectives.

Approach:

- Use past tense except for when referring to recognized facts. After all, the manuscript will be submitted after the entire job is done.
- Sort out your thoughts; manufacture one key point with every section. If you make the four points listed above, you will need a least of four paragraphs.
- Present surroundings information only as desirable in order hold up a situation. The reviewer does not desire to read the whole thing you know about a topic.
- Shape the theory/purpose specifically - do not take a broad view.
- As always, give awareness to spelling, simplicity and correctness of sentences and phrases.

Procedures (Methods and Materials):

This part is supposed to be the easiest to carve if you have good skills. A sound written Procedures segment allows a capable scientist to replacement your results. Present precise information about your supplies. The suppliers and clarity of reagents can be helpful bits of information. Present methods in sequential order but linked methodologies can be grouped as a segment. Be concise when relating the protocols. Attempt for the least amount of information that would permit another capable scientist to spare your outcome but be cautious that vital information is integrated. The use of subheadings is suggested and ought to be synchronized with the results section. When a technique is used that has been well described in another object, mention the specific item describing a way but draw the basic

principle while stating the situation. The purpose is to text all particular resources and broad procedures, so that another person may use some or all of the methods in one more study or referee the scientific value of your work. It is not to be a step by step report of the whole thing you did, nor is a methods section a set of orders.

Materials:

- Explain materials individually only if the study is so complex that it saves liberty this way.
- Embrace particular materials, and any tools or provisions that are not frequently found in laboratories.
- Do not take in frequently found.
- If use of a definite type of tools.
- Materials may be reported in a part section or else they may be recognized along with your measures.

Methods:

- Report the method (not particulars of each process that engaged the same methodology)
- Describe the method entirely
- To be succinct, present methods under headings dedicated to specific dealings or groups of measures
- Simplify - details how procedures were completed not how they were exclusively performed on a particular day.
- If well known procedures were used, account the procedure by name, possibly with reference, and that's all.

Approach:

- It is embarrassed or not possible to use vigorous voice when documenting methods with no using first person, which would focus the reviewer's interest on the researcher rather than the job. As a result when script up the methods most authors use third person passive voice.
- Use standard style in this and in every other part of the paper - avoid familiar lists, and use full sentences.

What to keep away from

- Resources and methods are not a set of information.
- Skip all descriptive information and surroundings - save it for the argument.
- Leave out information that is immaterial to a third party.

Results:

The principle of a results segment is to present and demonstrate your conclusion. Create this part a entirely objective details of the outcome, and save all understanding for the discussion.

The page length of this segment is set by the sum and types of data to be reported. Carry on to be to the point, by means of statistics and tables, if suitable, to present consequences most efficiently.You must obviously differentiate material that would usually be incorporated in a study editorial from any unprocessed data or additional appendix matter that would not be available. In fact, such matter should not be submitted at all except requested by the instructor.

Content

- Sum up your conclusion in text and demonstrate them, if suitable, with figures and tables.
- In manuscript, explain each of your consequences, point the reader to remarks that are most appropriate.
- Present a background, such as by describing the question that was addressed by creation an exacting study.
- Explain results of control experiments and comprise remarks that are not accessible in a prescribed figure or table, if appropriate.
- Examine your data, then prepare the analyzed (transformed) data in the form of a figure (graph), table, or in manuscript form.

What to stay away from

- Do not discuss or infer your outcome, report surroundings information, or try to explain anything.
- Not at all, take in raw data or intermediate calculations in a research manuscript.

- Do not present the similar data more than once.
- Manuscript should complement any figures or tables, not duplicate the identical information.
- Never confuse figures with tables - there is a difference.

Approach

- As forever, use past tense when you submit to your results, and put the whole thing in a reasonable order.
- Put figures and tables, appropriately numbered, in order at the end of the report
- If you desire, you may place your figures and tables properly within the text of your results part.

Figures and tables

- If you put figures and tables at the end of the details, make certain that they are visibly distinguished from any attach appendix materials, such as raw facts
- Despite of position, each figure must be numbered one after the other and complete with subtitle
- In spite of position, each table must be titled, numbered one after the other and complete with heading
- All figure and table must be adequately complete that it could situate on its own, divide from text

Discussion:

The Discussion is expected the trickiest segment to write and describe. A lot of papers submitted for journal are discarded based on problems with the Discussion. There is no head of state for how long a argument should be. Position your understanding of the outcome visibly to lead the reviewer through your conclusions, and then finish the paper with a summing up of the implication of the study. The purpose here is to offer an understanding of your results and hold up for all of your conclusions, using facts from your research and generally accepted information, if suitable. The implication of result should be visibly described. Infer your data in the conversation in suitable depth. This means that when you clarify an observable fact you must explain mechanisms that may account for the observation. If your results vary from your prospect, make clear why that may have happened. If your results agree, then explain the theory that the proof supported. It is never suitable to just state that the data approved with prospect, and let it drop at that.

- Make a decision if each premise is supported, discarded, or if you cannot make a conclusion with assurance. Do not just dismiss a study or part of a study as "uncertain."
- Research papers are not acknowledged if the work is imperfect. Draw what conclusions you can based upon the results that you have, and take care of the study as a finished work
- You may propose future guidelines, such as how the experiment might be personalized to accomplish a new idea.
- Give details all of your remarks as much as possible, focus on mechanisms.
- Make a decision if the tentative design sufficiently addressed the theory, and whether or not it was correctly restricted.
- Try to present substitute explanations if sensible alternatives be present.
- One research will not counter an overall question, so maintain the large picture in mind, where do you go next? The best studies unlock new avenues of study. What questions remain?
- Recommendations for detailed papers will offer supplementary suggestions.

Approach:

- When you refer to information, differentiate data generated by your own studies from available information
- Submit to work done by specific persons (including you) in past tense.
- Submit to generally acknowledged facts and main beliefs in present tense.

Administration Rules Listed Before Submitting Your Research Paper to Global Journals Inc. (US)

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

Segment Draft and Final Research Paper: You have to strictly follow the template of research paper. If it is not done your paper may get rejected.

- The **major constraint** is that you must independently make all content, tables, graphs, and facts that are offered in the paper. You must write each part of the paper wholly on your own. The Peer-reviewers need to identify your own perceptive of the concepts in your own terms. NEVER extract straight from any foundation, and never rephrase someone else's analysis.

- Do not give permission to anyone else to "PROOFREAD" your manuscript.

- Methods to avoid Plagiarism is applied by us on every paper, if found guilty, you will be blacklisted by all of our collaborated research groups, your institution will be informed for this and strict legal actions will be taken immediately.)
- To guard yourself and others from possible illegal use please do not permit anyone right to use to your paper and files.

Criterion for Grading a Research Paper (Compilation) by Global Journals Inc. (US)

Please note that following table is only a Grading of "Paper Compilation" and not on "Performed/Stated Research" whose grading solely depends on Individual Assigned Peer Reviewer and Editorial Board Member. These can be available only on request and after decision of Paper. This report will be the property of Global Journals Inc. (US).

Topics	Grades		
	A-B	**C-D**	**E-F**
Abstract	Clear and concise with appropriate content, Correct format. 200 words or below	Unclear summary and no specific data, Incorrect form Above 200 words	No specific data with ambiguous information Above 250 words
Introduction	Containing all background details with clear goal and appropriate details, flow specification, no grammar and spelling mistake, well organized sentence and paragraph, reference cited	Unclear and confusing data, appropriate format, grammar and spelling errors with unorganized matter	Out of place depth and content, hazy format
Methods and Procedures	Clear and to the point with well arranged paragraph, precision and accuracy of facts and figures, well organized subheads	Difficult to comprehend with embarrassed text, too much explanation but completed	Incorrect and unorganized structure with hazy meaning
Result	Well organized, Clear and specific, Correct units with precision, correct data, well structuring of paragraph, no grammar and spelling mistake	Complete and embarrassed text, difficult to comprehend	Irregular format with wrong facts and figures
Discussion	Well organized, meaningful specification, sound conclusion, logical and concise explanation, highly structured paragraph reference cited	Wordy, unclear conclusion, spurious	Conclusion is not cited, unorganized, difficult to comprehend
References	Complete and correct format, well organized	Beside the point, Incomplete	Wrong format and structuring

INDEX

O

P

R

S

T

V

W

save our planet

Global Journal of Computer Science and Technology

Visit us on the Web at www.GlobalJournals.org | www.ComputerResearch.org
or email us at helpdesk@globaljournals.org

ISSN 9754350