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

Global Journal of Computer Science and Technology : E

Network, Web & Security

DISCOVERING THOUGHTS AND INVENTING FUTURE

HIGHLIGHTS

- Architectural Metrics Scorecard
- Enhanced Chat Application
- Telecommunication Networks
- QoS Provisioning Approach

Computer Server Farm

Volume 12 | Issue 11 | Version 1.0 ENG

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

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

Volume 12 Issue 11 (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: Open Association of Research Society
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

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

Packaging & Continental Dispatching

Global Journals, India

Find a correspondence nodal officer near you

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

eContacts

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

Pricing (Including by Air Parcel Charges):

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

Editorial Board Members (HON.)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Contents of the Volume

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 12 Issue 11 Version 1.0 June 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

An Architectural Metrics Scorecard Based Approach to Intrusion Detection System Evaluation for Wireless Network

By Rupinder Singh & Dr. Jatinder Singh
Khalsa College, Amritsar, Punjab, India

Abstract - Wireless IDS architectural metrics are used to compare the intended scope, architecture of wireless IDS, and how they match the deployment architecture. These metrics can be used to evaluate the architectural efficiency of a wireless IDS and can help in designing efficient wireless IDS. Wireless IDS analyze wireless specific traffic including scanning for external users trying to connect to the network through access points and play important role in security to wireless network. Design of wireless IDS is a difficult task as wireless technology is advancing every day, Architectural metrics can play an important role in the design of wireless IDS by measuring the areas concern with the architecture of a wireless IDS. In this paper we describe a set of architectural metrics that are relevant to wireless IDS. A "scorecard" containing the set of values is used as the centerpiece of testing and evaluating a wireless IDS. Evaluation of a wireless IDS can be done by assigning score to various architectural metrics concern with wireless IDS. We apply our architectural metrics scorecard based evaluation approach to three popular wireless IDS Snort-wireless, AirDefense Guard, and Kismet. Finally we discuss the results and the opportunities for further work in this area.

Keywords : *Architectural Metrics, Wireless, Metrics, IDS, and Scorecard.*

GJCST-E Classification: *C.2.0*

Strictly as per the compliance and regulations of:

An Architectural Metrics Scorecard Based Approach to Intrusion Detection System Evaluation for Wireless Network

Rupinder Singh [α] & Dr. Jatinder Singh [σ]

Abstract - Wireless IDS architectural metrics are used to compare the intended scope, architecture of wireless IDS, and how they match the deployment architecture. These metrics can be used to evaluate the architectural efficiency of a wireless IDS and can help in designing efficient wireless IDS. Wireless IDS analyze wireless specific traffic including scanning for external users trying to connect to the network through access points and play important role in security to wireless network. Design of wireless IDS is a difficult task as wireless technology is advancing every day, Architectural metrics can play an important role in the design of wireless IDS by measuring the areas concern with the architecture of a wireless IDS. In this paper we describe a set of architectural metrics that are relevant to wireless IDS. A "scorecard" containing the set of values is used as the centerpiece of testing and evaluating a wireless IDS. Evaluation of a wireless IDS can be done by assigning score to various architectural metrics concern with wireless IDS. We apply our architectural metrics scorecard based evaluation approach to three popular wireless IDS Snort-wireless, AirDefense Guard, and Kismet. Finally we discuss the results and the opportunities for further work in this area.

Keywords : Architectural Metrics, Wireless, Metrics, IDS, and Scorecard.

I. Introduction

A new and exciting world has been opened by wireless. Its technology is advancing every day and its popularity is increasing. The biggest concern with wireless, however, has been its security, for some time wireless has had very poor, if any, security on a wide-open medium. Along with improved encryption schemes, a new solution to help combat this problem is the Wireless Intrusion Detection System (WIDS). An Intrusion Detection System (IDS) is a device or software application that monitors network and/or system activities for malicious activities or policy violations and produces reports to a Management Station (Wikipedia, 2012). A wireless IDS performs this exclusively for the wireless network. This system monitors traffic on network looking for threats and alerting personnel to respond.

Author α : Assistant Prof., P.G. Deptt. of Computer Science and Applications, Khalsa College, Amritsar, Punjab, India.
Author σ : Principal, Golden College of Engg. & Tech., Gurdaspur, Punjab, India. E-mails : rupi_singh76@yahoo.com, bal_jatinder@rediffmail.com

Lord Kelvin said "If you cannot measure it, you cannot improve it". This fact also applies to wireless network security issues. An activity cannot be managed if it cannot be measured, this is a widely accepted management principle and security falls under this rubric. Metrics can be an effective tool for security providers to discern the effectiveness of various components of their security programs. Metrics can play an important role in the designing of wireless IDS. Security Metrics that are related to wireless network are hard to generate because the discipline itself is still in the early stages of development. There is not yet a common vocabulary and not many documented best practices to follow [1].

This paper provides an architectural metrics scorecard based approach to evaluate Intrusion Detection Systems that are currently popular for wireless in the commercial sector. We describe a testing methodology we developed to evaluate wireless IDS by assigning score to various architectural metrics concern with it. The approach followed in this paper do not compare wireless IDS against each other, but against a set of architectural metrics concern with wireless IDS.

The generalized approach of this paper will allow systems with any wireless requirements to tailor evaluation of ID technologies to their specific needs. Since evaluation is against a static set of architectural metrics the evaluation may be extended for other metrics like logistical metrics, performance metrics, quality metrics etc. The standard approach of comparison used in this paper also gives us scientific repeatability.

II. Snort, Airdefense Guard and Kismet Wireless Ids

In order to explain architectural metrics scorecard based evaluation approach to wireless IDS, we choose three wireless IDS namely Snort-wireless, AirDefense Guard, and Kismet as these are one of the most popular and works on different technology.

a) Snort Wireless IDS

Snort is an open source network intrusion detection and prevention system (IDS/IPS) that combines the benefits of signature, protocol, and anomaly-based inspection, and is the most widely

deployed IDS/IPS technology worldwide. With millions of downloads Snort has become the de facto standard for IDS/IPS [4]. Snort-wireless allows for custom rules to be created based on framing information from a wireless packet. It also contains rules to attempt to find rogue access points, war drivers, and ad hoc networks.

Snort-wireless works by implementing a detection engine that allows registering, warning, and responding to attacks previously defined. Snort-wireless is available under GPL (General Public License) and runs under Windows and GNU/Linux. It is among the most widely used, has a number of predefined signatures and continuously updated. Snort wireless can be configured in three modes namely sniffer, packet logger, and network intrusion detection. In addition to all of these basic Snort-wireless features, Snort-wireless can be set up to send real-time alerts. This provides with the ability to receive alerts in real time, rather than having to continuously monitor Snort system. Snort is like a vacuum that takes packets and allows to do different things.

b) AirDefense Guard Wireless IDS

AirDefense Guard is a wireless IDS that provides advanced intrusion detection for wireless LANs based on signature analysis, policy deviation, protocol assessment policy deviation and statistically anomalous behavior. AirDefense Guard is able to respond to attacks with Active Defense technology, which interfaces with the access points to disconnect the attackers connection to the WLAN.

AirDefense can be used to identity theft. This is done by stealing an authorized MAC address, an intruder has full access to the network. However, AirDefense tracks the digital fingerprints vendor-specific characteristics and personal trademarks of authorized users to identify intruders in the network. AirDefense can be used to detect Denial-of-Service (DoS) attacks. AirDefense is able to quickly recognize the early signs and protocol abuses of a DoS attack that jams the airwaves and shuts down a wireless LAN. AirDefense can also be used to detect Man-in-the-Middle attacks. Posing as an access point, intruders can force workstations to disassociate from authorized access points and route all traffic through the intruder. The intruder can then gain access to the network by posing as an authorized user and simultaneously operating on multiple channels. AirDefense detects man-in-the-middle attacks and ensure that access points only operate on set channels and proper protocols are used.

c) Kismet Wireless IDS

Kismet is an 802.11 layer2 wireless network detector, sniffer, and intrusion detection system. Kismet will works with any wireless card that supports raw monitoring mode, and can sniff 802.11b, 802.11a, 802.11g, and 802.11n traffic. Kismet also supports plugins that allows sniffing other media such as DECT. Kismet identifies networks by passively collecting packets and detecting standard named networks, detecting hidden networks, and inferring the presence of nonbeaconing networks via data traffic [8]. Kismet wireless IDS without sending any loggable packets is able to detect the presence of both wireless access points and wireless clients, and associate them with each other. Unlike most other wireless network detectors. Kismet has the ability to log all sniffed packets and save them in a tcpdump /Wireshark or Airsnortcompatible fileformat. Kismet also captures PPI headers. Kismet also has the ability to detect default or "not configured" networks, probe requests, and determine what levels of wireless encryptions is used on a given access point. Kismet also supports logging of the geographical coordinates of the network if the input from a GPS receiver is additionally available [12].

III. Architectural Metrics Scorecard Based Approach

a) Developing Scorecard

Centerpiece of testing and evaluating wireless IDS will be a “scorecard” containing the set of architectural metrics and their definitions. Each metric can have low (+), average (++), or high (+++) score, where higher scores will be interpreted as more favorable ratings.

The architectural metrics used are general characteristics that are relevant to architecture of a wireless IDS. The method used for observing each architectural metric value can be either analysis (source code analysis) or open source material (such as specifications, white papers or reviews provided by vendors or users). We use open source material to analyze each architectural metrics for wireless IDS. We examine publicly available research papers, reports, product documentation, published conference material (proceedings) and other material available for public review.

b) Architectural Metrics for a Wireless IDS

Architectural metrics are used to compare the intended scope and architecture of wireless IDS and how they match the deployment architecture. These metrics evaluate the architectural efficiency of a Wireless IDS [13]. The metrics defined in this area are shown in Table 1. Other Architectural metrics that may be included are: Anomaly Based, Autonomous Learning, Host/OS Security, Interoperability, Package Contents, Process Security, Signature Based, and Visibility [6].

Table 1 : Selected architectural metrics for a wireless IDS

Architectural Metrics	Description
Adjustable Sensitivity	The difficulty of altering the sensitivity of a wireless IDS in order to achieve a balance between false positive and false negative error rates at various times and for different environments.
Required Data Storage Capacity	The amount of disk space needed to store logs and other application data.
Load Balancing Scalability	It measures the ability of a wireless IDS to partition traffic into independent, balanced sensor loads.
Multiple Sensor Support	The cardinality of sensors supported.
Reordering and Stream Reassembly	It can be used to find an attack that has been artificially fragmented and transmitted out of order.
State Tracking	This metric is useful in hardening wireless IDS against storms of random traffic used to confuse it.
Data Pool Selectability	This metric is used to define the data source to be analyzed for intrusions.
System Throughput	Maximal data input rate that can be processed successfully by the wireless IDS.

Table 2 : Scorecard for Snort wireless, AirDefense, and Kismet wireless IDS. + : Low score ; ++ : Average score ; +++ : High Score

Architectural Metrics	Snort wireless	AirDefense Guard	Kismet
Adjustable Sensitivity	+++	++	++
Required data Storage Capacity	+	++	+++
Load Balancing Scalability	+++	+++	++
Multiple Sensor Support	+++	+++	+++
Reordering and Stream Reassembly	+++	+++	+++
State Tracking	+++	+++	+++
Data Pool Selectability	+++	+++	+++
System Throughput	+++	++	++

c) Architectural Metrics Scorecard Based Approach

In this section we will apply above mentioned approach to popular wireless IDS Snort-wireless, AirDefense Guard, and Kismet. We choose these three for evaluation as they are one of the most widely used and have different ways of working. Below with table 2 we describe how scores to architectural metrics related to these three wireless IDS are assigned.

Architectural metric Adjustable Sensitivity can be assigned score depending on the following criteria:

Low Score (+): No Adjustability.

Average Score (++): Adjustability via static methods.

High Score (+++): Intelligent, dynamic Adjustability.

Snort-wireless makes use of the SSL Dynamic Preprocessor (SSLPP), which decodes SSL and TLS traffic and optionally determines if and when Snort-wireless should stop inspection of it. Encrypted traffic is ignored by Snort-wireless for both performance reasons and to reduce false positive and false negative error rate [15]. So, Snort-wireless gets a high score (+++) for metric adjustable sensitivity. Kismet wireless provides alerts based on fingerprints (specific nets tumbler versions). In an attempt to disclose the SSID of a network, Nets tumbler sends out unique packets. This is not done in all situations, but when it is detected the potential for false positives is very low [16]. So, kismet gets average score for metric adjustable sensitivity. As described in [17] Air defense guard delivered a false positive for a Nets tumbler scan that turned out to be one of test laptops pinging an AP. Air Defense acknowledged that its Nets tumbler, signature needs some tweaking. So, it gets average score for metric adjustable sensitivity.

Architectural metric Required Data Storage Capacity can be assigned score depending on the following criteria:

Low Score (+): Large capacity storage needed to store log and other files.

Average Score (++): Medium capacity storage needed to store log and other files.

High Score (+++): Low capacity storage needed to store log and other files. Databases are used with Snort wireless to store log and alert data. Logging data to files in the disk is fine for smaller applications. However, keeping log data in disk files is not appropriate when there are multiple Snort-wireless sensors or there is need to keep historical data as well. Databases also allow to analyze data generated by Snort-wireless sensors. Snort-wireless uses rules stored

in text files that can be modified by a text editor. Rules are grouped in categories. Rules belonging to each category are stored in separate files. These files are then included in a main configuration file called snort.conf. Alerts are also stored in log files or databases where they can be viewed later on by security experts. Snort wireless needs a large database as its rules grows and gets a for this metric. Airdefense guard makes use of average data storage. Kismet wireless makes use of predefine rules and therefore needs less storage to store files.

Architectural metric Load Balancing Scalability can be assigned score depending on the following criteria:

Low Score (+): No load balancing scalability.

Average Score (++): Low load balancing scalability.

High Score (+++): Highly capable of partitioning traffic into independent, balanced sensor loads.

If the bandwidth being passed by the network interface associated with a Snort-wireless instance is greater than it can handle, more instances of Snort-wireless can be launched and the traffic can be load balanced across the instances. An Adaptive load balancing architecture for snort is discussed in [18]. So, snort wireless gets a +++ score for this metric.

Motorola AirDefene guard wireless IDS clients use a sophisticated load-balancing algorithm when too many clients attempt to connect to a particular access point. The clients use a beacon element to perform pre-emptive roaming and load balancing, thereby moving from a heavily loaded AP to one that is less loaded. Kismet wireless is not as capable as Snortwireless and AirDefense Gurad for load balancing scalability.

Architectural metric Multiple Sensor Support can be assigned score depending on the following criteria:

Low Score (+): Very less number of sensors supported.

Average Score (++): Average number of sensors supported.

High Score (+++): Large number of sensors supported.

A corporate environment probably have multiple locations and there is need to install Snort-wireless sensors. There are multiple ways to setup and install Snort-wireless in the enterprise as a distributed IDS. One method is to connect multiple sensors to the same centralized database. All data generated by these sensors is stored in the database. A user then uses a web browser to view this data and analyze it.

In an alternate mechanisms, Snort-wireless sensors do not have a direct connection to the database server. The sensors may be configured to log to local files. These files can then be uploaded to a centralized server on a periodic basis using utilities like SCP. The only problem with this approach is that the data in the database is not strictly "real-time". There is a certain delay which depends upon frequency of uploading data using SCP to the centralized database server. This arrangement is shown in Figure 1 [7].

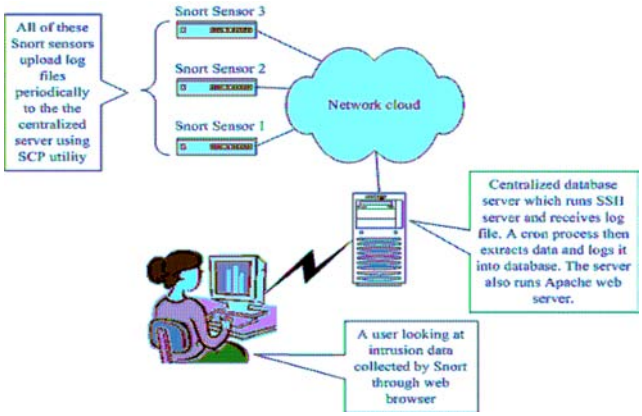


Figure 1 : Distributed Snort-wireless installation with the help of tools like SCP and Barnyard [7]

Snort wireless gets a +++ score for this metric. The Air Defense solution is based on a Distributed Collaborative Intelligence Architecture (DCIA), pioneered by Air Defense, to provide the most comprehensive wireless intrusion protection. DCIA uses a dedicated network of sensors and embedded client based agents that continuously monitor the airwaves and wireless activity for attacks and policy violations. In addition, the sensors use an intelligent channel scanning algorithm to detect traffic across the RF spectrum. So, Air Defense guard also gets a +++ score. Like Snort-wireless and Air defense Kismet wireless also have a support to multiple sensors.

Architectural metric Reordering and Stream Reassembly can be assigned score depending on the following criteria:

Low Score (+): No capability to find an attack that has been artificially fragmented and transmitted out of order.

Average Score (++): Very less capability to find an attack that has been artificially fragmented and transmitted out of order.

High Score (+++): Highly capable to find an attack that has been artificially fragmented and transmitted out of order.

The open source IDS Snort wireless implement target-based analysis with the frag3 preprocessor. Frag3 is able to reassemble overlapping fragments using the same policy as the destination host. A user configures the IDS to apply specific fragmentation reassembly policies for individual hosts or networks. Then, when the Snort sees overlapping fragments bound for any of these hosts, it knows the appropriate reassembly policy to apply—allowing both Snort and the destination host to reassemble the fragments identically.

Snort wireless gets a +++ score as it is able to find an attack that has been artificially fragmented and transmitted out of order. AirDefense Guard and Kismet wireless are also capable for out of order attaks.

Architectural metric State Tracking can be assigned score depending on the following criteria:

Low Score (+): No capability to detect storms of random traffic used to confuse wireless IDS.

Average Score (++): Less capability to detect storms of random traffic used to confuse wireless IDS.

High Score (+++): High capability to detect storms of random traffic used to confuse wireless IDS.

Snort wireless gets a high score for metric state tracking as Snort wireless provides many configuration and command line options to detect storms of random traffic that can be specified in the snort configuration file. Table 3 describes such commands. AirDefense guard and Kismet wireless are also able to track state and gets a +++ score.

Architectural metric Data Pool Selectability can be assigned score depending on the following criteria:

Low Score (+): Poor capability to detect the data source to be analyzed for intrusion.

Average Score (++): Average capability to detect the data source to be analyzed for intrusion.

High Score (+++): Highly capable to detect the data source to be analyzed for intrusion

Snort wireless gets a +++ score for metric data pool selectablity as Snort is a very complex pattern matcher geared toward detecting patterns of network attack traffic. On any given network, on any given day, Snort can fire thousands of alerts. Snort wireless makes use of ACID, SGUIL, SnortSnarf, Snort_stat.pl, Swatch tools to analyze intrusion data. AirDefense guard and kismet wireless like Snort-wireless are also able to properly select data pool.

Table 3 : Snort configuration commands

Command	Description
Enable_decode_ drops	Enables the dropping of bad packets identified by decoder (only applicable in inline mode).
Enable_tcpopt_e xperimental_dro ps	Enables the dropping of bad packets with experimental TCP option. (only applicable in inline mode).
Enable_tcpopt_o bsolete_ Drops	Enables the dropping of bad packets with obsolete TCP option. (only applicable in inline mode).
Enable_tcpopt_tt cp_drops	Enables the dropping of bad packets with T/TCP option. (only applicable in inline mode).
Enable_tcpopt_d rops	Enables the dropping of bad packets with bad/truncated TCP option (only applicable in inline mode).
Enable_ipopt_dr ops	Enables the dropping of bad packets with bad/truncated IP options (only applicable in inline mode).

Architectural metric System Throughput can be assigned score depending on the following criteria:

Low Score (+): Wireless IDS can successfully process less data input rate.

Average Score (++): Wireless IDS can successfully process average data input rate.

High Score (+++): Wireless IDS can successfully process high data input rate.

If Snort has to work with a high speed connection, then there is need to use unified logging and a unified log reader such as barnyard. This allows Snort-wireless to log alerts in a binary form as fast as possible while another program performs the slow actions, such as writing to a database. AirDefense Guard and Kismet wireless process less data input rate as compare to snort wireless and both gets ++ score for the metric system throughput. Figure 2 shows score of Snort-wireless, Airdefense and Kismet IDS.

IV. Conclusion and Future Work

Unwanted activities on a wireless network can be detected by a wireless IDS. Architectural design of a wireless IDS is a difficult task as the technology of design of wireless network is changing at a pace which brings additional challenges in the design of wireless IDS. This paper provides an architectural metrics scorecard based approach that can be used for evaluating a wireless IDS in order to find out the areas in which wireless IDS is weak and needs improvement. Depending upon the requirements of the system these metrics me given priorities and appropriate wireless IDS may be selected after developing the scorecard.

In this paper we define various architectural metrics concern with wireless IDS and a scorecard method to evaluate a wireless IDS by assigning scores to various architectural metrics. We use our evaluation methodology to test popular wireless IDS Snort-wireless, Air Defense Guard, and Kismet. This paper defines commonly used architectural metrics that are important to a wireless IDS, but a lot is required to be done to find out more ones like anomaly based, autonomous learning, Host/OS security, interoperability, package contents, process security, signature based, visibility etc. More architectural metrics and their definitions can be defined as lessons are learned while evaluating a wireless network. Future work also includes applying the evaluation methodology to other metrics concern with wireless IDS like logistical metrics, performance metrics, quality metrics etc.

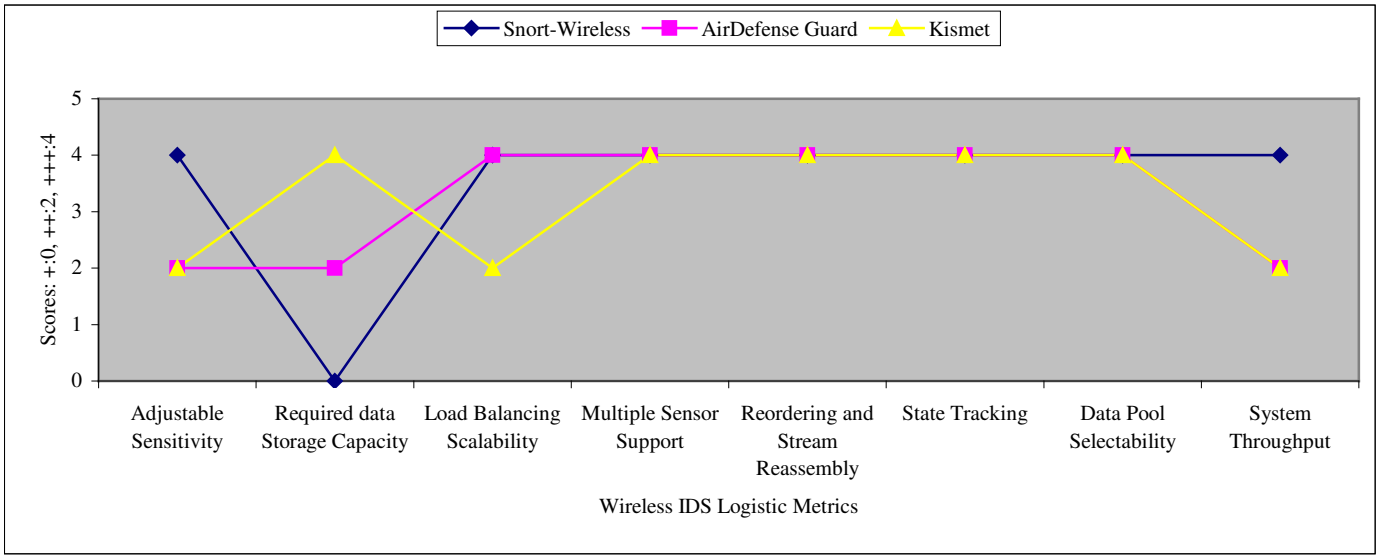


Figure 2 : Graph showing score of Snort-wireless, Air Defense and Kismet wireless IDS

References Références Referencias

1. Rupinder Singh, Dr. Jatinder Singh, "A Metrics-Based Approach to Intrusion Detection System Evaluation for Wireless Network," International Journal of Education and Applied Research (IJEAR)Vol.1, Issue 1, Ver. 1: Jul.- Dec., 2011, ISSN : 2249-4944.
2. http://downloads.visionid.ie/wireless/Dedicated_Distributed_Sensing_The_Right_Approach_to_Wireless_Intrusion_Prevention.pdf
3. Motorola Enterprise WLAN Design Guide Volume November 2008, Available at: http://www.scantexas.com/asset/support/Motorola%20Enterprise%20WLN%20Design %20Guide.pdf
4. Stephen Northcutt, "Snort 2.1 Intrusion Detection," Second Edition, Shroff Publishers, ISBN: 81-7336-894-9.
5. G. A. Fink, B. L. Chappell, T. G. Turner, and K. F. O'Donoghue, "A Metrics - Based Approach to Intrusion Detection System Evaluation for Distributed Real – Time Systems," WPDRTS April 2002, Ft. Lauderdale, Florida.
6. Harrykar Freelance, "HARRYKAR'S TECHIES BLOG Snort, IDS, IPS, NSM, hacking andbeyond," 31 May 09.
7. Rafeeq Ur Rehman,"Intrusion Detection System with Snort Advanced IDS Techniques Using Snort, Apache, MySQL, PHP, and ACID," Prentice Hall, ISBN 0-13-1407 33-3. Available at: http://ptgmedia.pearsoncmg.com/images/013147333/downloads/0131407333.pdf
8. http://www.kismetwireless.net/
9. SNORT Users Manual 2.9.0, Snort Project, March 2011
10. J. Gómez, C. Gil, N. Padilla1, R. Baños, and C. Jiménez, "Design of a Snor – Based Hybrid Intrusion Detection System," IWANN 2009, Part II, LNCS 5518, 2009.
11. Reijo Savola, "On the Feasibility of Utilizing Security Metrics in Software Intensive Systems," IJCSNS, VOL. 10 No.1, January 2010.
12. http://en.wikipedia.org/wiki/Kismet
13. Snehal Boob and Priyanka Jadhav, "Wireless Intrusion Detection System," International Journal of Computer Applications (0975–8887) Volume 5– No.8, August 2010.
14. http://www.snort.org/
15. SNORT Users Manual 2.9.1, the Snort Project September 20, 2011. Available at: http://www.snort.org/. assets/166/snort_manual.pdf
16. http://www.kismetwireless.net/documentation.html
17. http://www.networkcomputing.com/wireless/22962263?printer_friendly=this-page
18. M. Alam, Qasim Javed, M. Akbar, "Adaptive load balancing architecture for snort,". http://www.geocities.ws/raza_nust/incc.pdf

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 12 Issue 11 Version 1.0 June 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

"Enhanced Chat Application"

By Avinash Bamane, Parikshit Bhoyar, Ashish Dugar & Lineesh Antony
Pune University

Abstract - We have come across various chat applications to instantly communicate with people. We have used various types of chat application in web-based applications. All these chat applications support text messages to be sent between the users in the instant they press Enter key. But if some problem has to be explained using diagrams, that is where most of these chats are helpless. The chat application we intend to do solves this problem as we are going to integrate a paint like editor to the chat window, so that diagrams could also be drawn and sent through chat. This could be helpful to many of the professional institutions like schools, colleges and industrial units. So we intend to design this application for LAN of these organizations. The people could use many features of this chat application to communicate and brainstorm within a LAN. For this application we need design it on a Client-Server architecture.

Though the primary focus of our application is on the feature of providing communication through diagrams and figures, we would also provide different features in our chat app like using predictive texting, providing themes, voice to smiley, etc. thus making an enhanced chat application.

GJCST-E Classification: *H.4.3*

Strictly as per the compliance and regulations of:

"Enhanced Chat Application"

Avinash Bamane [α], Parikshit Bhoyar [σ], Ashish Dugar [ρ] & Lineesh Antony [ω]

Abstract - We have come across various chat applications to instantly communicate with people. We have used various types of chat application in web-based applications. All these chat applications support text messages to be sent between the users in the instant they press Enter key. But if some problem has to be explained using diagrams, that is where most of these chats are helpless. The chat application we intend to do solves this problem as we are going to integrate a paint like editor to the chat window, so that diagrams could also be drawn and sent through chat. This could be helpful to many of the professional institutions like schools, colleges and industrial units. So we intend to design this application for LAN of these organizations. The people could use many features of this chat application to communicate and brainstorm within a LAN. For this application we need design it on a Client-Server architecture.

Though the primary focus of our application is on the feature of providing communication through diagrams and figures, we would also provide different features in our chat app like using predictive texting, providing themes, voice to smiley, etc. thus making an enhanced chat application.

I. Introduction

We have used various types of chat application in web-based applications. All these chat applications support text messages to be sent between the users in the instant they press Enter key. Now suppose two friends are discussing Geometry problems which actually contain figures drawings and diagrams. When these two are actually far away from each other and still want discuss these problems simple texting is not the ideal solution for this. It would be so much better for them if they could communicate using actual diagrams and figures. Even telephoning won't help.

One solution we have come up with is to create a chat application using which we not only communicate using text messages but also with figures and diagrams. This would be helpful to a lot of professionals all over the world. It would also be popular for ordinary users. Our chat application is designed for professional organizations like schools, colleges, industrial units and organizations.

Though the primary focus of our application is on the feature of providing communication through diagrams and figures, we would also provide different features in our chat app like using predictive texting, exchange of files, providing themes, voice to smiley, etc.

Author α σ ρ ω : BE Computer, Pimpri Chinchwad College of Engineering.

II. System Features

The Chat application we intend to design would provide us with the following features:

- **Creating an Account:** The user gives his personal information, chooses a UserID and a password of his own choice. The database on the server side is updated after this.
- **Login and Logout:** These functions indicate the availability or non-availability of the user.
- **Handling Users:** It allows administrator to add or remove any user account in case of changes due to termination, resignation, violation of any rules or for some other reasons.
- **Instant Messaging:** This is a regular feature of any chat. This chat application would also provide this feature between multiple users.
- **Drawing:** The application allows users to use the paint window within the chat to draw basic figures like lines, rectangles, circles, etc or free hand.
- **Painting and Coloring:** The application allows users to use colors to draw figures and fill the figures. Different colors have been provided.
- **Predictive Text:** In this feature we would give user the option of using different words by predicting what the user is going to type from initial alphabets. The predictive texting is self learning. If the user has used typed "computer" word once. Then on typing of the letters "com", the word "computer" would be displayed.
- **Transferring images:** The chat application would also have to transfer images drawn by the users between each other.

III. System Architecture

Following diagram shows the architecture for the Enchanced Chat Application. In this diagram it shows how Application Work.

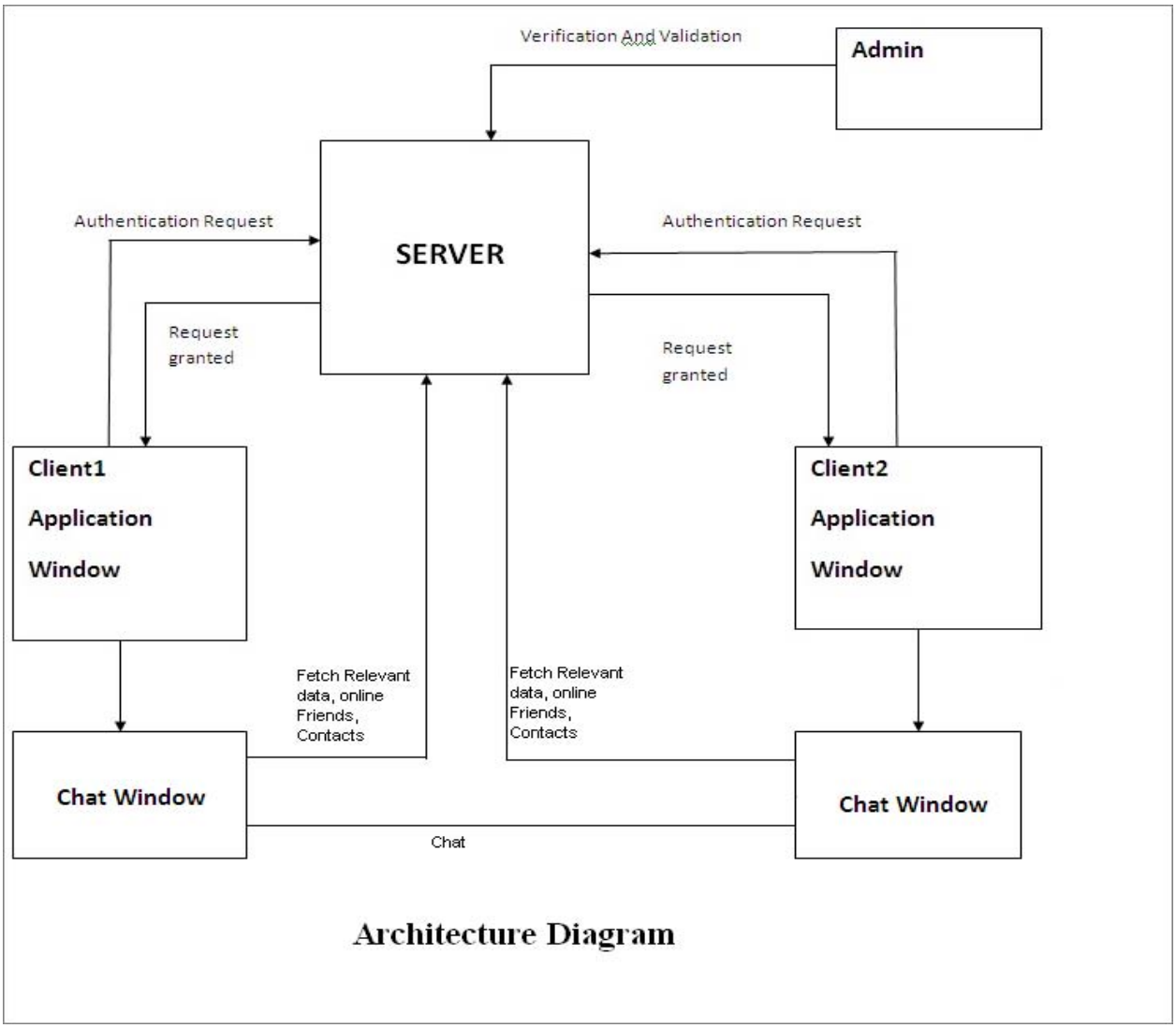


Fig.1 : System Architecture Diagram

The chat application would be accomplished on a Server-Client Architecture within a lan. The client–server model of computing is a distributed application that partitions tasks or workloads between the providers of a resource or service, called servers, and service requesters, called clients. The Server Side would be a continuously running service listening to the different Clients asking its services. The chat application would be installed on every communicating client. A Database of users would be maintained by the Server. When a client PC logins to the application, the Server authenticates the user of the client PC. Once the user is authenticated the IP address of the client is registered to the Server and it sends the list of online user friends and other relevant data to the Client. When the user wishes to chat to some other user, his IP address along with a Port address would be sent to the other user and vice versa. Thus a connection would be established and the two client PCs would be able to chat together.

IV. System Features

The system that we have built encompasses the following features. The working and explanation of the features have been given.

a) Chat Server

The System that we have designed is based on client-server architecture. So creating a server is necessary. The functions of a server are to maintain user information, maintaining the record of users logged in to the system and providing the IP addresses to the clients who want to chat.

In the Server side a server-socket is created which accepts connection from client those who have logged in. Once any user logs in and makes connection with the server, it is assigned a thread. Input stream and output stream objects are created in the run method. If the user has requested for registration then a new entry is added to the Database. If the request is for sign in

then the user is verified and then his flag is set as an online user.

b) Painting

Once the user logs in, he can use the application to draw and send images. This has been implemented by using a painting class. The following functionalities have been provided to the user. He can draw any of the following figures like point, line, circle, rectangle and rounded rectangle. Free hand drawing is also possible. Filled circle, filled rectangle and filled rounded rectangle are the other drawing figures available. User can use any of the ten colors for drawing. An eraser has been provided for erasing the drawn figures. These are the functionalities provided to the user. The working of the painting functionality can be explained. The painting class has implemented the action listener and mouse listeners. The action such as selecting the drawing tool and color of drawing is recorded. On the mouse click event the initial coordinates of the location of mouse is saved. The initial coordinates and the new coordinates on mouse move are used to draw the figures. Whenever the mouse is moved the paint function is called and the figures are drawn. The socket used for sending to the other client has already been created and is used by the paint function to send the coordinates to the other client. The receive class receives the coordinates sent by the other class which is then used by the receive panel to draw the images and figures. The server socket created for that particular connection is used to receive the coordinates, type of the figure and the color. In this way drawing has been done in the application.

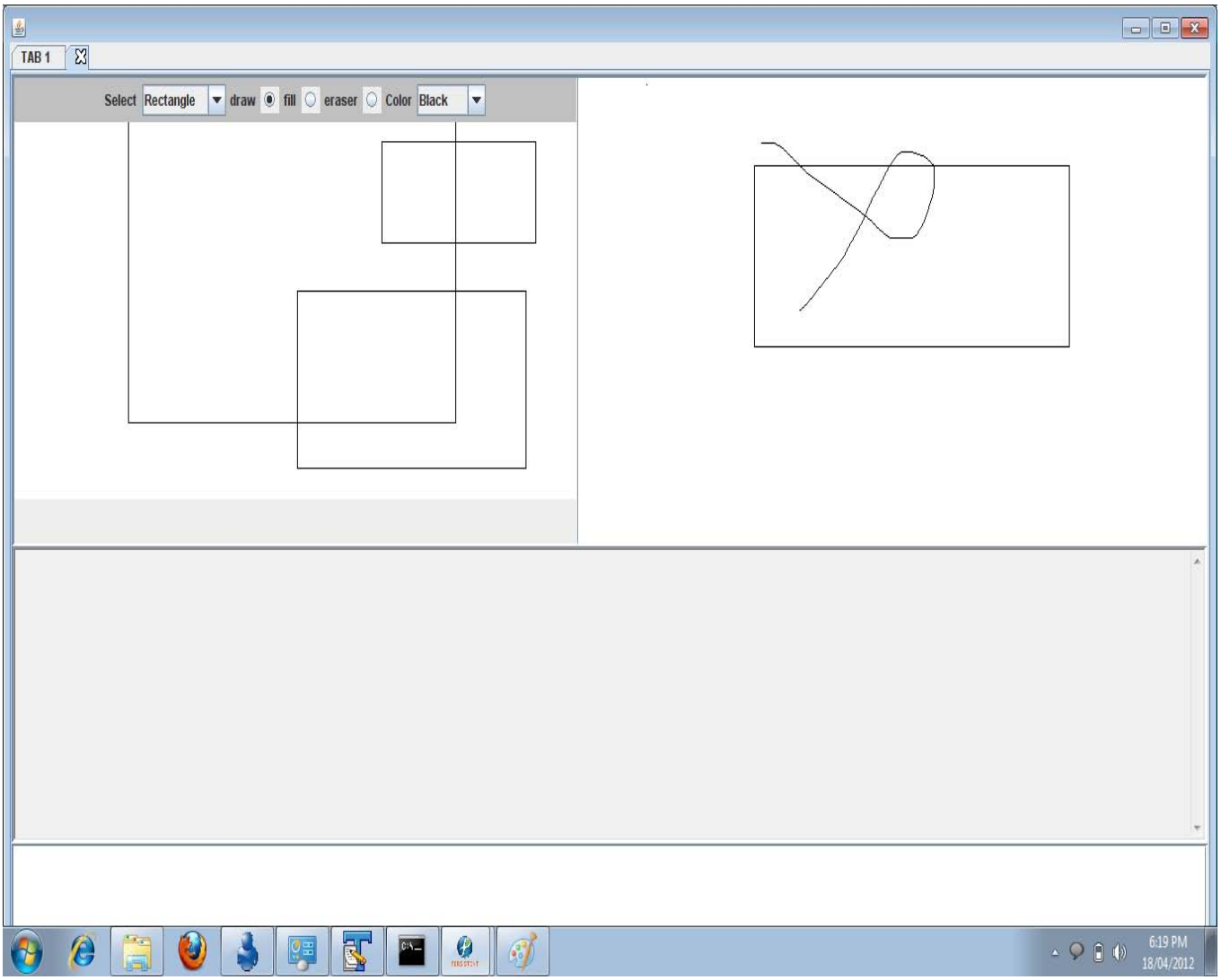


Fig. 2 : Painting done in the application

c) Message Texting

The user can type and send text messages to the other user instantly. This has been accomplished by socket connection. The SplitWindow class gets the sending socket used for connection. The text messages are sent through the socket. The key listener has been implemented on the bottom-most window where a user types the message. On the press of the Enter key, the

text message is sent to the other user and displayed over the text area of both the user. The receive function on the other side differentiates the text messages from those of the drawing and text messages and sends it to the text-area of the receiving user. In this way the texting has been implemented in this application.

d) Predictive Texting

Predictive testing is another enhancement that has been made in this application. Basically predictive texting means to predict what a user is going to type from the set of letters (substring) that user has already typed. The predictive texting system that has been implemented for this application is a self-learning from the typing of the users using. It does not have a prior database of words but instead adds the database of words as the user types. The words are stored for the particular session of conversation after which the words are not available again. So that the words do not clash with some other user who might later sit on the machine and logins to his account.

The Split Window class is where the windows for texting and painting have been implemented. In the class the auto-text complete class is called on the bottom most text field. So on key press events, the functioning of predictive texting begins. If the total length of the word is 3, the hash-chain class is called. A hash table is created for size of 10 words. The substring of 3 letters is passed as on of the parameters to the find function of the hash table. It computes the hashing value for the given substring which can be used to search all the words beginning with the substring or else can be used to insert the word to the specified location of the hash value. The hash function used for this purpose can be explained as follows. The hash value is calculated by summing up the ascii value of the letters of the substring, then a modular division is performed on the sum by the array size of the hash table. Thus a maximum of 10 words can be stored for a particular substring.

A frequency count of the words used has been maintained which provides the recurrence of words in typing. More the frequency of the words higher will be their priority. The lower priority words would be deleted from the hash table when it fills up. In this way the predictive texting has been implemented.

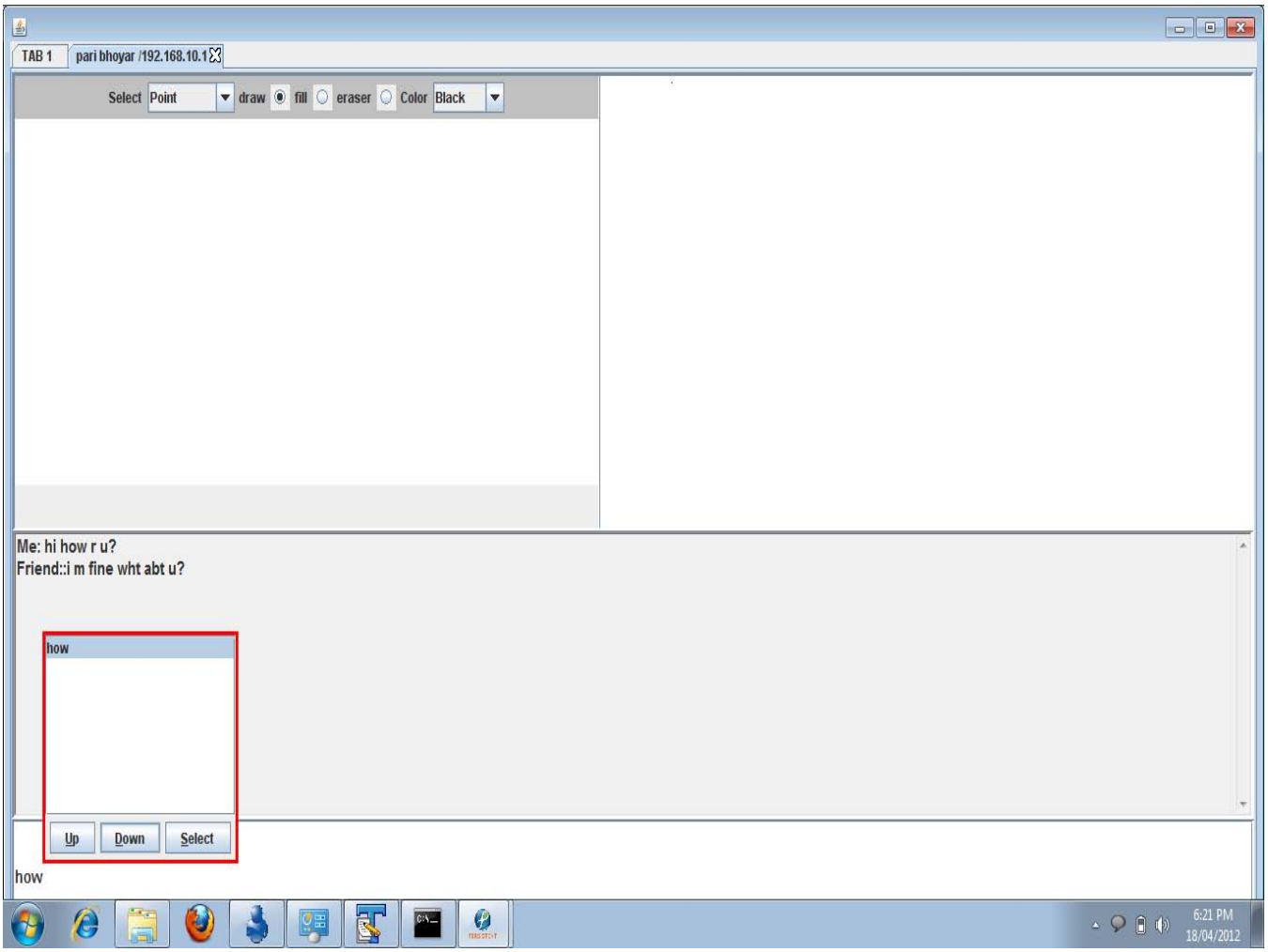


Fig. 2: Predictive texting done in the application

V. Tools Used and Other Requirements

a) Software tools used

- JDK for executing the application
- Oracle for storing the database of users
- Editplus, JCreator and Netbeans for coding the program

b) Hardware requirements

- A Local Area Network – can use switches, hubs and LAN cables.
- Two or more machines where the application could be run and one server machine.

VI. Conclusion

Chatting is a very common used application among the users. General users use the instant messaging services to communicate with other individual users. In our project we have provided with many enhanced features for a chat application. The features like painting along with chat would be a fun to use and interactive feature for a general user. For professional users it would be very useful for communicating important flowcharts, diagrammatic representation of some problem, making important symbols, etc. It opens up a wide variety of uses for individuals. The predictive texting feature would help a user to chat easily. Various figures of various formats could be opened and sent to other user. It would also give freedom of using any tool for drawing.

The chat application is so aimed that the people could have a better experience of chatting. It has the potential to attract more and more users to interact and connect.

Bibliography

1. Lam, Edmund Y. and Joseph W. Goodman. "Discrete Cosine Transform domain restoration of defocussed images." *Applied Optics*. 37, 6213-6218 (1998).
2. Ken Kabeen and Peter Gent. "Image Compression and Discrete Cosine Transform" College of Redwoods.
3. Predictive Text Entry using Syntax and Semantics - Sebastian Ganslandt, Jakob Jörwall, Pierre Nugues
4. http://www.java2s.com/Code/Java/JSTL/SimpleChatApplication.htm
5. http://www.codeproject.com/KB/java/java_applet_chat_with_gui.aspx
6. http://oreilly.com/catalog/javmesser/chapter/ch02.html

Global Journal of Computer Science and Technology (E) Volume XII Issue XI Version I
12
June 2012

This page is intentionally left blank

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 12 Issue 11 Version 1.0 June 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Study of Routing Protocols in Telecommunication Networks

By Pawandeep Chahal & Dr. Jatinder Singh
Desh Bhagat Institute of Engg. & Mgt, Moga

Abstract - In this paper we have discussed the problem of routing in telecommunication networks and the salient characteristics of some of the most popular routing schemes. In particular, we have discussed the characteristics of adaptive and multipath routing solutions versus static and single-path strategies.

GJCST-E Classification: C.2.2

Strictly as per the compliance and regulations of:

Study of Routing Protocols in Telecommunication Networks

Pawandeep Chahal [α] & Dr. Jatinder Singh [σ]

In this paper we have discussed the problem of routing in telecommunication networks and the salient characteristics of some of the most popular routing schemes. In particular, we have discussed the characteristics of adaptive and multipath routing solutions versus static and single-path strategies.

I. Routing: Definition and Characteristics

Routing can be characterized in the following general way. Let the network be represented in terms of a directed weighted graph G = (V, E), where each node in the set V represents a processing and forwarding unit and each edge in E is a transmission system with some capacity/bandwidth and propagation characteristics. Data traffic originates from one node and can be directed to another node (unicast traffic), to a set of other nodes (multicast traffic) and/or to all the other nodes (broadcast traffic). The node from where the traffic flow originates is also called source, or starting end-point, while the nodes to which traffic is directed are the final end-points, or destinations. The nodes in-between that forward traffic from sources to destinations are called intermediate, or relay, nodes. A flow is a vector in $R^{|E|}$ that for a traffic pair (s, D), $s \in V$, $D \subseteq V$, assigns a way of forwarding the data traffic from s to the nodes in D across the network while respecting the edge capacities and such that the sum of entering flows minus exiting flows at each node is null.

The general routing problem is the problem of defining path flows to forward incoming data traffic such that the overall network performance is maximized. At each node data is forwarded according to a decision policy parameterized by a local data structure called routing table. In this sense, a routing system can be properly seen as a distributed decision system.

According to the different characteristics of the processing and transmission components, as well as of traffic pattern and type of performance expected to be delivered, a variety of different classes of specific routing problems of practical and theoretical interest can be defined. For example, routing telephone calls in a network of mobile devices is a problem presenting characteristics which are quite different from those of the problem of routing telephone calls in a cable telephone network, which, in turn, is a problem much different from the problem of routing data packets in a best-effort connectionless data network as the Internet.

An important difference between routing and the combinatorial problems that have been considered so far consists in the presence of input data traffic which characterizes the problem instance. That is, the routing problem is composed of two parts: (i) the communication structure, which in a sense defines the constraints, and (ii) the traffic patterns that make use of this structure. It is always necessary to reason taking into account the two aspects together. For instance, the set of all the disjoint shortest paths (taken with respect to link bandwidths and propagation times) between all the network node pairs is not, in general, the optimal solution to the routing problem at hand. The optimal solution is obtained by considering the specific temporal and spatial distribution of the input traffic taken as a whole and solving simultaneously all the shortest path problems related to all the source–destination pairs relevant for traffic data. In fact, each allocated path flow recursively interferes with all the other path flows since it reduces the capacity which is available along the used links. Therefore, in a sense, the order of path flows allocation does really matter, as well as the possibility of rerouting path flows over time. That is, the knowledge about the characteristics of the input traffic is a key aspect to allow optimizing the allocation of the path flows in order to obtain optimal network-wide performance. On the other hand, in the case of routing this is rarely the case, since the characteristics of the incoming data traffic are hardly known with precision in advance. In the most fortunate cases, only some statistical knowledge can be assumed.

In practice, the routing problem in telecommunication networks must be solved online and under dynamically changing traffic patterns whose characteristics are usually not known in advance and recursively interact with the routing decisions. Moreover, routing is a fully distributed problem, a characteristic that usually rules out the use of global knowledge and/or centralized actions, and introduces problems of perceptual aliasing [15] (or hidden networks state) from the point of view of the nodes. Performance metrics usually consists of multiple conflicting objectives constrained by the specific characteristic of the

Author α : Research Scholar, CMJ University, Shillong , Meghalaya-793 003, Asst. Prof, Department of IT, Desh Bhagat Institute of Engg. & Management, Moga.
Author σ : Prof. , Dean, Desh Bhagat Institute of Engg. & Management, Moga.

transmission and processing technology. Finally, routing is a business-critical activity, therefore, any implementation of a routing system is required to be efficient, fault-tolerant, reliable, secure, etc.

In figure.1 traffic data must be forwarded from the source node 1 to the target node 13. Several possible paths are possible. Each node will decide where to forward the data according to the contents of its routing table. One (long) path among the several possible ones is showed by the arrows.

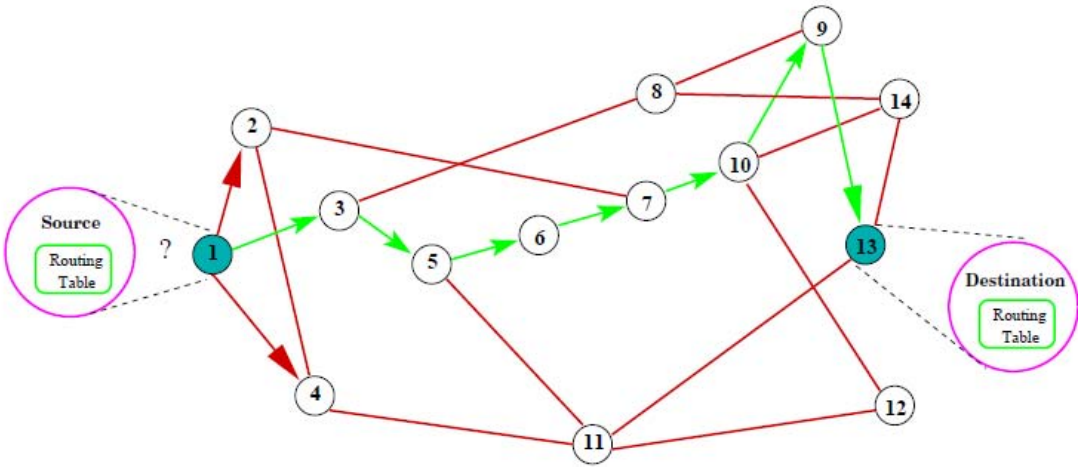


Figure 1 : Routing in networks

It is apparent that these characteristics do not find any counterpart in the class of static combinatorial problems considered so far. To have an idea, a VRP that could share a similar level of complexity, should have an unknown distribution of customer arrivals, a tight interaction among the vehicles (sort of traffic jams), strict time windows, backhauls, and the possibility for the drivers to get only local information.

When the characteristics of the traffic flows are known in advance, the problem can be solved in a centralized way, and other additional simplifications are possible, routing can be framed in the general terms of a multi-commodity flow problem, which is an important class of problems modeling the transfer of commodities from source locations to destinations.

At each network node:

- Acquisition and organization of up-to-date information concerning the local state, that is, information on the local traffic flows and on the status of the locally available resources.
- Build up a view of the global network state, possibly by some form of exchanging of the local state information.
- Use of the global view to set up the values of the local routing table and, consequently, to define the local routing policy with the perspective of optimizing some measure of network performance.
- Forward of the user traffic according to the defined routing policy.
- Asynchronously and concurrently with the other nodes repeat the previous activities over time.

II. Routing Algorithms Classification

Routing algorithms are usually designed in relationship to the type of both the network and the services delivered by the network. Under this perspective, given the variety of possible network types and delivered services, it is hard to identify meaningful and exhaustive classifications for routing algorithms. Therefore, the algorithms are classified according to few very general characteristics that can be singled out. Additional general characteristics that can be used to classify routing algorithms can be derived by the meta-algorithm, which suggests that different choices for either the optimization criteria or the strategies for building and using the local and the global views can result in different classes of algorithms. In particular, since the strategies for building the local and global views are strictly related to the way both traffic information and topological information are managed in order to define the routing tables, a classification of the different routing systems is precisely given according to the algorithm behavior, which can be static or adaptive with respect to topology and/or traffic patterns. Moreover, since different choices in the criterion to be optimized can generate different classes of algorithms, a further classification is given in this sense, making a distinction between optimal and shortest path routing. A final classification is drawn according to the number of paths that are used or maintained for the same traffic

session or destination. In this sense, algorithms are divided in single-path, multi-path and alternate-path.

a) Architecture: Centralized vs. Distributed

In centralized algorithms, a main controller is responsible for the updating of all the node routing tables and/or for every routing decision. Centralized algorithms can be used only in particular cases and for small networks. In general, the controller has to gather information about the global network status and has to transmit all the decisions/updates. The relatively long time delays necessarily involved with such activities, as well as the lack of fault-tolerance (if not at the expenses of redundant duplications), make centralized approaches unfeasible in practice. From now on only non-centralized, that is, distributed routing systems are considered. In distributed routing systems, every node autonomously decides about local data forwarding. At each node a local routing table is maintained in order to implement the local routing policy. The distributed paradigm is currently used in the majority of network systems.

b) Types of routing tables: Static vs. Dynamic

Routing tables can be statically assigned or dynamically built and updated. It is evident that the performance of the two approaches can be radically different, and the appropriateness of one approach over the other tightly depends on the characteristics of the network scenario under consideration.

In both cases routing tables are built in order to possibly optimize some network-wide criteria which are made depending in turn on costs associated to network elements. That is, to each link, or whatever network resource of interest (e.g., available processing power of a routing node), a value (integer, real, nominal, etc.), here called cost, is assigned according to some metric in order to have a measure of either utilization level or physical characteristics (e.g., bandwidth, propagation delay). Therefore, the process of finding routing paths optimized with respect to the chosen criteria can be actually intended as the minimization process with respect to the defined costs (e.g., the overall cost criterion can be expressed in terms of a sum of the link costs or of the path/link flows). If trusting information about the incoming traffic patterns is available, then an optimal routing approach (i.e., a multi-commodity flow formulation) can be used to actually carry the minimization, otherwise other approaches, like those based on independent shortest path calculations, are called for.

Static routing: In static (or oblivious) routing systems, the path to forward traffic between pairs of nodes is determined without regard to the current network state. The paths are usually chosen as the result of the offline optimization of some selected cost criterion. Once defined the paths to be used for each source-destination pair, data are always forwarded along these paths.

Costs and accordingly, routing tables, are assigned either by an operator or through automatic procedures independently from the current traffic events. The use of the links' physical characteristics is one of the simplest ways to assign static link costs (e.g., a link with characteristics of high bandwidth and low propagation delay will have associated a low cost). For instance, the cost default value of a link for the Internet intra-domain protocol Open Shortest Path First (OSPF) [55, 54] as automatically assigned by most CISCO routers is 108 /b, with b being the unload bandwidth of the link [56].

Routing tables can be also assigned on the basis of some a priori knowledge about the expected input traffic. For instance, traffic statistics can be periodically recorded, and if some regularity can be spot, these can be used in turn to model the incoming traffic and assign the routing tables as the result of optimal routing calculations.

Dynam ic routing: Dynamic (or adaptive) routing goes beyond static routing by admitting the possibility of building/changing the routing tables online according to the current traffic events. It is useful to distinguish between the ability of adapting to the changing traffic conditions and to topological modifications (e.g., link/node failures, link/node addition/removal).

Topological adaptivity is in a sense more fundamental. It is not reasonable to think that every resource addition/removal should be explicitly notified by the human operator. Instead, is a minimal requirement to ask the distributed routing system to have the ability to automatically get aware of such modifications? This is what actually happens in most of the currently used routing protocols. Clearly, different protocols react in different way to such events. For instance, Bellman-Ford algorithms, since they do not make explicit use of global network topology and only use the notion of distance, suffer the problem of the so-called counting-to-infinity, that is, when a link becomes suddenly unavailable, in the worst case it might take infinite time to adjust the routing tables accordingly.

On the other hand, the most common intra-domain routing protocol, OSPF [55], is a shortest path algorithm based on topology broadcast and is able to be fully and efficiently adaptive with respect to topological modifications. However, OSPF is not really adaptive with respect to traffic modifications, such that link costs are static, and may change only when network components become unreachable or new ones come up.

As another example, the Enhanced Interior Gateway Routing Protocol (EIGRP), which is the CISCO's proprietary intra-domain protocol, is an extension of the Bellman-Ford based on the DUAL algorithm [34], such that it overcomes the counting-to-

infinity problem and uses link costs which are dynamically assigned according to the following formula:

$$C = \left[k_1 B + \frac{k_2}{256-L} + k_3\right] \frac{k_5}{R-k_4} \quad (1)$$

Where k_i, i = 1, . . . , 5 are constants, L is the link load assigned as an integer over a scale going from 1 to 255. D is the topological delay, that is, the amount of time it takes to get to the destination using that link in case of unloaded network. R is the reliability of the path expressed as the fraction of packets that will arrive at destination undamaged and $B = 10^7 / \min_i b_i$, where b_i is the bandwidth of path to destination. The parameters B and D are defined during the router configuration, while L and R are estimated through measurements. However, the default link cost is also defined as C = B + D.

Generally speaking, adaptivity to traffic events is commonly obtained by monitoring local resource utilization (usually in terms of link costs), building up statically estimates of these costs, using these costs to update the local routing table and possibly exchanging this information with other nodes in order to allow some form of dissemination of fresh local information. The nature of the local statistical information and the modalities of information exchange characterize the different algorithms.

Adaptive routers are, in principle, the most attractive ones, because they can adapt the routing policy to varying traffic conditions. As a drawback, they can cause oscillations and inconsistencies in the selected paths, and, in turn, these can cause, circular paths, as well as large fluctuations in measured performance. Stability and inconsistency problems are more evident for connection-less than for connection-oriented networks. The problems with adaptive routing are well captured by the following sentence, slightly changed from the original citation: Link arrival rates depend on routing, which in turn depends on arrival rates via routing selected paths, with a feedback effect resulting.

Intuitively, the general non stationarity of the traffic patterns, as well as the above feedback effect, generate non-trivial problems of parameters setting in any adaptive algorithm. If the link costs are adaptively assigned in function of the locally observed traffic flows, which is, for instance, the amount of the variation in the traffic flows that should trigger an update of the link costs and in turn of the routing table. Should every update trigger a transmission of the new costs/routing table to other nodes in the network. In general, every answer to these questions will contain some level of arbitrariness. In fact, the values assigned to the parameters of the algorithm define the tradeoff between reactivity to local traffic changes and stability in the overall network response.

c) Optimization criteria: Optimal vs. Shortest paths

Shortest path routing is the routing paradigm most in use in real networks. In shortest path routing the optimizing strategy for path flows consists in using the minimum cost paths connecting all the node pairs in the network, where the paths are calculated independently for each pair. That is, shortest path routing adopts a per pair perspective. On the other hand, optimal routing, which is the other main reference paradigm (at least from a theoretical point of view), has a network-wide perspective, since the path flows are calculated considering all the incoming traffic sessions. Clearly, in order to adopt such a global strategy, optimal routing requires the prior knowledge of the statistical characteristics of all the incoming flows, a requirement which is usually quite hard to satisfy.

According to an optimization perspective, a more coarse-grained distinction can be also made between minimal and non-minimal routing algorithms. Minimal routers allow packets to choose only paths which are minimal with respect to some cost criterion, while in non-minimal algorithms packets can be forwarded along any of the available paths according to some heuristic decision strategy [9]. Both optimal and pure shortest path routing implement minimal routers. On the other hand, ACO algorithms for routing are not minimal, due to the presence of stochastic components playing a major role in decision-taking.

d) Load distribution

Data traffic toward the same destination d can be forwarded along always the same link or it can be spread along multiple paths. Actually, when routing tables are updated being adaptive to traffic patterns, the resulting effect can be that of actually spreading the data packets toward the same destination over multiple paths at the same time, if the updating interval is shorter than or comparable to the inter-arrival time of the packets directed to d. However, this is a quite particular and unlikely case, while, more precisely:

Multipath and alternate path routing: With multipath routing is intended the situation in which multiple next hop entries for the same destination are maintained in the routing table and used to forward data according to some (usually distance-proportional) scheme.

On the other hand, alternate routing is the situation in which information about multiple paths is maintained in the routing table but is used only as a backup in the case the primary path becomes unavailable because of failure or suddenly congested such that its quality scores poorly.

Multipath routing can be effectively visualized in the terms of defining through the distributed routing tables, instead of a collection of single paths between

each source and destination, a directed, possibly acyclic, graph rooted at the destination. Figure 5.2 graphically shows the situation. The directed links represent the available routing alternatives for packets bound for d according to the local routing tables. The leftmost graph shows a global distributed assignment of the routing tables that results in multiple loop-free paths connecting each source s_i, i = 1, 2, 3 to the destination d. The rightmost graph shows the routing table assignment that would result from a single-path shortest path routing algorithm. It is evident the difference in resources utilization in the two cases. With the single-path policy only three links are actually going to be used to forward packets toward d. This means that if the traffic rate at one of the three sources is higher than the bandwidth of the single link, either packet must be dropped or they will incur high delays. In the multipath case, the effective bandwidth available to each source is much higher, and the whole network bandwidth can be fully exploited through statistical multiplexing of link access. Clearly, in the case of lightly loaded network, when for instance the bandwidth of each single link is able to carry to whole traffic of each source, the single-path assignments will provide the best performance in terms of both maximal throughput and minimal end-to-end delays.

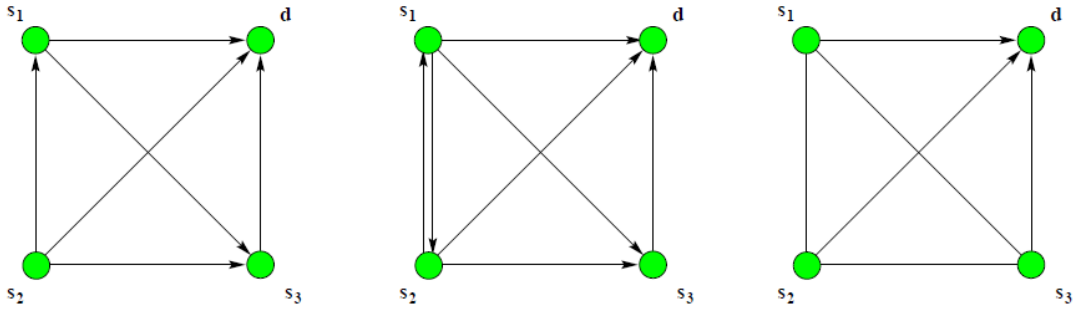


Figure 2 : Multipath routing from sources s_i, i = 1, 2, 3 to destination d

In the figure 2 the directed links show the possible routing decisions that are available at nodes for a packet bound for d according to their routing tables. The links are assumed to have all the same unit cost. The leftmost graph shows a routing policy which is globally loop-free independently from the specific policy adopted to locally spread the data along the different links. That is, the combination of the routing policies of all the nodes defines a directed acyclic graph rooted in d. The middle graph shows an assignment of the routing tables which can give rise to packet looping between $s_1$and s_2, depending on the specific utilization of the local multiple alternatives as a function, for instance, of the distance to the destination. If the distances/costs are calculated in a wrong way, possibly because of traffic fluctuations, is easy to incur in packet looping in this case. The rightmost graph shows the assignment of the routing tables resulting from a single-path shortest path calculation [8].

The multipath solution will likely show also maximal throughput, but the end-to-end delays will be worse than those of single-path since some packets will be forwarded along routes that are longer than one hop. The middle graph of the figure points out another potential drawback in multipath routing: loops can easily arise because of "wrong" composition of the local routing policies. In the case of the figure, packets can bounce between s_1 and s_2 according to the policy adopted to spread data over the available multipath and to the costs that are assigned to the different links in the perspective of reaching d.

There are the three key design issues in multipath routing protocols [7]: (i) how many paths are needed, (ii) according to which criterion these paths are selected, (iii) which data distribution policy is adopted to use the selected paths. Issues (i) and (ii) are by far the most important ones since determine the final performance of the algorithm.

Regarding (i), is clear that the optimal answer would depend on the characteristics of the both the network and traffic. However, the general target is to get good load balancing while using a low number of paths. In fact, a high number of paths bring more complexity in the management of the routing tables and increases at the same time the probability of packet looping.

The criteria to select the paths referred in point (ii) differ from network to network. Paths might be selected not only according to their quality in the sense of distance/cost to the destination, but also according to other features, like the level of node and/or edge disjointness. Disjoint paths are in principle the most appealing ones, since they allow an effective and not interfering distribution of the load. On the other hand, the need for disjointness is strictly related to the packet production rate of the traffic sources. For low rates (inferior to the links' bandwidths) it might be not really necessary to search for disjoint paths since packets for the same destination will likely not interfere along the common parts of the followed paths. On the other hand, this might be the case for destinations which are hot spots and concentrates high rates of traffic from several sources. The issue of disjointness is particularly

important in the case of connection oriented networks providing quality of service, since disjointness means also increased robustness to failures for the single session: if multiple paths toward the same destination share several networks elements, the failure of one of these elements will cause the breakdown of the whole bundle of paths and consequently of the QoS session. Disjointness is even a more critical issue in the case of mobile ad hoc networks. In fact, in presence of high rates of data generation the use of multiple paths can be effective only if the paths are radio-disjoint. If this does not happen, packets from the same session hopping between different nodes situated in the same radio range will likely generate MAC-level collisions when accessing the shared radio channel. As a result, the use of multiple paths can in principle dramatically bring down the performance, instead of boosting it. In general quite difficult to identify disjoint paths. This is true in particular for mobile ad hoc networks, because of the highly dynamic conditions, and in connection-less networks, like the IP networks, since every routing table is built according to a local view and routing decisions are taken independently at each node, while it might be quite straightforward to do in connection-oriented networks. Referring to the last considered point (iii), the policies adopted to spread data on the available paths usually follow a proportional approach based on the estimated cost/quality of the paths. That is, each link is used for a destination proportionally to the estimated quality of the associated path toward that destination. This is the approach followed for instance in the Optimized MultiPath (OMP) [9] scheme, in which link load information is gathered dynamically. On the other hand, the Equal Cost MultiPath (ECMP) strategy [5] adopted by OSPF on the Internet, consists in considering only the set of paths with equal (best) quality and distributing the traffic evenly among them. In variance-based approaches [6] if J_{min} is the cost associated to the best path among the locally known ones, then all paths whose cost is $\leq vJ_{min}$, $v \geq 1$, are used for routing, depending on the specific value of the "variance" parameter v. In EIGRP the traffic is split over these paths proportionally to their metric.

The use of multipaths appears as particularly appealing in the case of QoS networks, since it can bring significant advantages during both the connection setup phase, when the requested resources must be found and reserved, and the data communication phase. In fact, at setup time, multiple concurrent reservation processes can be used for the same session [16], such that (a) the search can be speed up since multiple paths are tried out at the same time, (b) a failure in one or more of the processes does not affect the others, and (c) if several routes are made available for reservation the most appropriate one(s) can be selected. During the session running time, the availability of multiple paths can allow an easier recovering from link or node failures, as well as the shifting and/or splitting of the connection flow over other paths in order to gracefully adapt the load distribution and possibly minimizing the blocking probability for the forthcoming sessions. The positive features provided by the use of multipath routing at setup time suggest that it can play an important role especially to allocate bursty applications, as it is also confirmed by theoretical analysis in [7]. Interestingly, also the theoretical analysis in [6, 7], which refers to the use of multipath for best-effort routing in the IP networks, suggests that multipath can bring significant advantages to deal with bursty connection (while the long-lived connections, which account for the majority of the Internet traffic, preferentially should not be split over multiple paths).

A potential drawback of adopting a multipath strategy consists in the fact that if the data packets of the same traffic session are spread over different multiple paths, each associated to a possibly different traveling time, packets will likely arrive at destination out-of-order, creating problems to the transport protocol. For instance, facing such a situation, a TCP-like algorithm could easily get wrong and start asking for packet retransmissions while packets are just arriving out-of-order and slightly time-shifted. A solution to this problem could consist in hashing at the routing layer of each intermediate node the TCP connection identifiers (source and destination IP addresses) of each received packet in order to determine the next hop [56, 78]. In this way, packets from the same source/application are always forwarded along the same outgoing link, while the overall load is however balanced since different TCP connections are routed along possibly different links. This solution has the drawback that in case of few long-lived heavy loaded traffic sessions, network utilization can be result quite close to the single-path case, losing in this way the possibly advantages of using a multipath protocol. Moreover, if the number of traffic sessions is high, the memory requirements necessary to keep trace of all the hashed values might result unfeasible (at least for most of the current commercial routing boxes which are equipped with a limited small amount of memory). In more general terms, one might think that if multipath routing is used then the transport layer algorithms should be consequently adapted in order to fully exploit the potentialities of using multipath at the routing layer.

III. Optimal and Shortest Path Routing

Shortest path routing is the most popular form of routing strategy in current data networks. Therefore, it is customary to review in detail the characteristics of this class of algorithms. On the contrary, optimal routing algorithms are extremely important from a theoretical point of view, since they provide a solution which is globally optimal.

a) Optimal routing

Optimal routing has a network-wide perspective and its objective is to optimize a function of all individual link flows. Optimal routing models are also called flow models because they try to optimize the total mean flow on the network. They can be characterized as multi commodity flow problems, where the commodities are the traffic flows between the sources and the destinations, and the cost to be optimized is a function of the flows, subject to the constraints of flow conservation at each node and positive flow on every link. Obviously, the flow conservation constraint can be explicitly stated only if the arrival rate of the input traffic is known and if no packets can be dropped. The routing policy consists of splitting any source-target traffic pair at strategic points, then shifting traffic gradually among alternative routes. This usually results in the use of multiple paths for a same traffic flow between the same origin-destination pair and in conditions of load balancing.

The multi commodity flow model of an optimal routing problem is solved with respect to the so-called path flow variables x_p :

$$min \sum_{<i,j>} G_{ij} \left[\sum_{\substack{all\ paths\ p \\ containin\ g<i,j>}} x_p \right]$$

$$\sum_{p \in P_w} x_p = r_w, \qquad \forall w \in W$$

$$x_p \geq 0 \qquad \forall p \in P_w, w \in W \qquad (2)$$

Where W is the set of all origin-destination pairs in the network, r_w is the known input traffic rate of the origin-destination pair w ∈ W, and P_w is the set of all directed paths that can connect the w's origin-destination nodes. G_{ij} is the cost function associated to the data flow on the link <i, j>. The overall function to minimize is the sum of all these G_{ij}, that is, a function of the overall cost associated to all the assigned path flows x_p. The form of G_{ij} is left uninstantiated in the formula. According to the different characteristics of the network and of the provided services, each G_{ij} can be chosen in a variety of different ways. If multiple conflicting objectives have to be taken into account, it might result quite hard to define an additive function $G = \Sigma G_{ij}$ which is able to capture all of the objectives. In general terms, it is preferred to choose a functional form of G such that the problem can be solved with analytical methods, usually by derivation operations. A common choice for G consists in:

$$G_{ij}(F_{ij}) = \frac{F_{ij}}{C_{ij} - F_{ij}} + d_{ij} F_{ij}, \qquad (3)$$

Where the C_{ij} are related to the capacity of the link, the d_{ij} are the propagation delays, and F_{ij} is the flow through the link < i, j >. According to this formula, the cost function becomes the average number of packets in the network under the hypothesis, usually not valid in real networks that each queue behaves as an M/M/1 queue of packets. However, when formula 5.3 is used and under the M/M/1 hypothesis, the sum of the G_{ij} is the total delay experienced by data packets. Gallager proposed an algorithm to carry out these computations in a distributed way while ensuring also loop-freedom at every instant. Unfortunately, the algorithm critically depends on a global step-size parameter which depends in turn on the specific characteristics of the input traffic patterns. Such that the algorithm of Gallager can be used in practice only to provide lower bounds under stationary traffic. The cost function G can be also alternatively expressed not as a sum of functions G_{ij}, but also, for example, as a max-norm:

$$G = \max_{<i,j>} \left\{ \frac{F_{ij}}{C_{ij}} \right\},$$

However, in these cases it is usually more difficult to solve the problem analytically.

b) Shortest path routing

Shortest path routing has a single origin-destination perspective. The path between each node pair is considered in isolation from the paths for all the other pairs. In this sense, the shortest path perspective is opposed to that of optimal routing, which makes use of a cost function of the flows of all the origin-destination pairs considered altogether. No a priori knowledge about the traffic process is required, although such knowledge can be fruitfully used, when available.

Main characteristic of shortest path routing: In shortest path algorithms, at each node s, the local link which is on the minimum cost path to the destination d, for all the possible destinations d in the network is identified and used to forward the data traffic directed to d. The minimum cost path is calculated without taking into account the paths for the other destinations. That is, the path for each destination is treated as an entity independent from the paths (i.e., the paths flows) for all the other destinations. This is in contrast with the optimal routing approach that allocates each flow minimizing a joint function of all the flows in the network. The general common behavior of most implementations of shortest path algorithms is informally described in Algorithm 2:

At each network node:

1. Assign a cost to each one of the out links. The cost can be either static or adaptive; in the following it is assumed the most general case of adaptive link costs.
2. Periodically, and without the need for inter-node synchronization, transmit to the neighbors either estimates about cost and status (on/off) of the attached links, or some other information related to the estimated distance/delay from the node to the other known nodes in the network.
3. Upon receiving fresh information from a neighbor, update the local routing table and local information database (i.e., the local view of the global network status). The routing tables are updated in order to associate to each destination the out link that satisfies the conditions of minimum cost path. That is, for each network destination d, the out link belonging to the minimum cost path to reach d will be used to route data traffic bounded for d. The computation of the minimum cost paths is executed on the basis of the locally available information only.
4. The received information packet, and/or the updated routing information, can be in turn also forwarded to the neighbors, which might further forward it.
5. Data routing decisions are made according to a deterministic greedy policy by always choosing the link on the minimum cost path.
6. Asynchronously and concurrently with the other nodes repeat the previous activities over time.

Algorithm 2: General behavior of shortest path routing algorithms.

The general scheme of Algorithm 2 mainly addresses single-path algorithms. Multipath implementations can be realized by building and maintaining at each node information about more than one path toward each destination. Accordingly, the routing decisions at point 5 can be such that either all the equally good paths are considered for use, or also non-minimal strategies are adopted, such that a set of the n best paths are used in some way.

According to the different contents of the routing tables, shortest path algorithms can be further subdivided in two major classes termed distance-vector and link-state [2]. The following two subsections are devoted to the description of the characteristics specific to each class.

i. *Distance-vector algorithms*

In distance-vector algorithms, each node n maintains a matrix $D_d^n(i)$ of distance estimates for each possible network destination d and for each possible choice of next node i, where i ∈ N(n), the set of neighbor nodes of n. These distance estimates are used to build up the vector SD_{nd} of the shortest distances to d, which, in turn, is used to implement routing decisions. Hereafter, distance is to be intended in a general sense as an additive cost-to-go to reach the destination node. Figure 5.3 shows all the components of generic distance-vector schemes.

The stored topological information is represented by the list of the known nodes identifiers. The average memory occupation per node is of order O(Nn), where N is the number of nodes in the network and n is the average connectivity degree (i.e., the average number of neighbor nodes considered over all the nodes). Distance-vector algorithms forward a packet with destination d along the local link belonging to the path associated with the shortest estimated distance SD_{nd} to d. Therefore, the central component of the algorithm is the distributed computation of such minimum cost paths using the locally available topological description of the network, the costs-to-go received from the neighbors, and the local distance to the neighbors.

The framework of the distributed (asynchronous) dynamic programming provides and optimal and efficient way of carrying out the required computations given the topological description available at each node. The basic idea is the association of each node with a state of a DP backward algorithm. The value of each state n for each destination d, is the estimated shortest distance SD_{nd} from n to d. Link choices correspond to state actions. The resulting algorithm, the basic distributed Bellman-Ford algorithm (DBF) [4, 33], works in an iterative, asynchronous and distributed way. Every node n assigns, in a static or dynamic way, a cost to its local links.

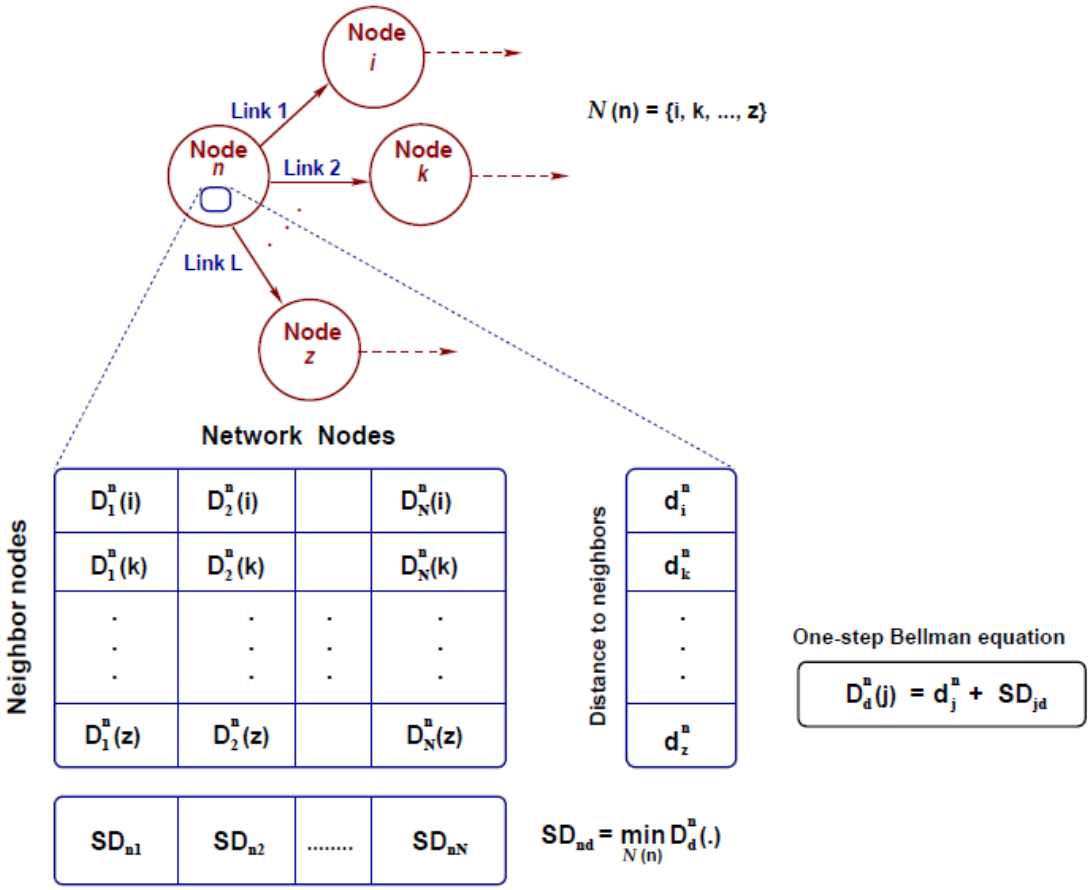


Figure 3 : Data structures and basic equations used in distance-vector algorithms

On the basis of this cost, the cost to travel (the "distance") d_i^n to each of the physically connected neighbors i ∈ N(n) is consequently defined. This one-step distance is used, in turn, within a one-step Bellman equation in order to compute/estimate the traveling distance to each one of the possible destinations d in the network for each one of the local next hops i:

$$D_d^n\ (i) = d_i^n + SD_{id} \quad (4)$$

Once the entries of the matrix D are set up, the vector SD of the shortest distances from n is set up accordingly:

$$SD_{nd} = \min_{j \in N(n)} \left[d_j^n + SD_{jd} \right] \quad (5)$$

The routing table is defined at the same time as the vector SD: for each destination d the chosen next hop node is the one minimizing the equation 5.5 used to compute SD.

Clearly, each node n, in order to compute the matrix of the estimates D, in addition to the locally estimated value d_i^n, needs to know the values SD_{id} from all its neighbors i ∈ N(n). This is the critical part of the distributed algorithm. At the beginning of the operations, the matrix D and the vector SD are initialized all over the network nodes with the same arbitrary values. Then, at each node n, when either the local cost estimates are updated, or an updated value of SD is received from one of the neighbors, the Equations 4 and5 are re-computed, the routing table is updated, and the possibly new value of SD_{nd} is sent, in turn, to all its neighbors. Iterating this distributed asynchronous behavior over the time, after a transitory phase, the distance estimations at each node converge to the correct minimum values with respect to the used cost metric. More precisely, the algorithm always converges and converges fast if the link costs, that is the distances d to the neighbors, are either stationary or decrease [3]. On the other hand, convergence is not anymore assured if link costs increase, or, when link failures result in network partitions the algorithm never convergence. This is the well-know problem of counting-to-infinity, which results from the fact that it might happen that using the distance communicated by a neighbor, a node computes in turn its distance to a destination on the basis of the length of the path passing through itself. Clearly, the node using this "circular" distance is unaware of the circularity since nodes only exchange distance and no path information.

IV. Conclusion

All the adaptive algorithms considered in the chapter gather traffic load information only according to a passive strategy. That is, it is common practice to monitor at the nodes the load associated to each attached link in order to update statistics that are in turn used either to compute distances or are broadcast to the other nodes. On the other hand, there is no notable example of gathering information according to also an active strategy. For example, by generating an agent and sending it into the network with the purpose of collecting some useful information about a well defined resource or destination.

Taking into account all the aspects discussed so far, it is possible to compile a sort of wish list for the design characteristics of novel routing algorithms, that are expected to: (i) be traffic adaptive, (ii) make use of multipaths, (iii) integrate both forms of collective rationality and continual and graceful adaptation of the routing policy, (iv) show robustness with respect to parameter setting, with possible self-tuning of the parameters in order to adapt to the characteristics of the specific network scenario, (v) limit loop formation, or at least ensuring that loops are very short-lived, (vi) possibly not fully rely on information bootstrapping or broadcasting, in order to obtain more robustness under dynamic and near saturation conditions, while at the same time providing at least near-optimal performance under static and low load conditions, (vii) make use of stochastic components in order to be more robust to the lack of global up-to-date information at the nodes, (viii) implement some form of (pro)active information gathering to complement passive information gathering one, while at the same time limiting the associated routing overhead. Our ACO algorithms for routing have been precisely designed according to these guidelines, resulting in novel traffic-adaptive algorithms for stochastic multipath routing.

Bibliography

1. T. Abe, S. A. Levin, and M. Higashi, editors. Biodiversity: an ecological perspective. Springer-Verlag, New York, USA, 1997.
2. M. Beckmann, C.B. McGuire, and C.B. Winstein. Studies in the Economices of Transportation. Yale University Press, 1956.
3. R. Bellman. Dynamic Programming. Princeton University Press, 1957.
4. R. Bellman. On a routing problem. Quarterly of Applied Mathematics, 16(1): 87–90, 1958.
5. D. Bertsekas, J. N. Tsitsiklis, and Cynara Wu. Rollout algorithms for combinatorial optimization. Journal of Heuristics, 3(3):245–262, 1997.
6. M. Birattari, G. Di Caro, and M. Dorigo. Towards the formal foundation of ant programming. In M. Dorigo, G. Di Caro, and M. Sampels, editors, Ants Algorithms - Proceedings of ANTS 2002, Third International Workshop on Ant Algorithms, Brussels, Belgium, September 12–14, 2002, volume 2463 of Lecture Notes in Computer Science, pages 188–201. Springer-Verlag, 2002.
7. J.A. Bland. Optimal structural design by Ant Colony Optimization. Engineering optimization, 33: 425–443, 2001.
8. J.A. Bland. Layout of facilities using an Ant System approach. Engineering optimization, 32(1), 1999. [38] J.A. Bland. Space-planning by Ant Colony Optimization. International Journal of Computer Applications in Technology, 12, 1999.
9. K. Bolding, M. L. Fulgham, and L. Snyder. The case for chaotic adaptive routing. Technical Report CSE-94-02-04, Department of Computer Science, University of Washington, Seattle, 1994.
10. E. Bonabeau, M. Dorigo, and G. Theraulaz. Swarm Intelligence: From Natural to Artificial Systems. Oxford University Press, 1999.
11. J. Broch, D.A. Maltz, D.B. Johnson, Y.C. Hu, and J. 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), 1998.
12. D. Camara and A.F. Loureiro. Gps/ant-like routing in ad hoc networks. Telecommunication Systems, 18(1–3):85–100, 2001.
13. H.S. Chang, W. Gutjahr, J. Yang, and S. Park. An Ant System approach to Markov Decision Processes. Technical Report 2003-10, Department of Statistics and Decision Support Systems, University of Vienna, Vienna, Austria, September 2003.
14. C. Cheng, R. Riley, S.P. Kumar, and J.J. Garcia-Luna-Aceves. A loop-free extended bellman-ford routing protocol without bouncing effect. ACM Computer Communication Review (SIGCOMM '89), 18 (4):224–236, 1989.
15. L. Chrisman. Reinforcement learning with perceptual aliasing: The perceptual distinctions approach. In Proceedings of the Tenth National Conference on Artificial Intelligence, pages 183–188, 1992.
16. I. Cidon, R. Rom, and Y. Shavitt. Multi-path routing combined with resource reservation. In IEEE INFOCOM'97, pages 92–100, 1997.
17. I. Cidon, R. Rom, and Y. Shavitt. Analysis of multi-path routing. IEEE/ACM Transactions on Networking, 7(6):885–896, 1999.
18. Colorni, M. Dorigo, V. Maniezzo, and M. Trubian. Ant system for job-shop scheduling. Belgian Journal of Operations Research, Statistics and Computer Science (JORBEL), 34:39–53, 1994.
19. M. Cottarelli and A. Gobbi. Estensioni dell'algoritmo formiche per il problema del commesso via

ggiatore. Master's thesis, Dipartimento di Elettronica e Informazione, Politecnico di Milano, Italy, 1997.
20. J.-L. Deneubourg, S. Aron, S. Goss, and J.-M. Pasteels. The self-organizing exploratory pattern of the argentine ant. Journal of Insect Behavior, 3:159–168, 1990.
21. J.L. Deneubourg, S. Goss, N. Franks, A. Sendova-Franks, C. Detrain, and L. Chretien. The dynamics of collective sorting: robot-like ants and ant-like robots. In S. Wilson, editor, Proceedings of the First International Conference on Simulation of Adaptive Behaviors: From Animals to Animats, pages 356–365. MIT Press, Cambridge, MA, USA, 1991.
22. G. Di Caro and M. Dorigo. AntNet: A mobile agents approach to adaptive routing. Technical Report 97–12, IRIDIA, University of Brussels, Belgium, June 1997.
23. G. Di Caro, F. Ducatelle, and L.M. Gambardella. AntHocNet: an ant-based hybrid routing algorithm for mobile ad hoc networks. In Proceedings of Parallel Problem Solving from Nature (PPSN) VIII, volume 3242 of Lecture Notes in Computer Science, pages 461–470. Springer-Verlag, 2004.
24. G. Di Caro, F. Ducatelle, and L.M. Gambardella. AntHocNet: an adaptive nature-inspired algorithm for routing in mobile ad hoc networks. European Transactions on Telecommunications, 16(5), October 2005.
25. E. W. Dijkstra. A note on two problems in connection with graphs. Numerical Mathematics, 1:269–271, 1959.
26. M. Dorigo, G. Di Caro, and L. M. Gambardella. Ant algorithms for discrete optimization. Artificial Life, 5(2):137–172, 1999.
27. J.J. Garcia-Luna-Aceves and S. Murthy. A path-finding algorithm for loop-free routing. IEEE/ACM Transactions on Networking, February 1997.
28. F. Glover. Tabu search, part I. ORSA Journal on Computing, 1:190–206, 1989.
29. J. Moy. OSPF version 2. Request For Comments (RFC) 1583, Network Working Group, 1994.
30. J. Moy. OSPF Anatomy of an Internet Routing Protocol. Addison-Wesley, 1998.
31. G. Owen. Game Theory. Academic Press, third edition, 1995.
32. M.L. Puterman. Markov Decision Problems. John Wiley & Sons, 1994.
33. Rome, Kay, and Friedemann Mattern. The design space of wireless sensor networks. IEEE Wireless Communications, 11(6):54–61, December 2004.

This page is intentionally left blank

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 12 Issue 11 Version 1.0 June 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Comparative Study of Gaussian and Nearest Mean Classifiers for Filtering Spam E-mails

By Upasna Attri & Harpreet Kaur
Punjab Technical University, Jalandhar India

Abstract - The development of data-mining applications such as classification and clustering has shown the need for machine learning algorithms to be applied to large scale data. The article gives an overview of some of the most popular machine learning methods (Gaussian and Nearest Mean) and of their applicability to the problem of spam e-mail filtering. The aim of this paper is to compare and investigate the effectiveness of classifiers for filtering spam e-mails using different matrices. Since spam is increasingly becoming difficult to detect, so these automated techniques will help in saving lot of time and resources required to handle e-mail messages.

Keywords : *Data-mining, Machine Learning, Classifiers, Filtering, spam E-mails.*

GJCST-E Classification: *H.1.0*

Strictly as per the compliance and regulations of:

Comparative Study of Gaussian and Nearest Mean Classifiers for Filtering Spam E-mails

Upasna Attri [α] & Harpreet Kaur [σ]

Abstract - The development of data-mining applications such as classification and clustering has shown the need for machine learning algorithms to be applied to large scale data. The article gives an overview of some of the most popular machine learning methods (Gaussian and Nearest Mean) and of their applicability to the problem of spam e-mail filtering. The aim of this paper is to compare and investigate the effectiveness of classifiers for filtering spam e-mails using different matrices. Since spam is increasingly becoming difficult to detect, so these automated techniques will help in saving lot of time and resources required to handle e-mail messages.

Keywords : Data-mining, Machine Learning, Classifiers, Filtering, spam E-mails.

I. Introduction

The Internet is a global system of interconnected computer networks to serve billions of users worldwide. As of 2011, more than 2.1 billion people – nearly a third of Earth's population – use the services of the Internet. E-mail has become one of the fastest and most economical forms of communication due to minimal costs, reliability, accessibility and speed. Wide usage of e-mail prone to spam e-mails. Spam e-mail is junk or unwanted bulk e-mail or commercial e-mail for recipients. Various problems that exist from spam e-mails are: wastage of network time and resources, damage to computers and laptops due to viruses and the ethical issues like advertising immoral and offensive sites that are harmful to the young generations. It hardly cost spammers to send out millions of e-mails than to send few e-mails, causing financial damage to companies and annoying individual users. Spam filter software can help mitigate this overwhelming chore. No spam filter software is 100% effective. Spam mail can contain viruses, keyloggers, phishing attacks and more. Clearly, a war is waging inside a user's inbox. Deployments of better ways to filter spam e-mails are needed. Several major kinds of classification method including decision tree induction, Bayesian networks, k-nearest neighbor classifier, case-based reasoning, genetic algorithm, fuzzy logic techniques, Neural Network (NN), Support Vector Machine (SVM), and Naïve Bayesian (NB) are showing a good classification result. Among the approaches developed to stop spam, filtering is an important and popular one.

Author α : CSE Department, DAV Institute of Engineering and Technology, Jalandhar, India. E-mail : upasnaa.08@gmail.com
Author σ : CSE Department, DAV Institute of Engineering and Technology, Jalandhar, India. E-mail : harpreet_daviet@yahoo.in

Recently, there is a growing emphasis on investigative analysis of datasets to discover useful patterns, called data mining. Data Mining is the extraction of interesting, valid, novel, actionable and understandable information or patterns from large databases for making decisive business decisions. Classification is a data mining (machine learning) technique used to predict group membership for data instances. Filtering is very important and popular approach to circumvent this problem of spam. For filtering spam e-mails from good ones, clustering technique is imposed as classification method on a finite set of objects. Clustering is the technique used for data reduction. It divides the data into groups based on pattern similarities such that each group is abstracted by one or more representatives.

Classification is a supervised learning method. The aim of classification is to create a model that can predict the 'type' or some category for a data instance that doesn't have one. There are two phases in classification: first is supervision in which the training data (observations, measurements, etc.) are accompanied by labels indicating the class of the observations. Second is prediction in which given an unlabelled, unseen instance, use the model to predict the class label. Some algorithms predict only a binary split (yes/no), some can predict 1 of N classes, and some give probabilities for each of N classes.

Clustering is an unsupervised learning. It is a method by which a large set of data is grouped into clusters of smaller sets of similar data. There are two phases in this method: In first phase the class labels of training data is unknown. Whereas in second phase, given a set of measurements, observations, etc. the aim is to establish the existence of classes or clusters in the data. There are no predefined classes. Besides the term clustering, there are a number of terms with similar meanings, including automatic classification, numerical taxonomy, botryology and typological analysis.

Various criteria to evaluate the best spam filter software as following:

- Blocking/Filtering: must have black and white lists, sensitivity settings, community based filtering, challenge and response techniques, and quarantine settings.

- Protection: must protect the user from e-mail that contains worms, viruses, Trojans, attachments with embedded key loggers and other malware.
- Rules: should give the user the ability to edit predefined rule settings as well as the creation of new rules.
- Compatibility: compatible with their current e-mail client or web-mail service provider.

There are two general approaches to mail filtering:

- Knowledge Engineering (KE)
- Machine Learning (ML).

In the knowledge engineering approach, a set of rules is created according to which messages are categorized as spam or legitimate mail. The major drawback of this method is that the set of rules must be constantly updated, and maintaining it is not convenient for most users. In the machine learning approach, it does not require specifying any rules explicitly. Instead, a set of pre-classified documents (training samples) is needed. A specific algorithm is then used to "learn" the classification rules from this data. The subject of machine learning has been widely studied and there are lots of algorithms suitable for this task.

Some of the existing approaches to solve the problem of spam mails could be listed as follows:

- Rule based: Hand made rules for detection of spam made by experts (needs domain experts & constant updating of rules).
- Customer Revolt: Forcing companies not to publicize personal e-mail ids given to them (hard to implement).
- Domain filters: Allowing mails from specific domains only (hard job of keeping track of domains that are valid for a user).
- Blacklisting: Blacklist filters use databases of known abusers, and also filters unknown addresses (constant updating of the data bases would be required).
- White list Filters: Mailer programs learn all contacts of a user and let mail from those contacts through directly (every one should first be needed to communicate his e-mail-id to the user and only then he can send e-mail).
- Hiding address: Hiding ones original address from the spammers by allowing all e-mails to be received at temporary e-mail-id which is then forwarded to the original e-mail if found valid by the user (hard job of maintaining couple of e-mail-ids).
- Checks on number of recipients:by the e-mail agent programs.
- Government actions: Laws implemented by government against spammers (hard to implement laws).
- Automated recognition of Spam: Uses machine learning algorithms by first learning from the past data available (seems to be the best at current).

II. Statement of the Problem

E-mail has been an efficient and popular communication mechanism as the number of Internet users increase. Therefore, e-mail management is an important and growing problem for individuals and organizations because it is prone to misuse. The blind posting of unsolicited e-mail messages, known as spam, is an example of misuse. Automatic e-mail filtering seems to be the most effective method for countering spam at the moment and a tight competition between spammers and spam-filtering methods is going on: the finer the anti-spam methods get, so do the tricks of the spammers. So, uses of machine learning algorithms are imposed to overcome this problem upto large extent. There is substantial amount of research is going on with machine learning algorithms. It works by first learning from the past data available for training and then used to filter the spam e-mails effectively. In this work, comparison of two machine learning algorithms is conducted. Gaussian and Nearest Mean classifiers are one of the most effective machine learning algorithms. Therefore, Comparison of these two algorithms is proposed to be conducted for investigating the effectiveness to filter the spam e-mails.

III. Objective of Work

The goals of this paper are three fold. (1) To convert the input data as per the requirement of Gaussian and Nearest Mean Classifiers for filtering spam e-mails. (2) To compare and investigate Gaussian and Nearest Mean classifiers for effectiveness of filtering spam e-mails by using Probability of Error (POE). (3) To investigate the effectiveness of Gaussian and Nearest Mean classifiers for filtering spam e-mails by comparing the Time taken for classification.

IV. Related Work

In this technical report (Sahami et al. 1998) developed probabilistic learning methods for filtering spam e-mail using Bayesian network. (Drucker et al. 1999) compared Support Vector Machine (SVM) with Ripper, Rochio and Boosting Decision Tree (classification algorithms) and concluded that Boosting Trees and SVMs had an acceptable performance in terms of accuracy and speed. In his paper (Tretyakov, 2004) compared Machine Learning algorithms i.e. Bayesian, k-Nearest Neighbor (k-NN), Artificial Neural Network (ANN) and SVM and concluded that none of

these algorithms achieve better precision as compared to each other.

In their work (Aery et al. 2005) concluded that structure and content of e-mails in a folder classifies effectively the incoming e-mails. (Kulkarni et al. 2005) in their paper concluded that e-mail messages can be treated as contexts and clustering is based on underlying content rather than occurrence of some specific string. In this technical report (Segal et al. 2005) presented SpamGuru: an anti-spam filtering system for enterprises that is based on three principles: plug-in tokenizers and parsers, plug-in classification modules and machine learning techniques. SpamGuru produces excellent spam detection results. In his work (Zhao C. 2005) combined three classifiers (k-NN, Classical Gaussian and Boosting with Multi-Layer Perceptron) to produce Mixture of Expert (MOE) and concluded that Boosting is effective and also outperforms MOE.

In their journal (Bratko et al. 2006) concluded that compression models outperform currently established spam filters. The nature of the model allows them to be employed as probabilistic text classifiers based on character-level or binary sequences. In his paper (Hoanca B. 2006) concluded that no e-mail control technique is 100% effective. This problem of spam is shifting to other communication medias also in the form of Spam on Instant Messages (SPIM) and in chat rooms (SPAT).

In this journal (Blanzieri et al. 2007) concluded that the feel of antispam protection in by now matured and well developed. But inboxes are full of spam. So, more sophisticated techniques and methods are required to mitigate this problem of spamming. In his paper (Lai C.C. 2007) compared three method (SVM, Naïve-Bayesian (NB) and k-NN) and concluded that NB and SVM outperforms k-NN using header of e- mails only. In their technical report (Youn et al. 2007) compared four classifiers (neural network, SVM, Naïve-Bayesian and J48) and concluded that J48 classifier can provide better classification results for spam e-mail filtering.

In this technical report (Blanzieri et al. 2008) concluded that now situation of spam is tolerable and one can give attention to produce robust classification algorithm. In this report (Sculley et al. 2008) showed the impact of noisy labeling feedback on current spam filtering methods and observed that these noise tolerant filters would not necessarily have achieved best performance.

In this journal (Xiao-Li et al. 2009) proposed spam detection using clustering, random forests and active learning with respect to term frequency and inverse document frequency for messages. (DeBarr et al. 2009) compared six classifiers to treat Arabic, English and mixed e- mails and concluded that features selection technique can achieve better performance than filters that do not used them. El-Halees A. (2009) proposed a semi supervised approach for image filtering and concluded that this approach achieves high detection rate with significantly reducing labeling cost. (Gao et al. 2009) discussed one of key challenges that effect the system which is identifying spammers and also discussed on potential features that describes system's users and illustrate how one can use those features in order to determine potential spamming users through various machine learning models has been done. These proposed features demonstrate improved results as compared to the previous work done on it. In their work (Madkour et al. 2009) improved NB classifiers and concluded better detection rate of precision when compared with some best variants of NB. (Song et al. 2009) When used into spam filtering, the standard support vector machine involves the minimization of the error function and the accuracy of the SVM is very high, but the degree of misclassification of legitimate e-mails is high. In order to solve that problem, a method of spam filtering based on weighted support vector machines. Experimental results show that the algorithm can enhance the filtering performance effectively.

In this paper (Basavraju et al. 2010) proposed a spam detection technique using text clustering based on vector space model and concluded that k-means works well for smaller data sets and BIRCH with k-NN in combination performs better with large data sets. In this paper (Gao et al. 2010) presented a comprehensive solution to image spam filtering which combine cluster analysis of spam images on server side and active learning classification on client side for effectively filtering image spam. In this journal (Nagwani et al. 2010) proposed a weighted e-mail attribute similarity based model for more accurate clustering.

V. Materials and Methods

The Matlab has been used as the programming tool for this simulation experiment. Random samples for each class of e-mail were generated and random partitioning of the samples of each class into two equal sized sets to form a training set and a test set for each class has been done. For each case, estimated the parameters of the Normal density function from the training set of the corresponding class. For each case the estimates of the parameters have been used to determine the Gaussian discriminant function. The Gaussian classifier for spam problem has been developed. The test samples have been classified for each class. For each case, the probability of classification error (POE) has been determined and also the time taken (in seconds) to classify has been measured. Further the nearest mean classifier has been implemented. The test samples of each class have been classified. For each case, the probability of classification error (POE) has been estimated and also the time taken (in seconds) for classification has been measured.

Finally comparison of the two methods for effectiveness against spam based on probability of error and time taken to classify has been conducted.

VI. Results and Discussions

During first execution 50 e-mail messages were generated and classified according to Gaussian and Nearest Mean method. The plot shows the variation of probability of error. It can be seen that the maximum POE is almost 0.108 in the case of Nearest Mean method and mostly the POE of the Gaussian method is generally less than the Nearest Mean method. However at some instances the POE of Gaussian method is more is at the 04th and 15th e-mail message (Fig. 1).

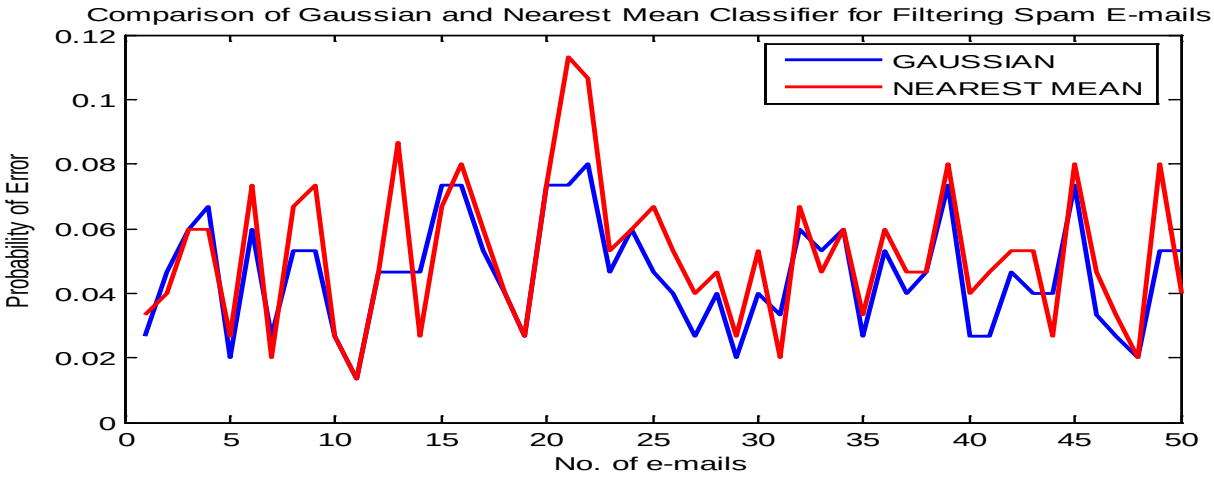


Fig. 1 : The variation of probability of error for 50 E-mails

When 100 e-mail messages were generated and classified according to Gaussian and Nearest Mean method then plot shows the variation of probability of error. It can be seen that the maximum POE is almost 0.087 in the case of Nearest Mean method and mostly the POE of the Gaussian method is generally less than the Nearest Mean method. However at some instances the POE of Gaussian method is more is at the 38th and 76th e-mail message (Fig. 2).

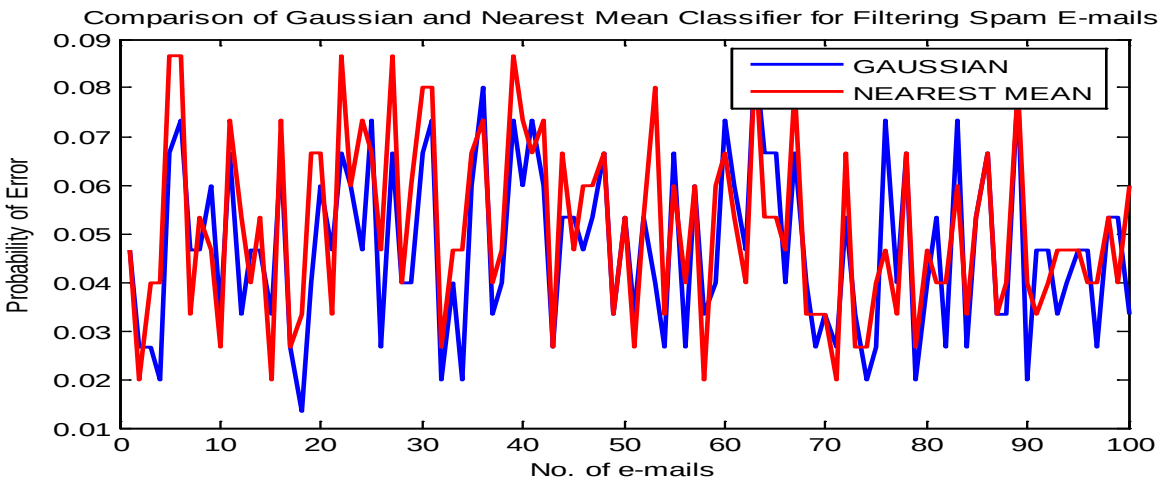


Fig. 2 : The variation of probability of error for 100 E-mails

When 150 e-mail messages were generated and classified according to Gaussian and Nearest Mean method, then plot shows the variation of probability of error. It can be seen that the maximum POE is almost 0.114 in the case of Nearest Mean method and mostly the POE of the Gaussian method is generally less than the Nearest Mean method. However at some instances the POE of Gaussian method is more is at the 40th and 140th e-mail message (Fig. 3).

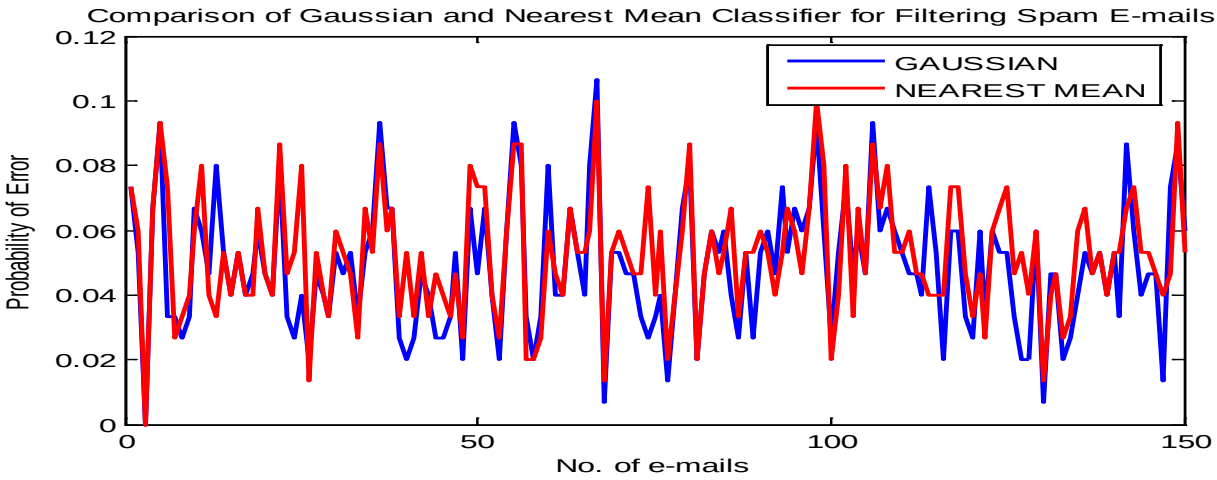


Fig. 3 : The variation of probability of error for 150 E-mails

During fourth execution 200 e-mail messages were generated and classified according to Gaussian and Nearest Mean method. The plot shows the variation of probability of error. It can be seen that the maximum POE is almost 0.104 in the case of Nearest Mean method and mostly the POE of the Gaussian method is generally less than the Nearest Mean method. However at some instances the POE of Gaussian method is more is at the 35th and 109th e-mail message (Fig. 4).

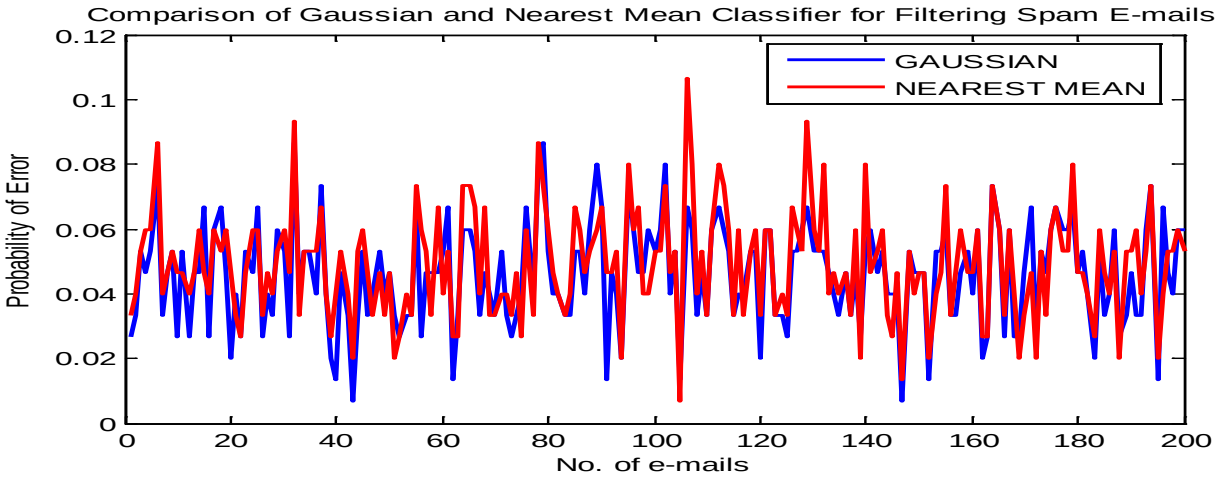


Fig. 4 : The variation of probability of error for 200 E-mails

In the next iteration 250 e-mail messages were generated and classified according to Gaussian and Nearest Mean method. The plot shows the variation of probability of error. It can be seen that the maximum POE is almost 0.117 in the case of Nearest Mean method and mostly the POE of the Gaussian method is generally less than the Nearest Mean method. However at some instances the POE of Gaussian method is more is at the 120th and 240th e-mail message (Fig. 5).

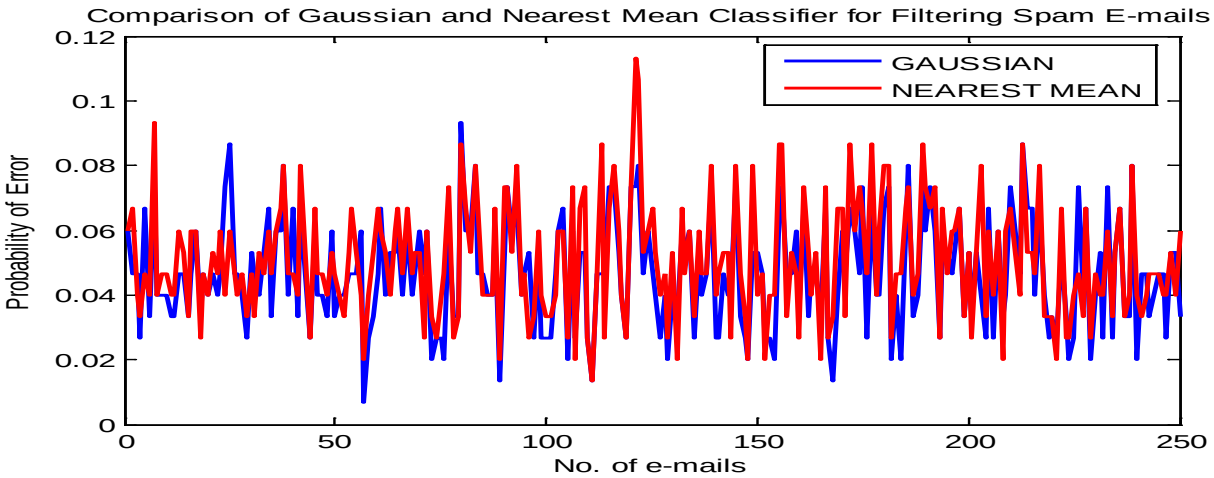


Fig. 5: The variation of probability of error for 250 E-mails

In the next experiment e-mail messages were generated and classified according to Gaussian and Nearest Mean method and the time taken to classify was plotted (Fig. 6). The plot shows that as the load of incoming e-mails increases the Gaussian classifier takes more time than the Nearest Mean classifier.

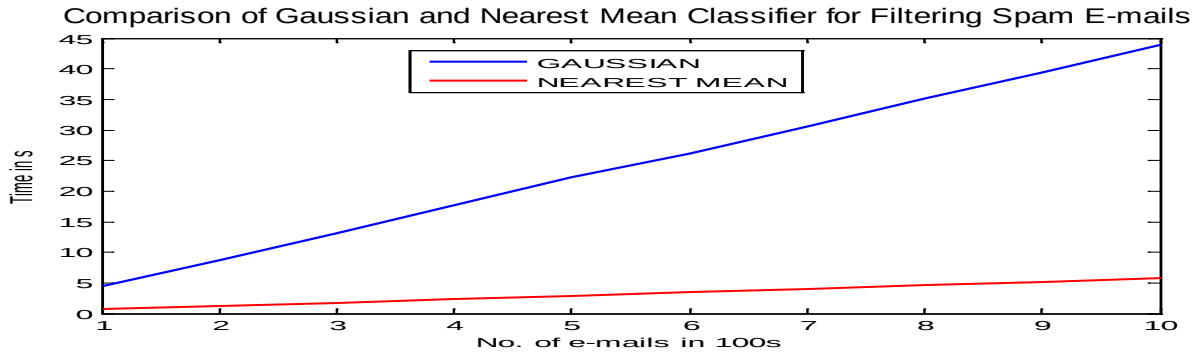


Fig. 6 : Evaluation of Gaussian and Nearest Mean Classifiers for Filtering Spam E-mails in time scale

VII. Comparison and Analysis

It is analyzed from the above results that most of the times Gaussian Classifier performs better (POE is less) than the Nearest Mean Classifier. But still there are few traces of Nearest Mean Classifier showing less POE than Gaussian Classifier (rare cases). To check the overall performance of these two methods, their average of POE is estimated as shown in Table-1

Sr. No.	No. of E-mails	POE (Avg) (Gaussian)	POE (Avg) (Nearest Mean)
1.	50	0.04587	0.05200
2.	100	0.04713	0.05107
3.	150	0.04876	0.05222
4.	200	0.04577	0.04933
5.	250	0.04680	0.05077

Table 1 : Average POE of Gaussian and Nearest Mean classifiers for Filtering Spam E-mails

The table-2 shows the average time taken to filter spam E-mails by Gaussian and Nearest Mean classifiers. It is observed that average time taken by Gaussian classifier is more than the Nearest Mean classifier.

Sr. No.	No. of E- mails	Avg. Time (in sec) Gaussian	Avg. Time (in sec) Nearest Mean
1.	100	0.04524	0.00717
2.	200	0.04391	0.00585
3.	300	0.04373	0.00577
4.	400	0.04403	0.00577
5.	500	0.04449	0.00577
6.	600	0.04368	0.00579
7.	700	0.04372	0.00577
8.	800	0.04408	0.00579
9.	900	0.04376	0.00577
10.	1000	0.04386	0.00578

Table 2 : Average Time Taken by Gaussian and Nearest Mean classifiers for Filtering Spam E-mails

VIII. Conclusion

It can be seen from Fig-1 to Fig-5 that most of the times Gaussian method gives better performance and the POE is less as compared to Nearest Mean method. Still a few times the Nearest Mean method resulted in less POE but these instances are rare. But Table-1 shows that the average Probability of error (POE) of Gaussian Classifier is less (better) than that of Nearest Mean Classifier. From Fig-6 it can be seen that as the load of incoming e-mails increases the Gaussian classifier takes more time than the Nearest Mean classifier. Table-2 shows that the average time taken by Gaussian classifier is more than the Nearest Mean classifier. Since in filtering spam e-mails, more weightage is given to accuracy than the time taken to classify. So, it can be concluded that in filtering spam e-mails the method of Gaussian Classification is better than the Nearest Mean method.

IX. Acknowledgment

The authors are grateful to DAV Institute of Engineering and Technology, Jalandhar (India) for providing continuous support throughout the work.

References Références Referencias

1. Sahami M. (1998), Dumais S., Heckermaan D. and Horvitz E., "*A Bayesian Approach to Filtering Junk-e-mail*", Technical Report, Stanford University and Microsoft Research, Redmond WA.
2. Drucker H. (1999), Donghui W., Vapnil V.N.: "*Support vector machines for spam categorization",* IEEE Transactions, 10(5), pp. 1048-1054.
3. Tretyakov K. (2004), "*Machine Learning Techniques in Spam Filtering*", Data Mining Problem-oriented Seminar, MTAT.03.177, pp. 60-79.
4. Aery M. (2005) Chakravarthy S., "*e-mailSift: E-mail Classification Based on Structure and Content*", supported by NSF grants IIS-0123730, IIS-0097517, IIS-0326505, and EIA-0216500.
5. Kulkarni A. (2005), Pederson T., "*Name Discrimination and E-mail Clustering using unsupervised Clustering and Labeling of Similar context*", 2nd Indian International Conference on Artificial Intelligence- (IICAI-05) pp. 703-722.
6. Segal R. (2005), Crawford J., Kephart J and Leiba B. "*SpamGuru: An Enterprise Anti-Spam Filtering System*", Technical Report, IBM Thomas J. Watson Research Center.
7. Zhao C. (2005), "*Towards better accuracy for Spam predictions*", Technical Report, University of Toronto, Ontario, Canada.
8. Bratko A. (2006), Cormack G.V., Lynam T.R., "*Spam Filtering Using Statistical Data Compression Models*", Journal of Machine Learning Research 7, pp. 2673-2698.
9. Hoanca B. (2006): "*How good are our weapons in spam wars?*" Technology and Society Magazine, IEEE, 25(1), pp. 22-30.
10. Blanzieri E. (2007), Bryl A., "*A Survey of Learning-Based Techniques of E-mail Spam Filtering*", Technical Report, University of Toreto, Italy.
11. Lai C.C. (2007), "*An empirical study of three machine learning methods for spam filtering*", ScienceDirect, Knowledge-Based Systems 20 249–254.
12. Youn S. (2007), McLeod D., "*A Comparative Study for E-mail Classification*", Technical Report, University of Southern California, Los Angeles, CA 90089 USA.
13. Blanzieri E. (2008), Bryl A., "*A Survey of Learning-Based Techniques of E-mail Spam Filtering*", Technical Report, University of Toreto, Italy.

14. Sculley D. (2008), Cormack G.V., "*Filtering E-mail Spam in the Presence of Noisy User Feedback*", Technical Report, Tufts University 161 College Ave. Medford, MA 02155 USA
15. Xiao-Li C. (2009), Pei-yu L., Zhen- fang Z., Ye Q., "*A method of Spam filtering based on weighted support vector machines*'', IEEE Xplore 978-1-4244-3930-0/09
16. DeBarr D. (2009), Wechsler H., "*Spam Detection using Clustering, Random Forests, and Active Learning*", CEAS 2009 – Sixth Conference on E-mail and Anti-Spam.
17. El-Halees A. (2009), "*Filtering Spam E-Mail from Mixed Arabic and English Messages: A Comparison of Machine Learning Techniques*", The International Arab Journal of Information Technology, Vol. 6, No.1, pp. 52-66.
18. Gao Y (2009), Yang M., Choudhary A., "*Semi Supervised Image Spam Hunter: A Regularized Discriminant EM Approach*", ADMA 2009, LNAI 5678, pp. 152–164.
19. Madkour A. (2009) , Hefni T., Hefny A., Refaat K.S., "*Using Semantic Features to Detect Spamming in Social Bookmarking Systems*", Human Language Technologies Group IBM Cairo Technology Development Center, El-Ahram, Giza, Egypt.
20. Song Y. (2009), Kołcz A., Giles C.L., "*Better Naïve Bayes classification for high-precision spam detection*", Softw. Pract. Exper. No. 39: pp. 1003–1024
21. Basavraju M. (2010) Prabhakar R."*A Novel Method of Spam Mail Detection using Text Based Clustering Approach*", International Journal of Computer Applications (0975 – 8887) Volume 5– No.4, pp. 15-26.
22. Gao Y., Choudhary A. and Hua G. (2010), "*A Comprehensive Approach to Image Spam Detection: From Server to Client Solution*", IEEE Transactions on Information Forensics and Security, Vol. 5, No. 4, pp. 826-837.
23. Nagwani N.K. (2010), Bhansali A, "*An Object Oriented E-mail Clustering Model Using Weighted Similarities between E-mails Attributes*",International Journal of Research and Reviews in Computer Science (IJRRCS) Vol. 1, No. 2, pp. 1-6.

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 12 Issue 11 Version 1.0 June 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

An Enhanced QoS Provisioning Approach for Video Streams using Cross Layer Design in IEEE 802.16

By V.R.Azhaguramyaa, S.J.K.Jagadeesh Kumar & M.Venkateshwaran
Sri krishna college of technology, kovaipudhur, coimbatore

Abstract - Wimax networks are increasingly deployed for commercial use because of its high bandwidth. This has necessitated application level changes in QoS provisioning techniques. In this paper, we propose an efficient method at the application layer of the wimax architecture. The video stream is partitioned at the application layer into I, P and B frames. Frames corrupted at receiver are detected using negative acknowledgements received from the physical layer. Probability of Byte Loss (BL) is calculated at physical layer which is used to calculate the redundant data. Redundant data is communicated from PHY layer to application layer via link layer using cross-layer signalling mechanism. Redundant data is piggybacked into the subsequent frame and sent only if BL is less than 0.2. This technique has improved the throughput of the network considerably which is evident from the performance analysis.

Keywords : *Application Layer, Cross layer design, QoS, video streaming, WiMAX.*

GJCST-E Classification: *H.4.3*

Strictly as per the compliance and regulations of:

An Enhanced QoS Provisioning Approach for Video Streams using Cross Layer Design in IEEE 802.16

V.R.Azhaguramyaa [α], S.J.K.Jagadeesh Kumar [σ] & M.Venkateshwaran [ρ]

Abstract - Wimax networks are increasingly deployed for commercial use because of its high bandwidth. This has necessitated application level changes in QoS provisioning techniques. In this paper, we propose an efficient method at the application layer of the wimax architecture. The video stream is partitioned at the application layer into I, P and B frames. Frames corrupted at receiver are detected using negative acknowledgements received from the physical layer. Probability of Byte Loss (BL) is calculated at physical layer which is used to calculate the redundant data. Redundant data is communicated from PHY layer to application layer via link layer using cross-layer signalling mechanism. Redundant data is piggybacked into the subsequent frame and sent only if BL is less than 0.2. This technique has improved the throughput of the network considerably which is evident from the performance analysis.

Keywords : Application Layer, Cross layer design, QoS, video streaming, WiMAX.

I. Introduction

With increasing demands in high-data-rate services and multimedia applications in wireless communications, the IEEE 802.16 standard family and the associated Worldwide Interoperability for Microwave Access (Wi-MAX) forum are developed and formed to support the broadband wireless access (BWA) in a wireless metropolitan area network (WMAN). Worldwide Interoperability for Microwave Access (WiMAX) is a MAC and PHY layer wireless communication technology for outdoor broadband wireless coverage at a municipal, regional or state wise level. The set of standards that define WiMAX are developed and maintained by IEEE 802.16 Working Group [1, 2]. Two major variants of WiMAX have emerged and are being deployed: 802.16d standards support fixed or slowly moving users and 802.16e supports mobile users. Mobile WiMAX is designed to support a wide range of applications ranging from video streaming to web browsing. All of these applications require different levels of Quality-of-service (QoS) and this imposes a variety of different performance requirements on the MAC and PHY layers.

a) OFDMA

Mobile WiMAX utilizes Orthogonal Frequency Division Multiple Access (OFDMA) modulation where the Orthogonal Frequency Division Modulation (OFDM) sub carriers are shared among the users. Thus the available system profiles are dependent of the subcarriers numbers that are utilized.

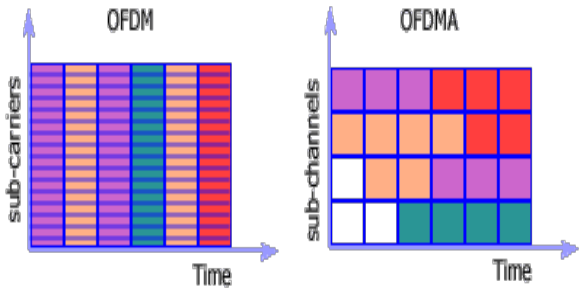


Fig. 1 : Sub Channelization in OFDM and OFDMA

In OFDM PHY, multiple subscribers use a time division multiple access (TDMA) to share the media. Combination of time division and frequency division multiple access in conjunction with OFDM is called Orthogonal Frequency Division Multiple Access (OFDMA) [12]. Figure 1 illustrates a schematic view of the two 802.16 PHYs discussed above.

Further in WiMAX systems, the data sub carriers are grouped into basic resource set units called slots. A slot is the minimum amount of resources that can be allocated to a certain user and its size in terms of sub carriers is specific to the subchannel allocation algorithm.

b) MIRACLE

A framework called Multi Interface Cross Layer Extension (MIRACLE) is designed where a set of dynamic libraries are loaded to add support for multi technology and cross-layering. A patch which also facilitates the use of dynamic libraries in ns2 is available. Working with dynamic libraries allows the development and subsequent use of new features without the need for re-compiling the whole simulator [13]. These libraries can be loaded on demand at simulation time. Moreover, the

Author α : PG Student, Department of Computer Science and Engineering, Sri Krishna College of Technology, Coimbatore.
E-mail : vrazhaguramyaa@gmail.com
Author σ : Prof. & Head, Department of Computer Science and Engineering, Sri Krishna College of Technology, Coimbatore.
E-mail : jagadeesh_sk@rediffmail.com
Author ρ : UG Student, Department of Computer Science and Engineering, Sri Krishna College of Technology, Coimbatore.
E-mail : venkatteshviji@gmail.com

architecture is highly modular as it allows the interconnection of multiple down and upstream modules at every layer in the protocol stack. Dedicated and broadcast channels are allocated, at each node, for the inter-layer communication of control as well as data messages. The framework can be used to simulate wired networks as well as a mixture of wired and wireless architectures.

II. Related Work

H. Schwarz *et al.* proposed an approach called Scalable Video Coding (SVC) that reduces the complexity at the server side and supports various types of clients. It encodes high quality video streams into groups of bit streams' including one base sublayer and multiple enhancements sublayers [9]. All clients subscribe for the base sublayer. The purpose of enhancement sublayers is to improve the video quality. The clients are given the option of choosing the enhancement sublayers depending on their network connection and the available resources.

J.She *et al.* illustrated an active frame dropping approach for streaming real-time video over IEEE 802.16 networks. In this approach, the base station drops a frame if it does not guarantee the safe delivery of the frame at the receiver's side with the application delay limit [10].

Hung-Hui Juan *et al.* proposed a cross-layer design between the streaming server and mobile WiMAX base stations [5] and showed that for each user the implementation of multiple connections with feedback information of the available transmission bandwidth is critical for supporting H.264/AVC-based scalable video coding in which the transmission packets can be further separated into multiple levels of importance.

James She *et al.* presented a cross-layer framework in which cross-layer design is applied to WiMAX IPTV multicast to guard against channel diversity between different receivers [6]. The solution again utilizes scalable video layers but, instead of a mapping onto different connections, superposition coding is employed. In such coding, more important data are typically modulated at BPSK whereas enhancement layers are transmitted with higher-order modulation such as 16QAM. A cross-layer unit performs the superposition at the BS, whereas at the subscriber stations video layers are selected according to channel conditions.

Ehsan Haghani *et al.* proposed a scheme to improve the MPEG video streaming quality for the end users [3]. Their solution concentrates on assigning priority to the more important frames and protects them against dropping.

L. Al-Jobouri *et al.* [4] put forth a cross layer protection mechanism through rateless encoding where the lost packet is recovered with the help of the additional redundant data added in the corresponding packet.

Lai-U Choi et al. has taken the problem regarding the quality of video streaming and they have provided the solution in which parameters from radio link layer and application layers are abstracted and based on that decision is distributed and the application layer and radio link layer will co-operate according the decision to provide a good quality video[14].

Nicola Baldo *et al.* presented a framework of dynamic libraries called miracle (Multi InteRfAce Cross Layer Extension) which extends the functionality of NS2 [13]. Its modular architecture aids in reusability and interoperability of codes. It has an embedded engine to handle cross layer messages.

III. Proposed Scheme

a) System Design

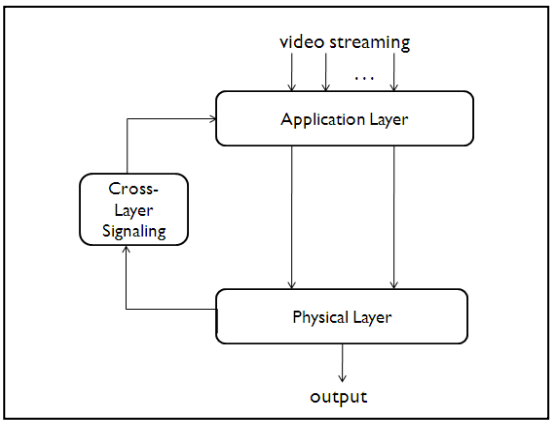


Fig. 2 : Schematic Representation of Proposed System

In the proposed cross-layer scheme, video partitioning is done at application layer. Video packets are transmitted to PHY layer then receiver signal strength is measured which is the basis of probability of channel byte loss (BL). The BL serves to predict the amount of redundant data to be added to the payload. BL is found and then communicated from the PHY layer via the link layer to the application layer using the cross-layer signaling mechanism. The packets with redundant data transmitted from application layer and in PHY layer Adaptive Modulation and coding is used to increase throughput. The whole process illustrated in Figure 2.

b) Video Partitioning

In an H.263 codec, when data-partitioning is enabled, inter-coded slices are normally divided into three separate partitions. I-frames are the least compressible but don't require other video frames to decode. P-frames can use data from previous frames to decompress and are more compressible than I-frames. B-frames can use both previous and forward frames for data reference to get the highest amount of data

compression. Receipt of a partition-I carrying packet is sufficient to enable a partial reconstruction of the frame. In adverse channel conditions, duplicate partition-I packets are transmitted. On the other hand, the duplicate partition-I stream should be turned off during favorable channel conditions. In order to decode partition-P and -B, the decoder must know the location from which each MB was predicted, which implies that partitions P and B cannot be reconstructed if partition-I is lost [4].

c) Cross Layer Signalling

An IEEE 802.21 Media Independent Handover (MIH) service provides a framework for cross-layer signalling that could be enhanced for more general purposes. IEEE 802.16g - Management Plane Procedures and Services consists the provision of cross-layer signaling. Upper-layer services, known as MIH users or MIHU communicate through the middleware to the lower layer protocols. One of the middleware services, the Media Independent Event Service (MIES) is responsible for reporting events such as dynamic changes in link conditions, link status and quality. In the proposed work, BL is found then BL and redundant data is communicated from the PHY layer via the link layer to the application layer using the cross-layer signalling mechanism [13].

d) Channel Adaptation

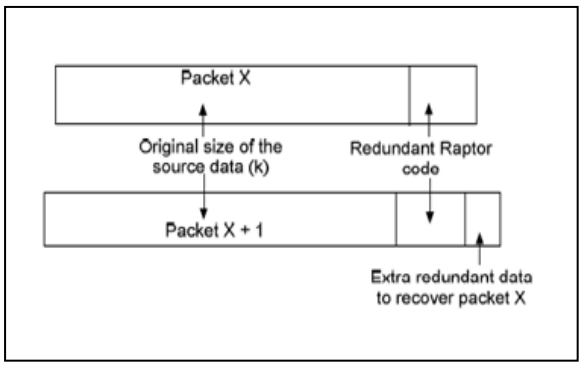


Fig. 3 : Additional redundant data piggybacked to the source data and original redundant data to the payload portion of packet to recover previous erroneous packet

When a negative acknowledgement is received by the physical layer The probability of channel byte loss (BL) serves to predict the amount of redundant data to be added to the payload. In an implementation, BL is found and then communicated from the PHY layer via the link layer to the application layer using the mechanism cross-layer signaling. The IEEE 802.16e standard specifies that an MS should provide channel measurements, which can either be Received Signal Strength Indicators or may be Carrier-to-Noise-and-Interference Ratio measurements made over modulated carrier preambles.

If the original packet length is L, then the redundant data is given simply by,

$$R = L\times BL+(L\times BL^2)+(L\times BL^3)+\ldots = L / (1-BL) - L \quad (1)$$

Where,

L - Packet length

BL - Byte Loss

R – Redundant data.

To achieve an incremental increase in redundant data, rateless channel coding is used. If a packet cannot be decoded, despite the provision of redundant data then additional redundant data are added to the next packet which is illustrated in Figure 3.

IV. Experimental Results

The simulation of WiMAX environment is done using NS 2.33 with MiracleWimax0.0.1 framework. Simulation scenario consists of one Base Station Node and 49 Mobile Nodes. The mode of operation is Point-to-multipoint (PMP). Table 2 shows some of the simulation parameters.

V. Simulation Parameters

PARAMETER	VALUE
Bandwidth	10 Mbps
Avg.Coverage area of Base Station	500 m
Maximum Height of Antenna	1.5 m
Transmission power of Base Station	0.025 W
Frequency	914 MHz
Propagation	Free space
Burst Time	500 ms
Idle Time	10 ms

a) Throughput Analysis

There is a considerable increase in Throughput which is depicted in Figure 4. Throughput is varied based on different modulation schemes.

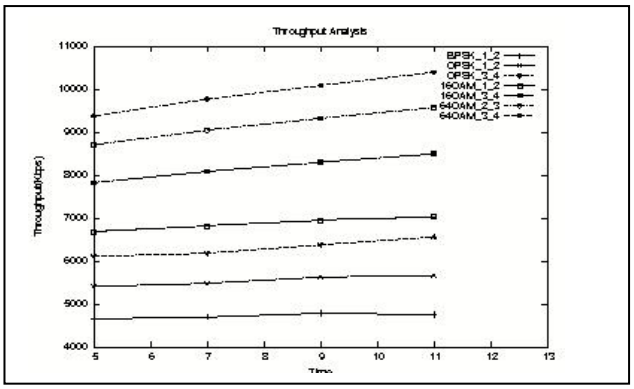


Fig. 4: Throughput vs. SimulationTime graph

In our proposed scheme, mandatory coding is AMC and as a optional technique Rateless encoding. With AMC the frame corruption is reduced. But if it is there any loss then Rateless coding used in conjunction with AMC and thus corrupted frames can be recovered.

VI. Conclusion

This paper employed an enhanced QoS provisioning approach in which corrupted frame is recovered by adding the redundant data to subsequent frame. This method uses piggy backing mechanism which improves the throughput and reduces the delay. Scarce radio resources of wimax network are better utilized through cross layer design.

Enhancing the same work for all type of service classes and comparison between this scheme and other cross layer schemes are reserved for future work.

References Références Referencias

1. IEEE 802.16-2004, IEEE Standard for Local and Metropolitan Area Networks –Part 16: Air Interface for Fixed Broadband Wireless Access Systems, October2004.
2. IEEE 802.16e-2005, IEEE Standard for Local and Metropolitan Area Networks –Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment. 2. Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands, February 2006.
3. Ehsan Haghani, Shyam Parekh, Doru Calin, Eunyoung Kim and Nirwan Ansari, "A Quality-Driven Cross-Layer Solution for MPEG Video Streaming Over WiMAX Networks," IEEE Transactions On Multimedia, vol. 11, no. 6, pp 1140-1147,Oct. 2009.
4. L. Al-Jobouri, M. Fleury, and M. Ghanbari, "Cross-layer Scheme for WiMAX Video Streaming," 3rd IEEE Computer Science and Electronic Engineering Conference (CEEC), pp 86-91, 2011.
5. H.-H Juan, H.-C. Huang, C. Huang, and T. Chiang, "Cross-layer mobile WiMAX MAC designs for the H.264/SVC scalable video coding," *Wireless Networks*, vol. 16, no. 1, pp. 113-123, 2009.
6. J. She, X. Yu, P.-H. Po, and E. H. Yang, "A cross-layer design framework for robust IPTV services over IEEE 802.16 network," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 2, pp. 235-245, 2009.
7. Kawadia and P.R. Kumar, "A cautionary perspective on cross layer design," *IEEE Wireless Commun. Mag.*, vol. 12, no. 1, pp. 3-11, 2003.
8. K. Balachandran, D. Calin, E. Kim, and K. M. Rege, "Proactive content rate selection for enhanced streaming media quality," in *Proc. IEEE Sarnoff Symp.*, pp. 1–6, Apr. 2008.
9. H. Schwarz, D. Marpe, and T. Wiegand, "Overview of the scalable video coding extension of the H.264/AVC standard," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 17, no. 9, pp. 1103–1120, Sep. 2007.
10. J. She, X. Yu, F. Hou, P.-H. Ho, and E.-H. Yang, "A framework of cross-layer superposition coded multicast for robust IPTV services over WiMAX," in *Proc. IEEE Wireless Communications and Networking Conf. (WCNC)*, Apr. 2008, pp. 3139–3144.
11. Seok-Yee Tang, Peter Muller and Hamid R. Sharif, "WiMAX Security and Quality Of Service An End-to-End Perspective," First Edition, Wiley, 2010.
12. J. G. Andrews, A. Ghosh, and R.Muhamed, *Fundamentals of WiMax*. Prentice-Hall, 2007.
13. Nicola Baldo, MarcoMiozzo, Federico Guerra, Michele Rossi and Michele Zorzi, "Miracle: TheMulti-Interface Cross-Layer Extension of ns2," EURASIP Journal onWireless Communications and Networking, Vol. 2010, Article ID 761792, pp 1-16.
14. Lai-U Choi, Wolfgang Kellerer, and Eckehard Steinbach, "On Cross-Layer Design for Streaming Video Delivery in MultiuserWireless Environments," EURASIP Journal onWireless Communications and Networking, Vol. 2006, Article ID 60349, pp 1–10.
15. http://www.isi.edu/nsnam/ns/ns

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 12 Issue 11 Version 1.0 June 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Web Based E-Learning Solution for Quality Education

By Muhamma d Haris Abid, Zahid Javed, Shahbaz Shoukat, Muhammad Sohaib Ashraf & Muhammad Zia Qammar

University of Agriculture, 38000, Faisalabad, Pakistan

Abstract - Nowadays computers education is necessary in every sector whether it is public or private. General applications like Word processor, Spread sheet, Presentations and email usage is demanded during hiring someone. Under development countries like Pakistan where literacy rate is already low, facing these challenges to produce a quality computer professional. Students have to pay huge amount to get a quality computer training away from their doorstep. Private sector is trying their best to fill this gap for professional education but they offered less quality that leads their efforts towards failure. Students have keen interest to get computers professional education that can help in their future life but they came back with frustration due to low quality of courses offered at high cost. In this situation the frustration can be reduced through Elearning Program. In this paper the author try to offer a web based E-learning solution according to current market requirements. This E-Learning solution may give some hope to those who are tired from current situations.

Keywords : *General Application, Training, Private Sector, E-learning.*

GJCST-E Classification: *J.1*

Strictly as per the compliance and regulations of:

Web Based E-Learning Solution for Quality Education

Muhammad Haris Abid [α], Zahid Javed [σ], Shahbaz Shoukat [ρ], Muhammad Sohaib Ashraf [ω] & Muhammad Zia Qammar [¥]

Abstract - Nowadays computers education is necessary in every sector whether it is public or private. General applications like Word processor, Spread sheet, Presentations and email usage is demanded during hiring someone. Under development countries like Pakistan where literacy rate is already low, facing these challenges to produce a quality computer professional. Students have to pay huge amount to get a quality computer training away from their doorstep. Private sector is trying their best to fill this gap for professional education but they offered less quality that leads their efforts towards failure. Students have keen interest to get computers professional education that can help in their future life but they came back with frustration due to low quality of courses offered at high cost. In this situation the frustration can be reduced through Elearning Program. In this paper the author try to offer a web based E-learning solution according to current market requirements. This E-Learning solution may give some hope to those who are tired from current situations.

Keywords :General Application, Training, Private Sector, E-learning.

I. Introduction

Technology exploiting is major concern in every field of life. Major goal of information technology is to provide such way which can help in these circumstances [1]. Organizations are now identifying the importance of information technology. ELearning is an advance way for getting knowledge through internet. Organizations are now utilizing e-learning methods for produce quality education which leads towards process improvement [3]. Elearning is a better option to support learning of individual and hence organizations goal achievement. Using elearning, end user can get vast knowledge at low cost with no traveling issues. E-learning is also providing ease of access to experts. User can gain knowledge with no timing restriction. There are no limitations of location; user can access it any time anywhere. Cisco and Lynda are offering elearning services now a day [9]. Recent research indicates that e-learning is fastest growing industries and earning billions. It is also opening ways for professional trainers. According to recent statistics, professional trainers are among 20 fastest mounting professionals [5]. While comparing with traditional education system, E-learning is offering number of courses as per desired by the students. Traditional learning is offering static material which is legacy according to current needs. While e-learning is offered variety of courses according to interest ofend user and requirements of market [10]. Normally e-learning trainings are developed by experts and professional so end user can get benefit according to recent requirements. World Wide Web (WWW) services are providing and improving rapidly services like e-leaning, e-survey, e-commerce and ebanking [3].

Author α σ : Department of Computer Science, University of Agriculture, 38000, Faisalabad, Pakistan.
Author ρ ¥ : Department of Computer Science, Comsats Institute of Information Technology, Chak Shahzad, Islamabad, Pakistan.
E-mail α : harisabid@hotmail.com
E-mail σ : zahidjaved.uaf@gmail.com
E-mail ρ : shahbaz.shoukat@gmail.com
E-mail ω : arham_sheikh@hotmail.com
E-mail ¥ : m_zia_qamar@yahoo.com

II. Distance Learning and Elearning

Layers shows at what level distance and elearning are located [6].

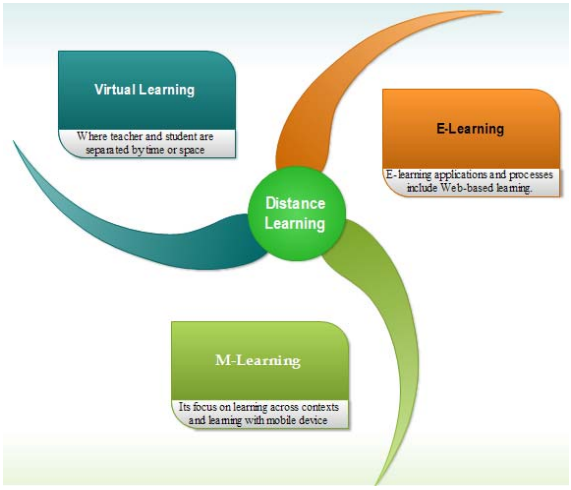


Figure 1: Distance Learning Modules

Distance learning is not new by its naming terminology. Term distance learning is common everywhere, e-learning is derived from it. Distance learning is always comfortable way of leaning for those who cannot afford traditional education due to distance, time and cost [8]. Many universities are offering distance learning courses by using workshops and virtual classes. Workshops and virtual class rooms are also bounded for time and location. People that are tired from traditional learning are also tired from these concepts like workshops and virtual classrooms [11]. E-

learning is free of all these where end user is not bounded for location and time. It is accessible from anywhere at any time with no restrictions [2]. It is also flexible and best choice for those who want to learn it separately.

III. E-Learning Devices

E-learning is not rocket science for which one requires costly devices. The major devices using by e-learning system are Desktop computers, Notebook computers and Tablet PC [6]. These devices are also available at low cost. Therefore end user will not face any kind of problems according to cost point of view [12].

a) E-Learning Components

Before starting e-learning solution one should know it components [7]. These are

i. *Contents*

Contents are most important for course whether it is traditional or internet based. Contents should be manageable, deliverable and according to standards. In other words contents are structure of courses which describes its entire context.

ii. *Page Design*

Page or learning environments has highly impact on student/ learner. It is like presentation of teacher in class room. Therefore e-learning modules page should be design according to end users expectations.

iii. *Content Commitment*

Content should be balanced and easy to learn. E-learning is way of self learning so content should be in such manner so students will not face any problem. E-learning developers and trainers should also focus to this point.

iv. *Usability*

Most of e-learning modules leads towards failure because of it are not verified, reviewed, not available when required and not up to date after some time according to current market demands.

v. *Spectators*

End users or spectators are the main components of e-learning as well as for traditional learning. E-learning module should be able to satisfy its spectator. Success and failure of elearning module is highly dependent on spectators.

IV. Empirical Work

The purpose of this paper is to provide an elearning solution according to current market requirements and which provide ease of access to end user. A web based elearning solution will offer to those who are interested to get quality education at his/her door step. Users have to pay affordable charges for course that he/she applied or registered. Different session will be offered for different number of courses at different time. User should have only internet facility to attend his/her training. He/ she can watch trainings anywhere. At the end a solution will be implemented which shows how this system will work. Implemented system will show how it is easy and effective.

a) E-Learning Web Application

There are many e-learning web applications are available now a days. Particularly in Pakistan these application are not fulfilling requirements of end user. They have poor quality in nature. Some is offering one feature and other is offering other. They are not well managed. In learning process content, intercommunication of teacher and student and evaluation are necessary components. Some existing e-learning modules do not even know them. Our elearning web application is following all necessary components of learning process. Following are the steps according to which this e-learning module will work.

i. *How to Access*

User can access our web based learning module very easily. User only has his/her personal computer with 1 MB internet connection speed. User has to visit our URL to access e-learning module.

ii. *How to Join*

User just has to visit our website and sing up by giving username and password to access e-learning module (Figure 2).

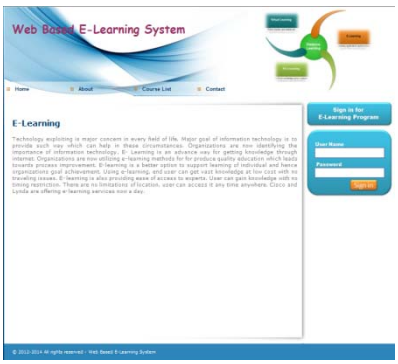


Figure 2: User Sign-up Form

iii. *Course Selection*

After creating free account user have to select his/ her course (Figure 3) which he / she want to learn. Course contents will be available against each course. Course benefits and certificate detail will also be available. Students just have to enrol them self by selection their course and timings he/ she feels sufficient for them. Each course has prerequisites which need to be fulfill by the student.

Figure 3: Course List

Three different sessions (Figure 4) of courses will be offered so one should decide his / her timings for learning.

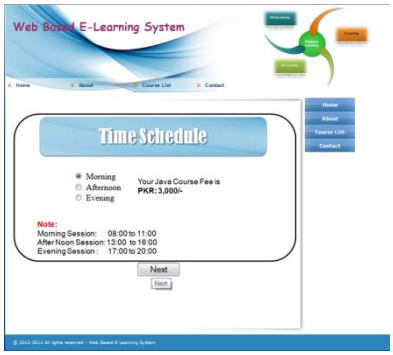


Figure 4: Course Time Schedule

iv. *Account Info/Payment Methods*

Users have to provide his/her account information for payment (Figure 5). He/She have to pay nominal payment against each course. There are many payment methods of this module like credit card, cheque, through mobile recharge or new techniques like easy paisa or UBL Omni (Figure 6). Users just have to pay for course what he/ she have to learn.

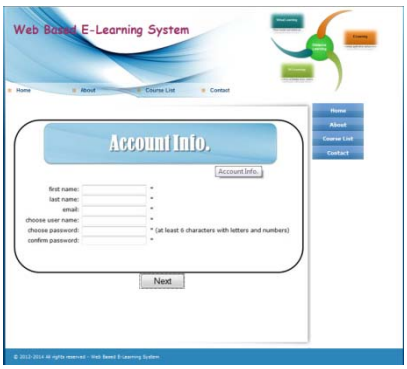


Figure 5: User Account Info

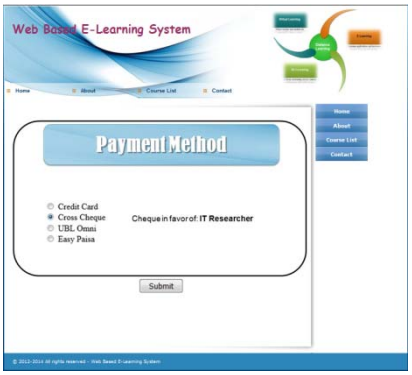


Figure 6: Payment Method

v. *Getting Started*

After course selection and fee payment user will be able to watch his/ her course videos (Figure 7). He will be able to comment on particular video or can give feedback to us. According to feedback rating of course will be performed. Students can watch their already watched videos at any time instead of daily session timings.

Figure 7: Watch Selected course Video

vi. *Contact to Trainer*

This e-learning module is providing contact with trainers (Figure 8). Each session will assign a trainer. This will help learners to understand course well. User can make contact with trainer through email or phone call. Trainer of particular training will be available at given time.

Figure 8: Contact Trainer

vii. *Evaluation Criteria*

Different evaluation criteria's will be offered. Different quizzes will be offered for evaluation purpose. If students fail in some quiz then negative points will be marked.

viii. *Award of Certificate*

Certificate will be awarded to students after completion of particular course. Certificate will be posted to his/ her mentioned postal address.

ix. *Job Opportunity*

After evaluation jobs will be offered to those who performed well in his/ her training session and quizzes.

V. Conclusion /Future Work

E-learning is playing vital role in training of professional education. It helps those who are not able to join regular classes or don't have time for traditional learning. Several elearning web sites are available especially in Pakistan but they are not fulfilling requirements of end users. They are offering less quality of training courses hence producing nothing. We are offering a elearning web based solution that will fulfil requirements of end user. It will be quality solution. This e-learning module will offer courses in some manageable form. In future we will convert this e-learning module to Mlearning. This will free of desktop PC's or Laptops. User will access our M-leaning solution on his/ her mobile device easily.

References Références Referencias

1. Bourner, T. and S. Flowers. (1997). Teaching and learning methods in higher education: A glimpse of the future. *Reflections on Higher Education, 9*, 77-102.
2. Brusilovsky, P., & Nijhavan, H. (1996). A Framework for Adaptive E-Learning Based on Distributed Re-usable Learning Activities. *Management*.
3. C. Groeneboer, D. Stockley, T. Calvert. (1997). Virtual-U: A collaborative model for online learning environments. *Proceedings Second International Conference on Computer Support for Collaborative Learning*, Toronto, Ontario.
4. Choudhury, V., Lopes, A. B. and Arthur, D. (2010). IT Careers Camp: An Early Intervention Strategy to Increase IS Enrollments. *Information Systems Research*, Vol. 21, No. 1, pp. 1-14.
5. Ferratt, T., W., Hall, S. R., Prasad, J. And Wynn, D., Jr. (2010). Choosing Management Information Systems as a Major: Understanding the smiFactors for MIS. *Communications of the AIS*, Vol. 27, No. 1, pp. 265-284.
6. Georgiev, T., Georgieva, E., & Smrikarov, A. (2004). M-Learning – a New Stage of E-Learning. *International Conference on Computer Systems and Technologies*, 1-5.
7. Jethro, O. O., Grace, A. M., & Thomas, A. K. (2012). E-Learning and its effects on teaching and learning in a global age. *Indian journal of education*, *1*(2), 73-78.
8. Kayte, O., G. Singh and J. Donoghue (2004). Implementinge Learning Programmes for Higher Education: A Review of the Literature. *J of Information Technology Education*, Volume 3, University of Wolverhampton, Wolverhampton, UK.
9. Mills, R. J., & Fadel, K. J. (2012). ELearning as a Career Path In Information Systems Curricula. *Journal of Business Education*, *5*(2).
10. Milne, J. (2005). *E*-Learning: The New E-xperts. Haymarket Professional Publications *Ltd*, pp. 28-33.
11. Qi, B., Liu, L., & Wang, C. (2009). Elearning Tools to Improve Students Learning Experience: a case study. *I .J .Modern Education and Computer Science*, (October), 1-9.
12. Tavangarian, D., Leypold, M. E., Nölting, K., Röser, M., & Voigt, D. (2003). Is e-Learning the Solution for Individual Learning? *Learning*, 273-280.

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 12 Issue 11 Version 1.0 June 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Wave Prediction and Delay Modeling for Teleoperation Via Internet

By Ehsan Kamrani & Mohamad Sawan
Harvard University

Abstract - This paper propose a novel approach for modeling the end-to-end time delay dynamics of the internet using system identification, and use it for controlling real-time internet-based telerobotic operations. When a single model is used, it needs to adapt to the operating conditions before an appropriate control mechanism can be applied. Slow adaptation may result in large transient errors. As an alternative, we propose to use an adaptive multiple model framework, and determine the best model for the current operating conditions to activate the corresponding controller. We employ multivariable wave prediction method to achieve this objective.

GJCST-E Classification: *b.4.m*

Strictly as per the compliance and regulations of:

Wave Prediction and Delay Modeling for Teleoperation Via Internet

Ehsan Kamrani [α] & Mohamad Sawan [α]

Abstract - This paper propose a novel approach for modeling the end-to-end time delay dynamics of the internet using system identification, and use it for controlling real-time internet-based telerobotic operations. When a single model is used, it needs to adapt to the operating conditions before an appropriate control mechanism can be applied. Slow adaptation may result in large transient errors. As an alternative, we propose to use an adaptive multiple model framework, and determine the best model for the current operating conditions to activate the corresponding controller. We employ multivariable wave prediction method to achieve this objective.

I. Introduction

The concept of teleoperation has been around for awhile. It involves remote control of a plant or machine from far distance via a medium environment. The distance can vary from tens of centimeters (micromanipulation) to millions of kilometers (space applications). Teleoperation takes several forms and can be done via any communication medium. Recently, the main focus has been on teleoperation via the Internet. Motivated by the availability, widespread access, and low cost of the Internet, many researchers have focused on the Internet-based teleoperation.

Since the Internet introduces random communication delays, several challenges and difficulties, such as loss of transparency and synchronization in real-time closed-loop telerobotic systems, may arise. In order to meet these challenges, a general and efficient modeling and analysis tool for the Internet delay needs to be developed. Several techniques have been proposed to compensate for this effect, such as a time forward observer developed for a supervisory control over the Internet by Brady and Tarn [1]-[3], a position-based force-feedback scheme implemented by Oboe and Fiorini [4], and a wave variable based technique developed by Niemeyer and Slotine [5].

The methods in [1] and [4] require knowledge of the remote plant, but the method in [5] does not. Due to possible uncertainties on the remote plant, the methods that require the knowledge of remote plant may not be applicable in all cases. The stability of such techniques may depend on the accuracy of knowledge on the remote plant. As such, the wave-based method has an advantage from this point of view, but may suffer from poor performance for delays significantly longer than the time constant(s) of the system. Wave variables were first introduced by Anderson and Spong [6]-[7], and were later presented in a more intuitive, physically motivated, passivity-based formalism by Niemeyer and Slotine [5]-[8]. Later the use of wave variables was extended to variable delay [9]-[10], as is the case for the Internet. Nevertheless, performance degradation for prolonged time delays is still a serious issue. In order to overcome these shortcomings, we propose a multimodel adaptive controller to choose the optimum controller.

Multi-model adaptive control schemes have been used in several applications [17]-[20]. In [21], we have used it in teleoperation control systems to maintain stability in the presence of time-varying or fluctuating delays. In this paper, we study the behavior of multi-model adaptive control systems in conjunction with wave prediction method for variable time delays. Furthermore, here we employ the ARX to model the time delays associated with the communications links, and identify its parameters using a system identification approach to be used in our proposed control system.

The rest of this paper is organized as follows. In Section 2 we propose an approach for modeling the time delay dynamics of the Internet. In Section 3, we explain the wave variable method as well as the Smith predictor. In Section 4, the multivariable Smith predictor is presented. In Section 5, we introduce a combination of wave variable and Smith predictor by adding the observer and the regulator block with a view to improving the performance. The adaptive control method for teleoperation systems is discussed in Section 6. In Section 7, we propose our control scheme which uses a multi-model adaptive controller for selecting the optimal controller. Section 8 contains the results and conclusions.

II. Dynamics of The Internet

a) QoS Parameters

The following four parameters describe the network QoS (Fig. 1): a) Time Delay, b) Jitter, c) Bandwidth, and d) Packet Loss. To improve the performance, the time delays need to be minimized. The impact of other parameters in Fig. 1 can be reduced using existing methods, which usually involve a tradeoff with the time delay. Therefore, QoS improvement in general involves minimization of the time delay, which is our focus in this paper.

Author α : Polystim Neurotechnologies Lab., Polytechnique of Montreal, Montreal,QC, CANADA. E-mail : ekamrany@yahoo.com

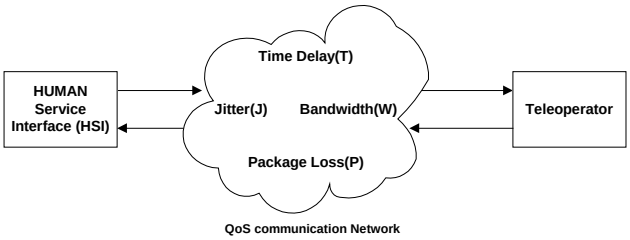


Fig. 1: Block diagram of teleoperation system in a QoS network

III. Internet Delay Measurement

a) Delay Dynamics of Internet in Iran

We have measured the delay for a number of Internet nodes in different geographical locations in Iran as well as another international node for different time intervals. Statistical results are shown in Table 1. Fig. 2 shows the variations in the delay during a 24 hour period with sampling at 1 min intervals.

Table 1: Characteristics of the measured delay in some Internet nodes

Minimum delay(ms)	Maximum delay(ms)	Std. deviation(ms)	Average delay(ms)	Place
639	1381	38.6454	846.01035	Sistan Univ.
723	1931	94.2156	930.7525	Tabriz Univ.
691	2831	83.0866	1911.55	T.M.U Univ.
86	337	61.0934	189.2639	www.yahoo.com

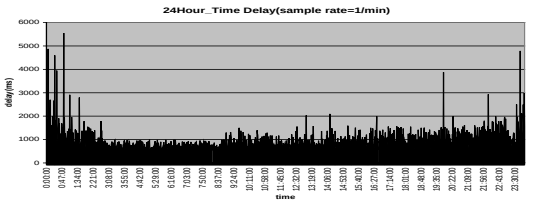


Fig. 2: Time delay in 24 hour with sampling interval of 1 min

IV. Black-Box Model of Internet Delay

The end-to-end packet delay dynamics is modeled as a SISO (Single-Input-Single-Output) system. The input is the inter-departure times between packets leaving the source, and the output is an end-to-end packet delay measured at the destination. We use the Auto-Regressive eXogenous (ARX) model and determine its coefficients using system identification approach (Fig. 3). Since the ARX is a linear time-invariant model, it cannot rigorously capture the non-linearity of the packet delay dynamics. Nevertheless, the ARX model is applied in many control engineering problems, because non-linearity around a stable operating point can be well approximated by a linear system.

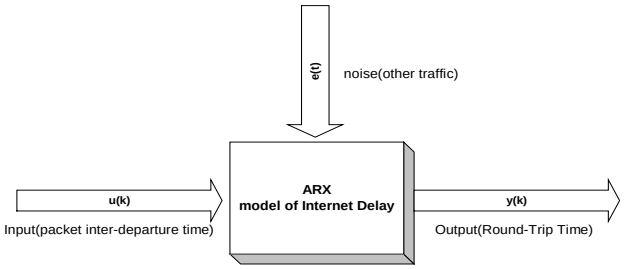
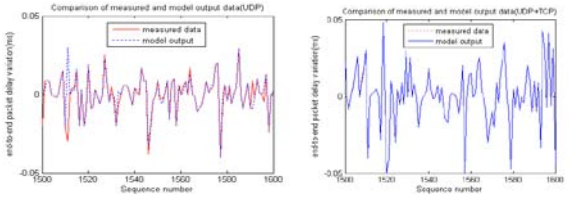


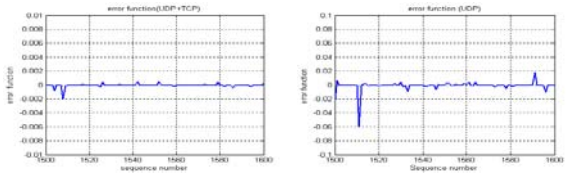
Fig. 3 : The ARX model for the end-to- end packet delay dynamics

Fig. 4 compares the measured data (solid line) and the model output (dotted line) in the UDP case, and the UDP+TCP case, respectively. It is evident that in both cases, the model output $\hat{y}(k \mid \theta)$ and the measured output $y(k)$ roughly coincide but slightly differ. This is because the measured end-to-end packet delay variation is disturbed by other unknown traffic not included in the model output $\hat{y}(k)$. According to the Fig. 5, the error of modeling is very low and so the model is acceptable.



(a) (b)

Fig. 4 : Comparison between measured data $y(k)$ and model output $\hat{y}(k)$ for (a) UDP case, and (b) UDP+TCP case



(a) (b)

Fig. 5: Error between measured data $y(k)$ and model output $\hat{y}(k)$ for (a) UDP case, and (b) UDP+TCP case

V. Wave Variables

a) Definition of Wave Variables

Wave variables were proposed in [6]-[7] for teleoperators with time delays, and is based on a more general framework of passivity for scattered operators. The basic mathematical formulations for wave variables can be described by power flow as

$$P = X_m F = U_t^T U_t - V_t^T V_t \quad (1)$$

Where F and X denote force and velocity, and U and V are incidental and reflected wave variables in

Fig. 6. We obtain *U* and *V* from power parameters *X* and *F* by

$$U = \frac{bX + F}{\sqrt{2b}}, \quad V = \frac{bX - F}{\sqrt{2b}} \tag{2}$$

Where *b* is a positive constant that depends on the communication link's parameters. In the bilateral control of force reflected systems, the transmission process is

$$U_s(t) = U_m(t-T), \quad V_m(t) = V_s(t-T) \tag{3}$$

Where *m* and *s* represent the corresponding side of the waves (master side or slave side) respectively, and *T* is a constant time delay. The stability of the system is preserved for any time delay, but performance is degraded proportionate to the actual delay.

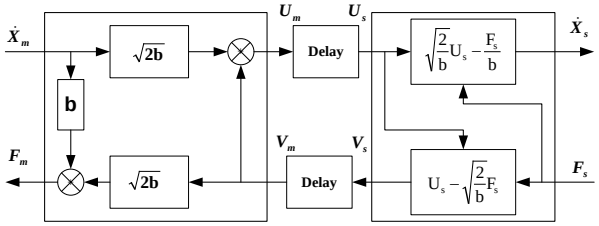


Fig. 6 : Transformation from power parameters to wave variables [5]

b) Passivity

Transformation of power parameters into wave variables affects the passivity of the system. The power inflow into the communication block at any time is given by (1). If we use (3) in (1) and assume that the initial energy is zero, the total energy in the communications link during the signal transmission between the master and the slave is

$$\begin{aligned} E &= \int_0^t P_{in}\,d\tau = \int_0^t (X_{md}F_m - \dot{X}_{sd}F_s)\,d\tau \\ &= \frac{1}{2}\int_0^t (U_m^T U_m - V_m^T V_m + V_s^T V_s - U_s^T U_s)\,d\tau \\ &= \frac{1}{2}\int_0^t (U_m^T U_m + V_s^T V_s)\,d\tau \geq 0 \end{aligned} \tag{4}$$

Where, X_{md} and X_{sd} are the desired velocities of the master and the slave, respectively. The system is passive independent of the delay *T*, meaning that this transformation makes wave variables robust to constant time delays. This is achieved at the cost of significant performance degradation for long delays. Recently, in [11] it was shown that incorporating a predictor or an observer in the communication channel can enhance the performance significantly in the presence of prolonged or variable delays over the Internet.

VI. Smith Predictor

a) Structure of Smith Predictor

A very effective time delay compensation method is to use the Smith Predictor [12]-[14] as shown in Fig. 7, in which *C(s)* is the controller, *P(s)* is the plant that includes communication delay, $\hat{P}(s)$ is the plant model, and $\underline{\hat{P}}(s)$ is the plant model without the time delay. Since the control signal is delayed, the same delay is accounted for in the controller to coordinate the feedback with system dynamics. The Smith Predictor works poorly unless the delay is precisely known [15].

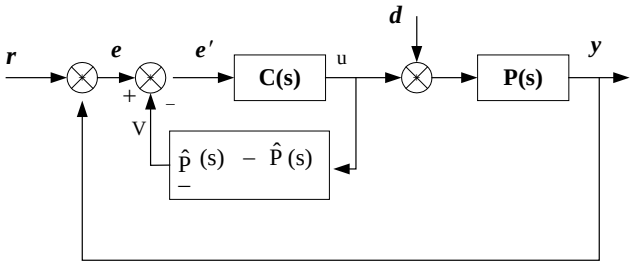


Fig. 7 : Smith Predictor block diagram

b) Multivariable Smith Predictor

The Smith Predictor is typically used for Single-Input-Single-Output (SISO) systems. However, if $P(s)$ and $\hat{P}(s)$ are transfer matrices then

$$P(s) = e^{-Ts}\begin{bmatrix} P_{11}(s)e^{-T_{11}S} & P_{12}(s)e^{-T_{12}S} \\ P_{21}(s)e^{-T_{21}S} & P_{22}(s)e^{-T_{22}S} \end{bmatrix}, \quad \hat{P}(s) = \begin{bmatrix} P_{11}(s) & P_{12}(s) \\ P_{21}(s) & P_{22}(s) \end{bmatrix} \tag{5}$$

Now, it is easy to show that the closed loop system is

$$P_{cl}(s) = PC(I + \hat{P}C)^{-1} \tag{6}$$

Thus we can remove the delay from the loop, similar to the SISO case.

VII. Nonlinear Adaptive Control

A typical teleoperation system consists of a local master manipulator (master site) and a remote slave manipulator (slave site). The human operator controls the local master manipulator to drive the slave in order to perform a given task remotely. The system must be completely "transparent" so that the human operator could feel as if he/she is able to directly manipulate the remote environment. Instead of perfect force tracking, the overall teleoperation system should behave as a free-floating mass plus linear damper specified by the control and scaling parameters.

Hung, Marikiyo and Tuan in [16] used the concept of a virtual manipulator to design a nonlinear control scheme that guarantees the asymptotic motion (velocity/position) tracking and has a reasonable force tracking performance even in when the acceleration, the values of dynamic parameters of manipulators as well as the models for human operator and the environment

are not available. In the absence of friction and other disturbances, dynamic models of the master and the slave manipulators are

$$F_{am} + F_{mam} = M_{xm}(q_m)\ddot{X}_m + C_{xm}(q_m, \dot{q}_m)\dot{X}_m + g_{xm}(q_m)$$
$$F_{as} + F_{ext} = M_{xs}(q_s)\ddot{X}_s + C_{xs}(q_s, \dot{q}_s)\dot{X}_s + g_{xs}(q_s) \quad (7)$$

If the followings are achieved

$$X_m(t) = X_s(t), \quad F_{as} = -F_{ext} \quad (8)$$

Then the system is said to be "transparent" to human-task interface. This requires knowledge of the manipulator acceleration, which in practice, is difficult to obtain. Moreover, there is a trade-off between motion tracking performance, force tracking performance, and system stability for a master-slave teleoperation system. In order to improve the performance, we increase the degree of freedom of the control system by utilizing a "virtual master manipulator." This manipulator is described by the following dynamic model

$$F_d = M_d \ddot{X}_d + K_d \dot{X}_d + K_p \ddot{X}_d \quad (9)$$

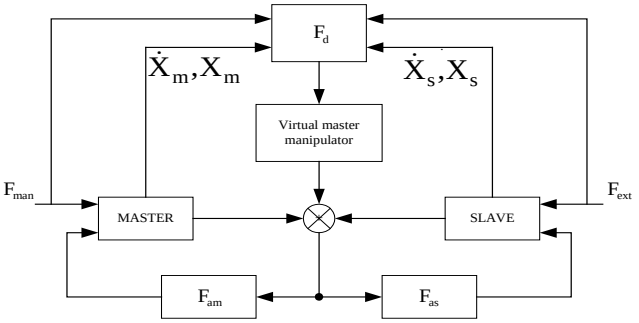


Fig. 8 : Block diagram of the adaptive control system

Fig.8 shows the block diagram of the overall teleoperation system using the virtual master manipulator.

VIII. The Proposed Control System

A switched system is utilized when there are abrupt changes in the structures and parameters of the dynamic system, which can be caused by component failures, repairs, environment changes, disturbances or changes in subsystems interconnections [17]-[18], and may result in improving the performance[19]-[20].

When a single identification model is used, it will have to adapt itself to the operating condition before appropriate controls can be taken. If the environment changes suddenly, the original model (and hence the controller) is no longer valid. If the adaptation is slow, it may result in a large transient error. However, if different models are available for different operating conditions, then suitable controllers corresponding to each condition can be devised in advance.

The control structure in Fig. 9 determines the best model for the existing operating condition at every instant, and activates the corresponding controller. This structure is based on *N* models which have been developed at various points across the operating range of the process. A controller is designed for each model, using the Diophantine pole–placement algorithm. A supervisor as shown in Fig. 10 compares the output errors for each one of the *N* models. A discrete equivalent of the performance index is given in (10), for the j^{th} model:

$$J_i(k) = \alpha e_i^2(k) + \beta \sum_{j=1}^{M} \exp(-j\lambda_i) e_i^2(k-j) \quad (10)$$

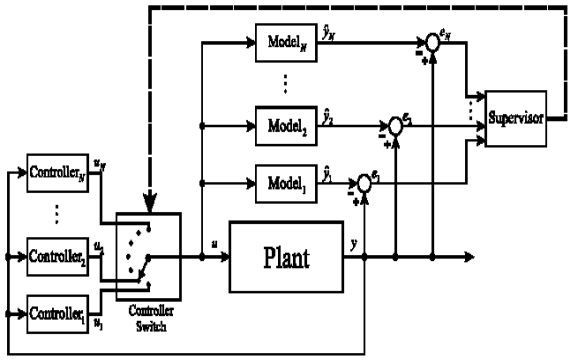


Fig. 9 : Multi-model adaptive control system

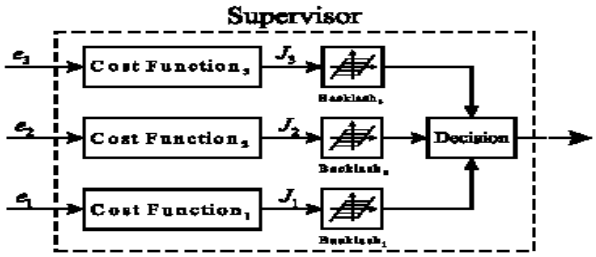


Fig. 10: Supervisor operation

Expansion of this controller for the master-slave teleoperation was proposed in [21], where the best model for the current operating condition is identified and the corresponding controller either in the master or in the slave is activated. The block diagram of this proposed control system is shown in Fig. 11.

Here we have used the ARX model for the communication delay, and obtained its parameters using a system identification approach; and studied its performance under abrupt changes in the time delay using simulation and analysis.

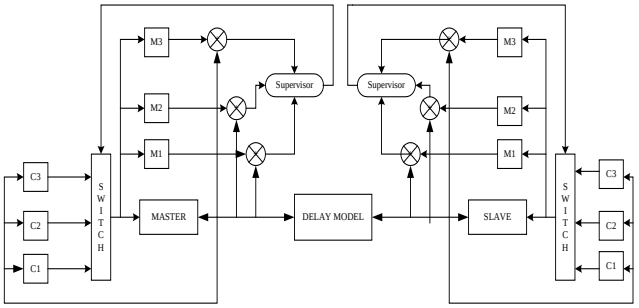


Fig.11 : The proposed master-slave multi-model adaptive control system block diagram for teleoperation via the Internet

IX. Results and Conclusions

We presented a new method for designing a robust stable Internet-based teleoperation system. Our focus is on the robustness against delay and its random nature. We have applied our proposed method to control a simple teleoperation system and studied its behavior for a time varying delay on the communication link between the plant and the controller.

This control scheme was initially proposed and analyzed in [21]. Here we focus on the behavior of the proposed control system under abrupt changes in the time delay. Furthermore, we have replaced the delay block in [21] with a delay model obtained using the ARX model, the parameters of which are obtained using system identification as discussed above.

Fig. 12 shows the system output using ordinary wave prediction method. In the output of our proposed method (Fig. 13) we note that the proposed control system is more robust with minim overshoot. Fig. 14 shows the step responses for ordinary and proposed control methods, when time delay changed abruptly from 700 msec to 2100 msec at t=50. We note that the proposed multi-model control strategy has a satisfactory response with small fluctuations. Fig. 15 shows the tracking response without wave prediction. In Figs. 16 and 17, the tracking responses of wave prediction and the proposed control methods are shown. The results indicate the usefulness of our proposed approach particularly for abrupt variations of the environment's parameters.

We can also use this structure together with the wave variable method, the Smith predictor method, and a combination of the two in linear and/or nonlinear controllers, time-based and/or non-time based controllers and other suitable types of controllers, so that the most fitting controller can be utilized depending on the circumstances.

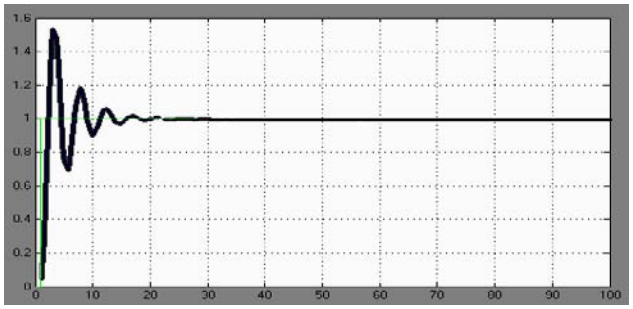


Fig.12 : System response using the ordinary wave-prediction method

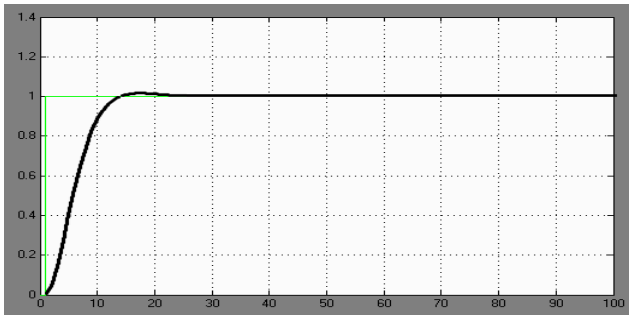


Fig.13: System response using our proposed method

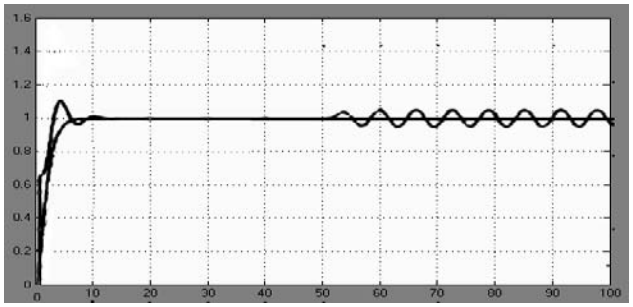


Fig.14: System step responses for the ordinary and the proposed control methods, when time delay changed abruptly

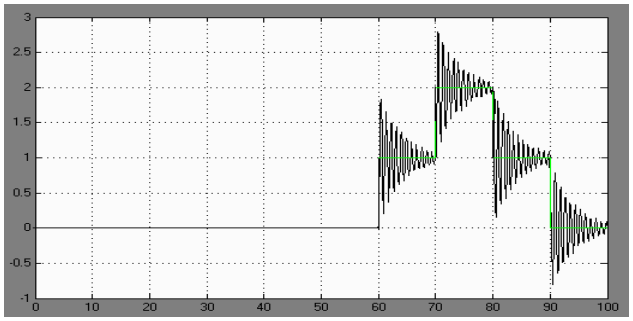


Fig.15: System tracking response without wave prediction

Fig. 16: System output tracking response with wave prediction

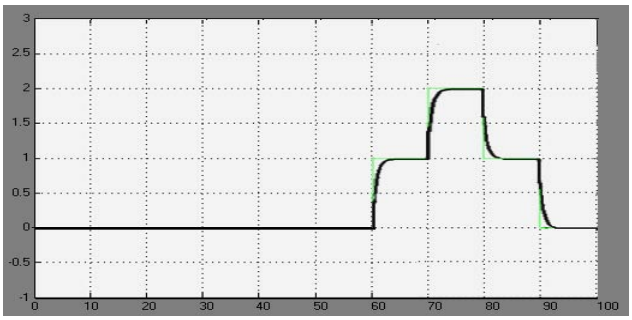


Fig. 17: System tracking response with proposed control system

References Références Referencias

1. K. Brady, *Time-Delayed Control of Telerobotic Manipulators*, Ph.D. Dissertation, Dept. Syst. Sci. Math., Univ. Washington, Seattle, 1997.
2. K. Brady and T. J. Tarn, "Internet-based remote teleoperation," *Proc. IEEE Int. Conf. Robotics and Automation*, Leuven, Belgium, May 1998, pp. 65–70.
3. T. J. Tarn and K. Brady, "A framework for the control of time-delayed telerobotic systems," *Proc. IFAC Robot Control*, Nantes, France, 1997, pp. 599–604.
4. R. Oboe and P. Fiorini, "A design and control environment for internet based telerobotics," *Int. J. Robot. Res.*, vol. 17, no. 4, pp. 433–499, Apr. 1998.
5. G. Niemeyer and J. E. Slotine, "Using wave variables for system analysis and robot control," *Proc. IEEE Int. Conf. Robotics and Automation*, Albuquerque, New Mexico, pp 1619-1625.
6. R. J. Anderson and M. W. Spong, "Bilateral control of teleoperators with time delay," *IEEE Trans. Automat. Contr.*, vol. 34, pp. 494–501, May 1989.
7. R. J. Anderson, *SMART Class Notes*, Intelligent Systems & Robotics Center, Sandia National Laboratories, Livermore, CA, 1994.
8. G. Niemeyer and J. E. Slotine, "Stable adaptive teleoperation," *IEEE Trans. Automat. Contr.*, vol. 36, pp. 152–162, Jan. 1991.
9. G. Niemeyer and J. E. Slotine, "Toward force-reflecting teleoperation over the Internet," *Proc. IEEE Int. Conf. Robotics and Automation*, Leuven, Belgium, May 1998, pp. 1909–1915.
10. Y. Yokokohji, T. Imaida, and T. Yoshikawa, "Bilateral teleoperation under time-varying communication delay," *Proc. IEEE/RSJ Int. Conf. Intelligent Robots and Systems*, vol. 3, Oct. 1999, pp. 1854–1859.
11. S. Munir and W. J. Book, "Internet-based teleoperation using wave variables with prediction," *IEEE/ASME Trans. Mechatronics*, vol. 7, no. 2, June 2002.
12. S. Ganjefar, H. R. Momeni, and F. Janabi-Sharifi, "Teleoperation systems design using augmented wave-variables and Smith predicator method for reducing time-delay Effects," *Proc. International Symposium on Intelligent Control*, Vancouver, Canada, October 2002, pp. 27-30.
13. J. M. Smith, "Closer control of loops with dead Time," *Chemical Engineering Progress*, vol. 53, no. 5, pp. 217-219, May 1957.
14. Z. Palmor, "Stability properties of Smith dead-time compensator controllers," *International Journal of Control*, vol 32, no. 6, pp 937-949, 1980.
15. W. J. Book and M. Kontz, *Teleoperation of a Hydraulic Forklift from a Haptic Manipulator over the Internet*, George W. Woodruff School of Mechanical Engineering, Georgia Institute of Technology, Atlanta, 2003.
16. N. Hung, T. Marikiyo, and H. Tuan, "Nonlinear adaptive control of master-slave system in teleoperation," *Control Engineering Practice*, no. 11, pp. 1-10, 2003.
17. E. Mosca and T. Agnoloni, *Switching Supervisory Control Based on Controller Falsification and Closed-Loop Performance Inference*, Dipartimento di Sistemi Informatica, Universita di Firenze, Firenze, Italy, 2002.
18. K. S. Narendra and J. Balakrishnan. "Adaptive control using multiple models," *IEEE Transactions on Automatic Control*, vol. 42, no. 2, pp. 171–187, Feb. 1997.
19. K. S. Narendra, J. Balakrishnan, and M. K. Ciliz, "Adaptation and learning using multiple models, switching, and tuning," *IEEE Control Systems Magazine*, vol. 15, no. 3, pp. 37–51, Jun. 1995.
20. L. Chen and K. S. Narendra, *Nonlinear Adaptive Control Using Neural Networks and Multiple Models*, Scientific Systems Company Inc., 500 West Cummings Park, Suite 3000, Woburn, MA 01801, USA and Center for Systems Science, Yale University, New Haven, Connecticut 06520, USA, 2001.
21. E. Kamrani, H. R. Momeni, and A. R. Sharafat, "A Multi-model adaptive control system for teleoperation via Internet," *Proceedings of the IEEE International Conference on Control Applications*, Taipei, Taiwan, September 2-4, 2004, pp. 1336-1340.
22. E. Kamrani, "Control of Teleoperation Systems via Internet: Robustness against Delay," A Thesis

Presented For The Degree of Master of Science in Electrical Engineering, Faculty OF Engineering, Tarbiat Modarres University, Tehran, Iran, Winter 2005

23. E. Kamrani, "The Survey on Web_Based Control Systems ," A Seminar Presented For The Degree of Master of Science in Electrical Engineering, Faculty OF Engineering, Tarbiat Modarres University, Tehran, Iran, Autumn 2003

This page is intentionally left blank

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 12 Issue 11 Version 1.0 June 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Sparse Matrix Representation for Web Opinions

By Dr.L.Venkateswara Reddy & B.R.Dileep Kumar
Sree Vidyanikethan Engg College

Abstract - Due to the advancement of Web 2.0 technologies, a large volume of Web opinions is available on social media sites such as Web forums and Weblogs. These technologies provide a platform for Internet users around the world to communicate with each other and express their opinions. Web opinions are short and sparse text messages with noisy content. In this paper, we are using a sparse matrix representation for web opinions and defining a preprocess way for it. Here, we are proposing an algorithm for matrix generation from vector of thread's. Due to this representation, we use opinions in efficient way.

Keywords : *Web opinion, sparse matrix representation.*

GJCST-E Classification: *I.2.4*

Strictly as per the compliance and regulations of:

Sparse Matrix Representation for Web Opinions

Dr.L.Venkateswara Reddy [α] & B.R.Dileep Kumar [σ]

Abstract - Due to the advancement of Web 2.0 technologies, a large volume of Web opinions is available on social media sites such as Web forums and Weblogs. These technologies provide a platform for Internet users around the world to communicate with each other and express their opinions. Web opinions are short and sparse text messages with noisy content. In this paper, we are using a sparse matrix representation for web opinions and defining a preprocess way for it. Here, we are proposing an algorithm for matrix generation from vector of thread's. Due to this representation, we use opinions in efficient way.

Keywords : Web opinion, sparse matrix representation.

I. Introduction

Web opinions are usually less organized and sparse messages. Web users who want to express their opinions on political and social issues, religion, consumer products, traveling experiences, movies, music, sports, health, technology or any topics of interests, they will submit a message to a Web forum platform, a Weblog platform or an individual Weblog site to share their opinions with others. A Weblog or Web forum is a channel for Web users to share their personal details to a circle of friends, amplify their voices and sentiment, establish online communication in a topic of interest, and promote an ideology.

The frame work for web opinion project are proposed by C. C. Yang and Tobun D. Ng [1]. The framework of the web opinion project is depicted in Figure 1.The framework has five major components: web opinions discovery and collection, web opinions analysis, web opinions evolution and understanding, and interactive information visualization.

Web opinions having some properties ,They are(1) the messages are less focused, (2) the messages are usually short with the length ranged from a few sentences to a couple paragraphs,

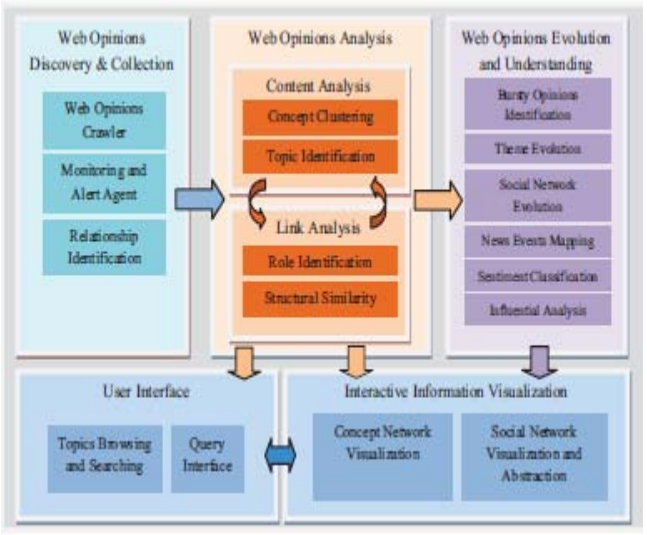


Fig.1: The framework of the web opinions analysis and understanding project

(3) different users may use different terms to discuss the same topic, therefore, the terms used in the messages are sparse, (4) the messages contain many unknown terms that do not exist in typical dictionary or ontology, e.g. iPhone, Xbox, (5) there are many noises, many Web opinions do not fall into any categories, (6) the volume of Web opinion messages is huge and it is expanding in an enormous rate, and (7) the topics in these messages are evolving.

II. Related Work

In our preliminary studies [2],[3], it is found that over 50% of Web opinions are noise. Due to the sparseness of terms being used in Web opinions, the distance measured by document vectors are usually large although the corresponding documents are related. These reasons cause the poor performance of Web opinion. The representation of Web opinions is not satisfied or applicable because of the Web opinion properties.

Sparse matrix: A sparse matrix is a matrix populated primarily with zeros. The sparsity corresponds to systems which are loosely coupled. The concept of sparsity is useful for which we have a low density of significant data. When storing and manipulating sparse matrices on a computer, it is beneficial and often necessary to use specialized algorithms and data structures that take advantage of the sparse structure of the matrix[5][6].

Author α : Professor, Dept. of CSE, Sree Vidyanikthan Engg. Coll., A.Rangempet, Tirupati, A.P, INDIA-517 102.
E-mail : lakkireddy.v@gmail.com
Author σ : M.Tech Student, Dept of CSE, Sree Vidyanikethan Engg. Coll., A.Rangempet , Tirupati , A.P, INDIA-517 102.
E-mail : boggarapudil@gmail.com

The Object of sparse matrix (Coordinate list) is, a set of triples, <row, column, value>, where row and column are integers and form a unique combination, and value comes from the set item.

For example, consider a matrix A as given below A.

$$= \begin{bmatrix} 1 & 2 & 0 & 0 \\ 0 & 0 & 9 & 4 \\ 0 & 3 & 0 & 2 \end{bmatrix}$$

The sparse matrix representations as shown below

$$(A) = \begin{matrix} R & C & V \\ \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 2 \\ 2 & 3 & 9 \\ 2 & 4 & 4 \\ 3 & 2 & 3 \\ 3 & 4 & 2 \end{bmatrix} \end{matrix}$$

R=row
C=Column
V=Value

III. Preprocessing

In the preprocessing, we have collected some web opinions with respect to threads. In this paper, we are using three steps [4] to make data ready to represent as sparse matrix:

Step 1: In this step, we exclude some words that are commonly used in conversation or casual online discussions and at the same time to use the most important set of terms to represent each thread for similarity comparison in the clustering process or some other process. After tokenizing a document, commonly used terms or stop words are first removed from the term set of each document.

Step 2: In this step, we are finding the statistics of term frequency *tf for* all terms.

Step 3: In this step, we create the document vector for each thread after applying above two steps. After this step we get vector of all threads and it use bigrams or two-word terms as part of the document vectors. Natural language processing is an ideal tool to identify noun and verb phrases, which carry higher specificity than single words or monograms and employ a method to form bigrams by joining two adjacent words without any punctuation or stop word between them.

IV. Representation in Sparse Matrix

First of all, we have to create a matrix for all opinions. The creation of matrix involved the following steps:

1. Vector Gathering.
2. Matrix Generation.

1. *Vector Gathering :*

In this step, we are collecting the threads which are pre-processed. After the preprocessing, we have the necessary terms with their Term Frequency and they are defined in a vector from. This step repeats until all the threads are completed.

2. *Matrix Generation:*

In the Matrix generation, we have already collected the vectors of all threads. Now we store them in the matrix form.

a) Column defines the terms occurring in threads.
b) Row defines the thread's *TF* (Term Frequency) according to the term.

Algorithm for GenMatrix( ):

```
1.  Initializing the row_Size=0, col_Size=0, th_Term={“ ”}.
2.  for all threads
3.  for each and every term in thread
4.  if (term not in th_Term) {
5.  add (term) to th_Term;
6.  add its TF
7.  }
8.  for all threads
9.  for all term in th_term
10. if (term not thread) {
11. add its TF=0
12. }
13. for all threads
14. {
15. col_size=0;
16. for all trem in th_trem
17. {
18. mat [row_Size][col_Size]=trem's TF;
19. col_Size++;
20. }
21. row_Size++;
22. }
```

In above algorithm, th_Term is a String array which store all the terms from all threads.

From line 02-07: This performs a Searching operation to find new term in thread and store it.

From line 08-12: In this module, adding TF as ZERO. For not having term in their thread.

From line 13-22: Finally, we are storing the value of TF of each thread into a matrix form.

Now, we have created a matrix and it having sparse data. The sparse matrix representation is same as we defined in the related work. Consider a matrix of 5 columns and 6 rows as shown in the below. Here 5-columns means five terms and 6 rows means six threads.

$$A = \begin{bmatrix} 0 & a_{12} & a_{13} & 0 & 0 \\ 0 & 0 & a_{23} & 0 & a_{25} \\ a_{31} & 0 & 0 & a_{34} & 0 \\ a_{41} & 0 & a_{43} & 0 & 0 \\ 0 & a_{52} & 0 & 0 & a_{55} \\ a_{61} & a_{62} & a_{63} & 0 & 0 \end{bmatrix}$$

Sparse matrix for A is given in below

$$spare\ (A) = \begin{bmatrix} 1 & 2 & a_{12} \\ 1 & 3 & a_{13} \\ 2 & 3 & a_{23} \\ 2 & 5 & a_{25} \\ 3 & 1 & a_{31} \\ 3 & 4 & a_{34} \\ 4 & 1 & a_{41} \\ 4 & 3 & a_{43} \\ 5 & 2 & a_{52} \\ 5 & 5 & a_{55} \\ 6 & 1 & a_{61} \\ 6 & 2 & a_{62} \\ 6 & 3 & a_{63} \end{bmatrix}$$

The above define is sparse matrix for matrix A. The matrix is having row, column and it's value. For example, take a value a_{62} is value at 6^{th}-row and 2^{nd}-column. Normal matrix representation take a 6X5=30 unit of memory and sparse matrix takes 39 units. Disadvantage of proposed system is time taking to create and its take more space. In advantages side, it gives good results in different functionality and in this modern days space is not a problem.

V. Conclusion

In this paper, we have proposed an algorithm for generating a matrix from vectors. From matrix, we represent it into sparse matrix. This is the best way to represent the opinions. It has different applications in data mining and gives the basic idea of functionality like clustering and etc. From the way of representation is easy to find the term frequency of terms and we can efficiently find the trending topics in discussion.

References Références Referencias

1. C. C. Yang and T D. Ng, "Web Opinions Analysis with Scalable Distance-Based Clustering", IEEE International Conference on Intelligence and Security Informatics, 2009, PP: 65-70.
2. C. C. Yang and T. D. Ng, "Terrorism and Crime Related Weblog Social Networks: Link, Content Analysis and Information Visualization," in IEEE International Conference on Intelligence and Security Informatics, 2007, PP: 55–58.
3. C. C. Yang and T. D. Ng, "Analyzing Content Development and Visualizing Social Interactions in Web Forum," in IEEE International Conference on Intelligence and Security Informatics, 2008, PP: 331–342.
4. C. C. Yang and T D. Ng, "Analyzing and Visualizing Web Opinion Development and Social Interactions with Density-Based Clustering" IEEE Transc. On Sys. Man and Cyb, Vol. 41(6), Nov.,2011, PP: 1144 - 1155.
5. Golub, Gene H.; Van Loan, Charles F. (1996). Matrix Computations (3rd ed.) Baltimore: Johns Hopkins. ISBN 978-0-8018-5414-9
6. Tewarson, Reginald P. (May 1973). Sparse Matrices (Part of the Mathematics in Science & Engineering series). Academic Press Inc.

This page is intentionally left blank

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 12 Issue 11 Version 1.0 June 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Telephony Calls over Bluetooth

By Ajinkya Salunke, Prashant Shelke & Apurva Sahasrabudhe
Sinhgad college of Engineering, Pune

Abstract - VoIP is born from the growing Internet infrastructure, which has over the years seen significant improvements in both bandwidth and end-to-end latency. Merging VoIP technologies with telephony infrastructures is of particular interest since it significantly reduces the costs. In this project, we are making voice calls over Intranet available on a mobile phone using Bluetooth as the access protocol. Bluetooth was selected because it is increasingly available in mobile telephones. Most modern mobile phones with a focus on wirelessly sharing data between the device and a host PC come equipped with a Bluetooth adaptor.

The project mainly consists of developing a Voice-over-Bluetooth (VoB) mobile application for Android phones and a PC application to enable voice calls over Intranet and Bluetooth connection. The mobile application connects to desktop application over BT to make and receive calls. The desktop application establish/receive call with/from other mobile/phone terminals over Intranet. When in range of a PC, a wireless Bluetooth connection to the IP network is made available to the mobile phone, offering the choice of connecting to a conventional mobile GSM network or to a lower-cost IP infrastructure. The vision for the future is to make the mobile phone's operation fully transparent to the user by making both technologies completely interchangeable.

Keywords : *Bluetooth, VoIP, Android.*

GJCST-E Classification: *C.2.1*

Strictly as per the compliance and regulations of:

Telephony Calls over Bluetooth

Ajinkya Salunke [α], Prashant Shelke [σ] & Apurva Sahasrabudhe [ρ]

Abstract - VoIP is born from the growing Internet infrastructure, which has over the years seen significant improvements in both bandwidth and end-to-end latency. Merging VoIP technologies with telephony infrastructures is of particular interest since it significantly reduces the costs. In this project, we are making voice calls over Intranet available on a mobile phone using Bluetooth as the access protocol. Bluetooth was selected because it is increasingly available in mobile telephones. Most modern mobile phones with a focus on wirelessly sharing data between the device and a host PC come equipped with a Bluetooth adaptor.

The project mainly consists of developing a Voice-over-Bluetooth (VoB) mobile application for Android phones and a PC application to enable voice calls over Intranet and Bluetooth connection. The mobile application connects to desktop application over BT to make and receive calls. The desktop application establish/receive call with/from other mobile/phone terminals over Intranet. When in range of a PC, a wireless Bluetooth connection to the IP network is made available to the mobile phone, offering the choice of connecting to a conventional mobile GSM network or to a lower-cost IP infrastructure. The vision for the future is to make the mobile phone's operation fully transparent to the user by making both technologies completely interchangeable.

Keywords : Bluetooth, VoIP, Android.

I. Introduction

Purpose : Telecom operators in growth markets are facing extreme network congestion due to high Tele density in metro cities. This leads to dropped calls and poor voice quality causing customer dissatisfaction and loss of business. This project aims to decongest telecom network, where possible, by employing Bluetooth technology and VoIP and use Internet as a secondary network to route phone calls. With this solution, the mobile phone transparently switches to Bluetooth and VoIP (when present) while establishing call.

Scope : We are developing this system to decongest the telecom network. Rather than using the GSM network we are going to route the telephony calls through Internet. This will reduce the problem of call drops and poor voice quality. Due to use of internet or intranet the service cost of telephony will reduce by considerable amount.

There are basically two applications - a Voice-over-Bluetooth (VoB) mobile application for Android phones and a PC application to enable voice calls over Internet or Intranet and Bluetooth connection. The mobile application connects to PC application over Bluetooth to make and receive calls. The PC application can be extended internally to establish/receive call with/from other mobile/phone terminals.

Product Perspective : We can see this system as a replacement or an alternative for the traditional GSM system. With this system the mobile application connects to desktop application over BT to make and receive calls. The PC application establish/receive call with/from other mobile/phone terminals.

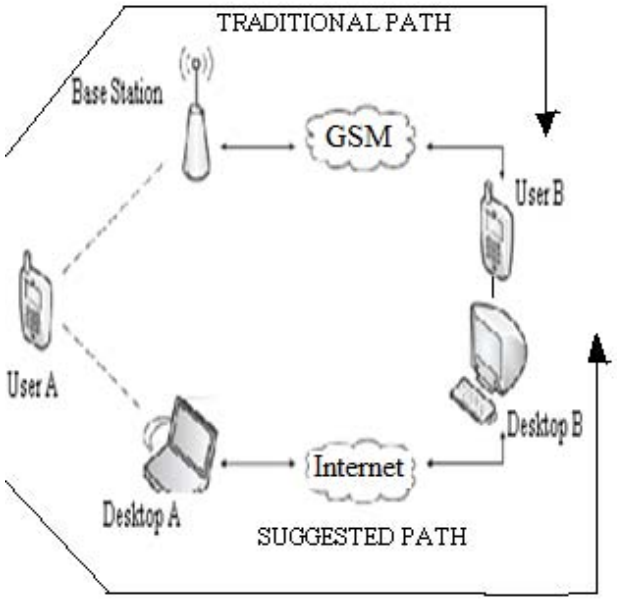


Fig. 1: System Block Diagram

Author α σ ρ : Department of Computer Engineering Sinhgad College of Engineering, Pune.
E-mail α : salunke_ajinkya@rediffmail.com
E-mail σ : prash_surya007@gmail.com
E-mail ρ : aps.apurva@gmail.com

II. System Architecture

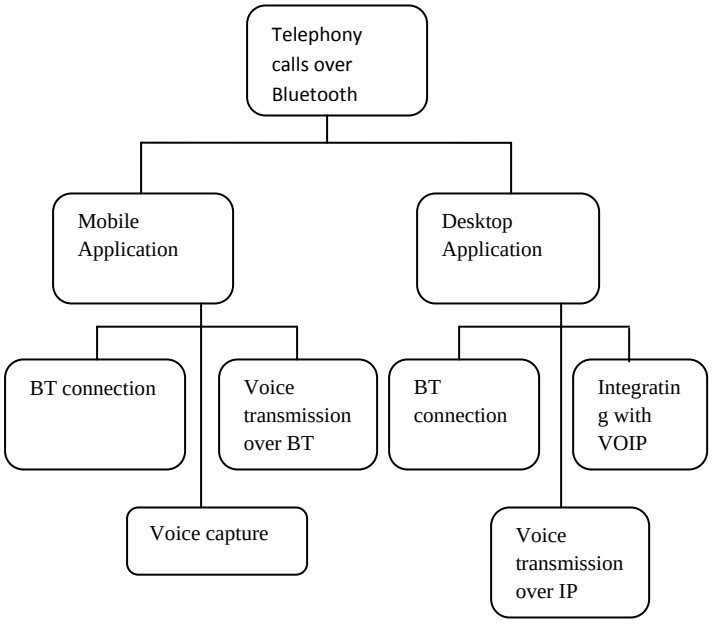


Fig. 2: Functional Decomposition

a) Mobile Application

In mobile application we have two functionalities viz. connect mobile to intended PC and capture and transfer voice.

In the former functionality the calling mobile first searches for the Bluetooth enabled PCs in range. For this purpose mobile application makes use of Service Discovery Protocol (SDP) which also returns Mac address of those PCs. After searching all the PCs in range the application connects to intended PC using the MAC address.

In later functionality the application captures real time voice using mobile multimedia API and transfers it over Bluetooth connection.

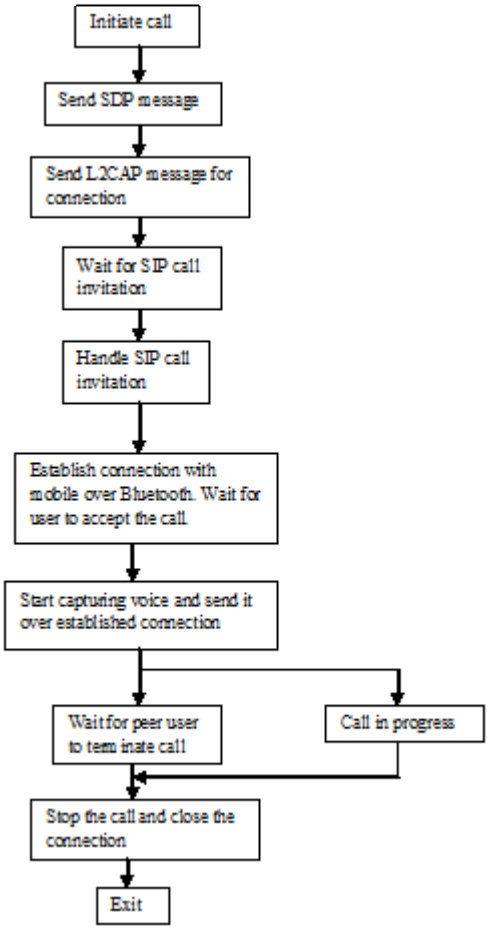
b) PC Application

In the PC application we are making use of VOICE OVER IP technology. This technology connects two PCs over Internet/Intranet and allows two systems communicate the real time data with each other.

After getting connected with mobile application, PC application starts sending and receiving data to and from corresponding mobile.

Also sender side PC application connects to receiver side PC application over intranet/internet and transfers data over established connection.

III. Work Flow



IV. Android Application

Android applications consist of loosely coupled components, bound using a project manifest that describes each component and how they interact.

There are six components that provide the building blocks for your applications:

Activities Your application's presentation layer. Every screen in application will be an extension of the Activity class. Activities use Views to form graphical user interfaces that display information and respond to user actions. In terms of desktop development, an Activity is equivalent to a Form.

Services The invisible workers of your application. Service components run invisibly, updating your data sources and visible Activities and triggering Notifications. They're used to perform regular processing that needs to continue even when your application's Activities aren't active or visible.

Content Providers A shareable data store. Content Providers are used to manage and share application databases. Content Providers are the preferred way of sharing data across application boundaries. This means that you can configure your own Content Providers to permit access from other

applications and use Content Providers exposed by others to access their stored data. Android devices include several native Content Providers that expose useful databases like contact information.

Intents A simple message-passing framework. Using Intents, you can broadcast messages system-wide or to a target Activity or Service, stating your intention to have an action performed. The system will then determine the target(s) that will perform any actions as appropriate.

Broadcast Receivers Intent broadcast consumers. By creating and registering a Broadcast Receiver, your application can listen for broadcast Intents that match specific filter criteria. Broadcast Receivers will automatically start your application to respond to an incoming Intent, making them ideal for event-driven applications.

Notifications A user notification framework. Notifications let you signal users without stealing focus or interrupting their current Activities. They're the preferred technique for getting a user's attention from within a Service or Broadcast Receiver. For example, when a device receives a text message or an incoming call, it alerts you by flashing lights, making sounds, displaying icons, or showing dialog messages. You can trigger these same events from your own applications using Notifications.

V. Conclusion and Future Work

Conclusion : We tried to study how Telephony calls over Bluetooth in conjunction with IP based network can be beneficial over GSM network. Network congestion, network unavailability problem could be totally removed with this solution. In case of critical communication this could be indispensible option as probability of internet server going down is very rare. Currently a simple application is used to send voice over IP. However tools provided by VoIP service provider can be used to achieve quality and efficiency. Long duration calls needs to be tested to exploit the communication support provided by mobile device. With this solution, dependency on service provider for mobile communication or GSM based communication is totally removed. Hence cost benefit could be achieved if the cost of IP based network is minimal.

Future Work : The implemented prototype could be enhanced to handle multiple concurrent calls. Also other communication applications like messaging, video calls could be built on the top of this application to experience mobile face to face communication in any situation. Also the GSM service provider based identity of mobile device (i.e. mobile no) could be replaced with other customized identity in conjunction with other device specific identity.

References Références Referencias

1. "SymPhone: Design and Implementation of a VoIP peer for Symbian mobile phones using Bluetooth and SIP " by Patrick Stuedi, Andreas Frei, Luc Burdet and Gustavo Alonso.
2. "System Solution for Wireless Voice and Data Access in an Enterprise Environment " -White Paper .V1.2 ,August 2002
3. "Implementing Voice over IP with Bluetooth Devices " by TOMAS LUNDQVIST ,Master's Degree Project ,Stockholm, Sweden 2009-06-24
4. http:/ / java. sun. com/ javame/ reference/ apis/ jsr135/ javax/ microedition/ media/ Manager. Html
5. "J2ME Bluetooth programming", Master's Thesis André N. Klingsheim Department of Informatics. University of Bergen. 30th June 2004.

This page is intentionally left blank

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 12 Issue 11 Version 1.0 June 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

A Novel Protocol for Barrier K-Coverage in Wireless Sensor Networks

By Majid Masoudi Nezhad, Mohammad Kherandish & Mohammad Mosleh
Islamic Azad University, Dezfoul Branch, Dezfoul, Iran

Abstract - One of major problems in the wireless sensor networks is the barrier coverage problem. This problem deals with the ability to minimizing the probability of undetected penetration through the barrier (sensor network). The reliability and fault tolerance problems are very important for long strip barrier coverage sensor networks. Also, another design challenge in sensor networks is to save limited energy resources to prolong the lifetime of wireless sensor network. In this paper we propose the fault tolerant k-barrier coverage protocol, called APBC. The proposed protocol maintains a good balance in using nodes energy, in order to prolong the network lifetime. The proposed protocol presents a proper way to provide the k-barrier coverage at nodes fails without re-executing the algorithm. The simulation results show that this method prolongs the lifetime of the network in comparison with RIS method.

Keywords : *Your Wireless Sensor Networks, barrier Coverage Protocol, Network Lifetime.*

GJCST-E Classification: *C.2.1*

Strictly as per the compliance and regulations of:

A Novel Protocol for Barrier K-Coverage in Wireless Sensor Networks

Majid Masoudi Nezhad [α], Mohammad Kherandish [σ] & Mohammad Mosleh [ρ]

Abstract - One of major problems in the wireless sensor networks is the barrier coverage problem. This problem deals with the ability to minimizing the probability of undetected penetration through the barrier (sensor network). The reliability and fault tolerance problems are very important for long strip barrier coverage sensor networks. Also, another design challenge in sensor networks is to save limited energy resources to prolong the lifetime of wireless sensor network. In this paper we propose the fault tolerant k-barrier coverage protocol, called APBC. The proposed protocol maintains a good balance in using nodes energy, in order to prolong the network lifetime. The proposed protocol presents a proper way to provide the k-barrier coverage at nodes fails without re-executing the algorithm. The simulation results show that this method prolongs the lifetime of the network in comparison with RIS method.

Keywords : Your Wireless Sensor Networks, barrier Coverage Protocol, Network Lifetime.

I. Introduction

The wireless sensor network (WSN) has emerged as a promising tool for monitoring the physical world. This kind of networks consists of sensors that can sense, process and communicate. Sensors can be deployed rapidly and cheaply, and thereby, enable large-scale and on-demands monitoring and tracking, over a wide range of applications, such as danger alerting, vehicle tracking, battlefield surveillance, habitat monitoring, etc [2].

Due to their portability and deployment, the sensor nodes are usually powered by batteries with limited capacities. And although the energy of sensor networks is slight, recharging their power sources is difficult or even impossible, usually. Thus, one of challenges in designing the sensor networks includes saving the limited energy resources to prolong the lifetime of WSN [3].

On the other hand, one of major problems in the sensor networks field is the coverage problem. This problem deals with the network ability to cover a certain area or some certain events. Various coverage formulations have been proposed in literature, among which the following three are most discussed [1]:

- Area coverage
- Point coverage
- Barrier coverage

Monitoring the whole area of the network is the main objective of area coverage problem. The objective of point coverage problem includes covering a set of stationary or mobile points, using as little sensor nodes as possible. Also, what can be considered in Barrier coverage problem is minimizing the probability of inability for intrusion detection, through a barrier sensor network [1].

For solving each problem, some algorithms have been presented. But this paper has focused on barrier coverage problem. The algorithms presented to solving this problem can be categorized into local barrier coverage algorithms and centralized ones [10]. In the first one, each node makes attempt to participate in barrier coverage, locally. This local coverage is able to provide an appropriate k-barrier coverage, in most times. a centralized barrier coverage it is run on one or more nodes in a centralized location usually near the data sink The major problem with their approach is that it is completely centralized, all sensor nodes must be able to communicate directly with the base station. This limits the scope of the network severely [17].

In another view point, the algorithms can be classified into weak barrier coverage and strong barrier coverage. The first assumes that the intruder does not know the traverse path and it will be detected with high probability, by the network. Strong barrier coverage guarantees to detect intruders no matter what crossing paths [17].

In [9], the concept of Accumulation Point Model (APM) and also a local algorithm for k-barrier coverage have been presented. In this paper, we use this concept differently, to provide a fault tolerant protocol. In the other word, a k-barrier coverage protocol, here called APBC, will be proposed. In order to prolong the lifetime of the network, the proposed protocol maintains a good balance in using nodes energies. It presents a proper way to provide the k-barrier coverage at nodes fail times, without re-executing the algorithm. Totally, a new method will be presented that try to guarantee the providing a k-barrier coverage, while decreasing the energy consumption.

Author α : Master Student of computer engineering, Islamic Azad University, Dezfoul Branch, Dezfoul, Iran.
E-mail : m.masudi@gmail.com
Author σ : Departement of Computer Engineering Dezfoul Branch Islamic Azad University Dezfoul Iran. E-mail : kheirandish@iaud.ac.ir.
Author ρ : Departement of Computer Engineering Dezfoul Branch Islamic Azad University Dezfoul Iran. E-mail : m.mosleh@iaud.ac.ir

For the purpose of this paper, it has been organized as follows: In Section II, we present some definitions, background, and related works. In Section III, we will present our Network Model and Section IV, has been dedicated to describing our Proposed Protocol. In Section V, we present the results of our simulations and finally, we will conclude the paper in Section VI. here.

II. Preliminary and Network Model

Your Some of local barrier coverage algorithms have been introduced in [5, 6, 9, 10, 13]. And [1, 4, 11] have introduced the centralized algorithms. One of algorithms for local barrier coverage, called RIS, has been presented in [13]. This algorithm is based on a power saving method, in which the sensor nodes are scheduled and switch between two modes, Active and Sleep. RIS provides a weak barrier coverage with the high probability of intrusion detection, in such a way that each sensor, in certain periods, selects Active or Sleep mode, with a predetermined probability rate, P. As mentioned earlier, the presented method will be based on the power saving method, used by RIS. However, the modes considered in sensor nodes have been changed to Active and Passive modes. It must be noticed that RIS does not guarantee the barrier coverage, deterministically. Also, if the deployment does not follow random uniform or Poisson distribution, and the lifetimes of the sensor nodes are not the same, there is no guidance on how to choose a value for P.

Furthermore, a directed algorithm, called CoBRA has been introduced in [5] to provide the barrier coverage in wireless Camera Sensor Networks (WCSN).And the algorithm presented in [6] coordinates the nodes moves in mobile sensor networks, to provide the barrier coverage. A proper way has been introduced in [7, 8] to providing a 3-dimentional barrier coverage, for under water 3-dimentional sensors.

But the network model used in [9] has been considered in this paper. In this model, a barrier area is considered to be covered which is a physical long strip region in optional shape (see Fig. 1). In such a model, it is assumed that each node knows its own location in the network and has a disk-like sensing region, with radius R. Although radio radiuses of nodes are not same and are integrated in real world, it is possible to ignore the differences in sensing radiuses, while evaluating the coverage in wireless sensor networks, in large scale.

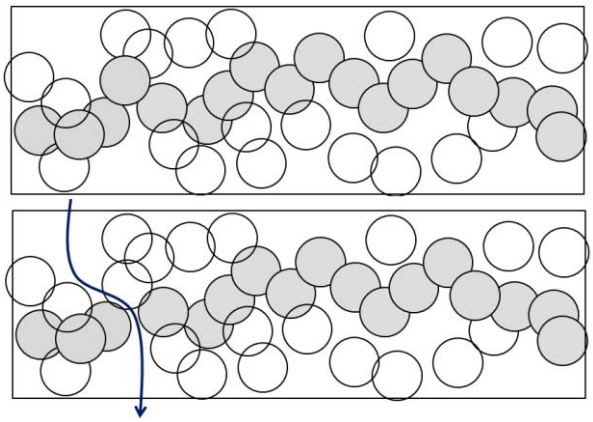


Figure 1: The reliability problems are very important for barrier coverage

The relationship between sensing radius of each node, RS, and its transition radius, R_t, can be described with $R_t \leq 2R_S$ [16]. As a result, when two nodes can communicate with each other, also their sensing areas overlap, certainly. So these two nodes will be able to provide the strong coverage by keeping themselves active. Thus the coverage can imply the connectivity (see Fig. 2). So we will focus on the coverage problem, only.

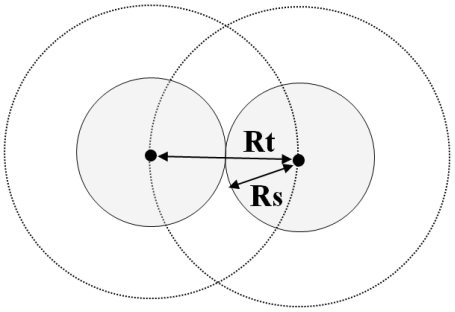
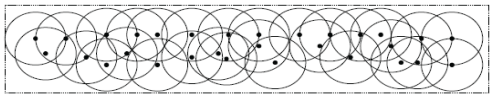


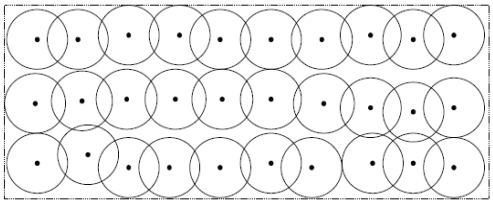
Figure 2: The transmission radius of sensor nodes is assumed to be at least twice the sensing range

On the other hand, according to different energy consumption models, the energy consumed by an sensor node, while dealing with a sensing task, is proportional to RS2 or RS4, where RS is the sensing radius of the sensor node [3] [17]. When the sensor node is sleeping, the consumed power is considered as zero [3]. In this paper, we take the sensing energy consumption as u.RS2, where u is a positive constant.

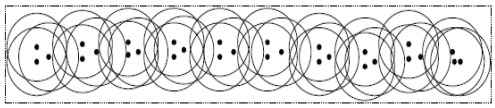
For analyzing the energy consumption, briefly, only the energy consumed by the sensing and transition functions (excluding the power consumption by calculations) has been considered here. Three consumption models, including APM, IBM and RPM have been introduced in [9] for nodes deployment (see Fig. 3).



(a) Random Point Model



(b) Independent Belt Model



(c) Accumulation Point Model

Figure 3: Deployment Models in Barrier Coverage Sensor Networks

Some of definitions required to explaining the presented method are as following:

Coverage Graph: The coverage graph of a sensor network is denoted by G= (V, E), in which each node is supposed to be associated with a vertex in vertices set (V). Each two nodes located in transition areas of each other, are considered as Neighbors, and an edge in edges set (E) is assumed between their associated vertices. In Fig. 4 and Fig. 5, a sensor network and its coverage graph have been shown. The relationship between the vertices and the edges can be described by Eq. (1).

$$\forall u, v \in V \quad \text{If } d_{uv} \leq R \Rightarrow e_{uv} \in E \qquad (1)$$

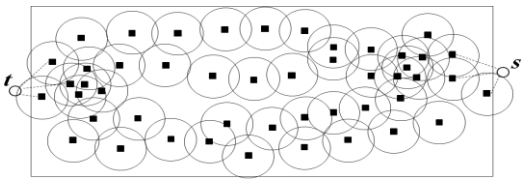


Figure 4: A Sensor network

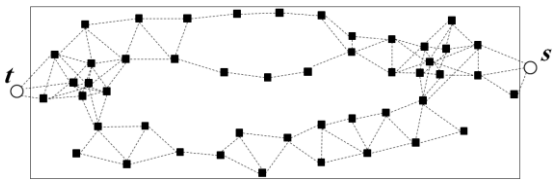


Figure 5: The coverage graph for the sensor network shown in Fig. 4

Barrier Belt: A barrier belt, τ , is a sub-graph $G\tau = (V\tau, E\tau)$ of the coverage graph, G = (V , E), and can be described by Eq. (2).

t, s∈ V τ

∀τ j contains distinct vertex set

V τ j = {s, v1, v2, v3,…, vi ,…, vnj ,t}

$$E\tau j = \{es\ v1, e\ v1\ v2, \ldots, e\ vi\ vi+1, \ldots, e\ nj\ t\} \qquad (2)$$

Where the edge set, E τ j = {es v1, e v1 v2 ,…, e vi vi+1 ,…, e nj t } forms a path, beginning at s toward t. nj ≤ |V|-2, in which the edges set , E τ forms a path from s to t : nj ≤ |V|-2

k-barrier Graph: A barrier graph, Gb= (Vb , Eb) is a sub-graph of coverage graph, where:

$$\forall \tau i, \tau j \subseteq G \text{ iff } V\tau i \cap V\tau j = \{s,t\} \cup H,\ H \subseteq M$$

$$, \forall vi \in H \Rightarrow vi \in M$$

where $G\tau j = (V\tau i , E\tau i) , G\tau j = (V\tau j , E\tau j)$

and H={v1 , v2 , … , vw}

and $M = V\tau 1 \cup V\tau 2 \cup V\tau 3 \cup \ldots \cup V\tau k$

and k ≥ 2 (3)

Accumulation Point: An accumulation point is a sub-graph, Ga= (Va, Ea), of a sensor network barrier graph G= (V, E), given the following (Fig. 6).

$$\text{If } v \in V_a \Rightarrow \forall u \in V_a , euv \in E_a \qquad (4)$$

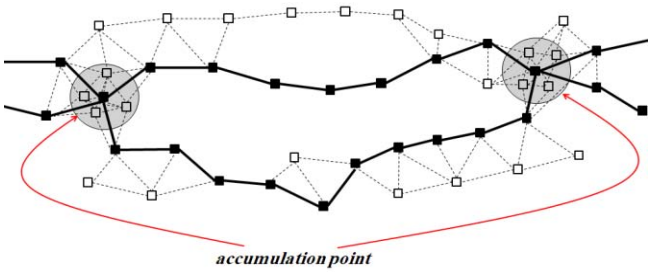


Figure 6: k-barrier coverage and two Accumulative Point

Node state: Each node, regarding whether it is the member of k-barrier graph, Gb=(Vb,Eb), and is the member of a Accumulation Point or not, has one of the modes mentioned bellow:

- Active-Accumulative
- Active-none Accumulative
- Sleep-Accumulative
- Sleep-none Accumulative.
- This template

III. The Proposed Protocol

As mentioned earlier, the main problem to be solved includes providing a k-barrier graph which creates and describes a k-barrier coverage in a barrier area. As a result, all paths crossing through the barrier area are covered k-times, by the network sensors.

The proposed method consists of three phases named startup phase, k-coverage creation phase and maintenance & recovery phase.

a) Starup Phase

At startup phase, the nodes recognize their neighbors, and the coverage graph, G= (V, E) is created. For this purpose, by sending a "hello"message,

each node introduces itself to its neighbors. After receiving this message, each node knows its neighbors and then by sending a special package (my-neighbors) presents its neighbors list to its all neighbors. So, after receiving the neighbors list from all neighbors, each node can find out whether it is a member of one or several accumulation points, G= (Va , Ea).

b) K-coverage Creation Phase

In this phase, a K-barrier graph, Gb=(Vb ,Eb) is created. So, k barrier belts, $G\tau = (V\tau , E\tau)$, should be created. For this purpose, one of the leftmost nodes that is the neighbor of virtual node, s, in the sensor network coverage graph, G= (V, E), is selected as the first node of barrier belt. Then the selected node selects the next node among its neighbors, to create the barrier belt. This process continues until the last virtual node, t, is reached.

Thus, whenever the proposed method is performed, one node is selected to create barrier belt between two virtual nodes, t and s, in the network graph. This process is repeated k-times and finally, the set of these nodes forms k-barrier graph, Gb= (Vb , Eb). In order to select the next node for barrier belt creation, each node (except active-none Accumulative ones) selects the next node among its neighbors, as following:

- If the node is not an Accumulation Point, it will select a next node among the neighbors being Accumulation Point members, such that the selected node has the least distance from the virtual node, t, too. But if there is no neighbor being Accumulation Point member, the node will select a neighbor with least distance from the virtual node, t, as the next node.
- If the node is an accumulation point member, it will select a neighbor with least distance from the virtual node, t, as the next node.

Each node, after selecting its neighbor as the next node, will inform it about this selection, by sending elect-you message. This process continues until reaching the virtual node, t.

c) Maintenance & Recovery Phase

In this phase, we try to maintain and recover the k-barrier graph coverage, G=(Vb, Eb), by using Accumulation Points created in k-barrier graph. This phase consists of two main works: first, the creation of new barrier belt and the second, recovering the fault barrier belt.

i. *Creating New Barrier Belt*

Each Active-Accumulative node creates a new barrier belt in certain periods until next Active-Accumulative node.

Therefore, barrier belts change continuously during network lifetime, in such a way that all sensor network nodes are used equally. For this purpose, each Active-Accumulative node sends a findNextAP message to the next active node, in certain periods. The mentioned message includes node location and ID card. Each node, after receiving this message, sends it to the next active node, until the message reaches the next active-accumulative node. The second Active-Accumulative node, after receiving the message, begins to create a barrier belt between itself and the first Accumulation Point, by using an algorithm such as that in k-barrier coverage creation phase.

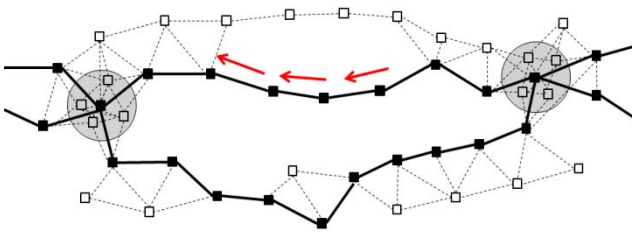
The only difference between these algorithms, surely very important, is considering both accumulative nodes instead of virtual nodes, s and t. Finally, the first Active-Accumulative node sends the inactive message to the next node. Each node, after this message, first sends it to the next active node and then goes to sleep mode.

This process continues until the message reaches the second Accumulation Point node and the previous barrier belt between these two Accumulation Points is removed. Fig.7 shows the process.

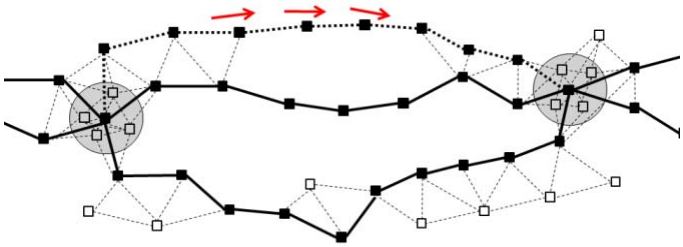
Considering this fact that the Active-Accumulation nodes perform as center and are active, always, their energy are consumed after a period of time. So, for this reason, each accumulation node, after a time period when the probability of node fail is high, replaces itself with one of the neighbor sleep-accumulation nodes, whenever it is informed about existence of such this neighbor. Each node, after receiving the message, changes into sleep mode and sends the message to the next node in barrier graph.

ii. *Reparation Fault Barrier Belt*

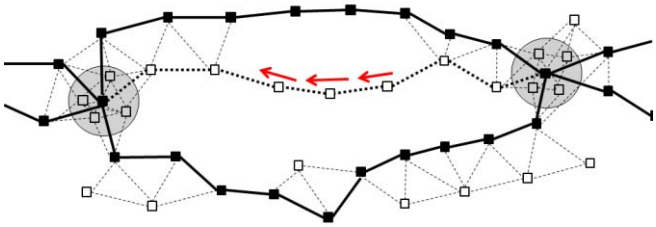
This process continues until the message reaches the first Active-Accumulation node. Then, after receiving this package, the next Active-Accumulative node begins to create a barrier belt between itself and the previous Accumulation Point. This is done by using an algorithm such as that used in k-barrier coverage phase. The only difference in executing this algorithm is considering the coordinates of both Accumulation nodes instead of virtual nodes, s and t. This process is shown in Fig. 8.



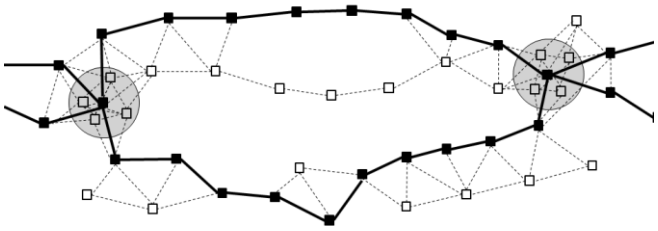
(A) Find Next AP Package



(B) Elect You Package



(C) Switch Inactive Package



(D) Modified $G_b = (V_b, E_b)$

Figure 7: Creating new Barrier Belt

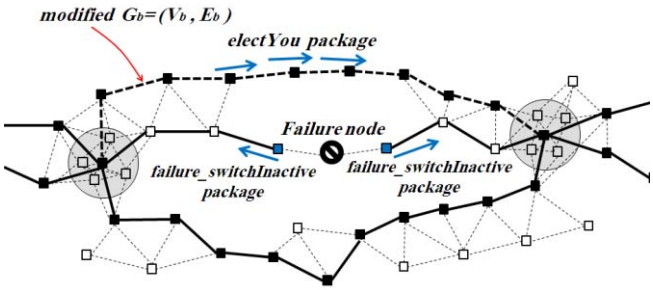


Figure 8: The Reparation Fault Barrier Belt

IV. Simulation Results

In this section, the proposed protocol has been simulated using Matlab and compared with RIS algorithm. We set the barrier area length as 2km which is supposed to be covered with 1500 nodes. Then the nodes are deployed randomly along the area. The width of barrier area, in different configurations, has been considered as 120m, 90m, 60m and 30m, respectively. Therefore, the nodes deployment density parameter will be 0.00625, 0.00833, 0.0125 and 0.025 nodes per m^2.

Notice that by more density, we don't mean using more sensor nodes and spending more different mode of nodes deployment. Considering that the nodes deployments are random, if thewidth of barrier region is considered less, the nodes deployment model will tend to APM model. We set transition and sensing radius of nodes as Rt=50m and RS=25m, respectively. The life time of nodes is assumed to be 60 days.

a) First Expriment

In this experiment, we evaluate how the proposed protocol leads to prolong the network lifetime by selecting the proper nodes for performing k-barrier coverage. In simulations, the probability of each node to fail before ending its lifetime, is considered as $\rho=0.07$. The simulation result has been presented in Fig.9.

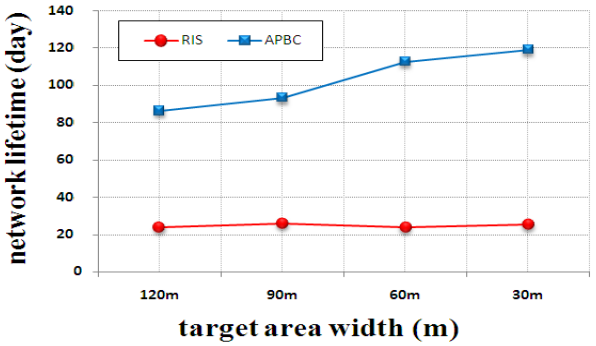


Figure 9: The proposed protocol leads to prolong the network life time by selecting the proper nodes for performing k-barrier coverage

b) Secend Expriment

Via the simulation, we evaluate the effect of nodes fails probabilities, before ending their lifetime, on the network lifetime, in whole. In various experiments, the probability of a node fail, before ending its lifetime, is considered as $\rho=0.07$, $\rho=0.13$ and $\rho=0.21$. The simulation results have been presented in Fig. 10. As shown, the performance of the proposed protocol doesn't change so much, while increasing the parameter ρ. The reason is that the proposed protocol, when a link fails, begins to recover the k-barrier graph and provide k-barrier coverage without re-executing the algorithm, completely. Therefore, there is no need to exchange the message and consume energy for re-executing the algorithm.

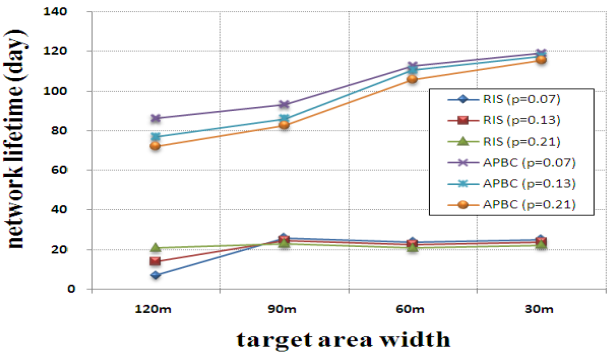


Figure 10: The performance of the proposed protocol doesn't change so much while increasing parameter ρ

Regarding the different slopes in diagrams, it is clear that more density in deployment, near to APM model, can yield to a more efficiency of protocol to maintain a balance in using nodes energies. Also, its efficiency for both recovering k-barrier coverage and fault tolerance will improve; because deploying a more density cause the proposed protocol to be more reliable in using the nodes energy, equally. Moreover, while failing nodes, it begins to recover k-barrier coverage, easily and with less massage overhead.

V. Conclusion

In this paper we proposed a k-barrier coverage protocol, called APBC, for prolonging the network lifetime. The proposed protocol tries to prolong the network lifetime by establishing a balance in using nodes energies. Moreover, the proposed protocol presents a proper way in which the nodes fail without re-executing the algorithm andconsuming much energy. According to simulation result, the proposed protocol, APBC, prolong the network lifetime in comparison with RIS method.

References Références Referencias

1. M. Ilyas, I. Mahgoub, Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems, CRC Press, London, Washington, DC, 2005.
2. Jie Jia, Jian Chena, Guiran Changa, Zhenhua Tana, "Energy efficient coverage control in wireless sensor networks based on multi-objective genetic algorithm" ,Elsevier , Computers and Mathematics with Applications 57, pp. 1756_1766, 2009.
3. Jie Jia, Jian Chena, Guiran Changa, Yingyou Wena, Jingping Songa,c,"Multi-objective optimization for coverage control in wireless sensor network with adjustable sensing radius", Elsevier, Computers and Mathematics with Applications 57 pp. 1767_1775. (2009).
4. S. Kumar, T. H. Lai, and A. Arora, "Barrier coverage with wireless sensors". In Proc. ACM Mobicom, 2005.
5. Kuei-Ping Shih, Chien-Min Chou, I-Hsin Liu, and Chun-Chih Li. "On Barrier Coverage in Wireless Camera Sensor Networks", 1550-445X/10 $26.00 © 2010 IEEE.
6. Teddy M. Cheng and Andrey V. Savkin. "A Distributed Self-Deployment Algorithm for the Coverage Mobile Wireless Sensor Networks", IEEE COMMUNICATIONS LETTERS, VOL. 13, NO. 11, NOVEMBER 2009.
7. Stanley Barr, Benyuan Liu, and Jie Wang, "Barrier Coverage For Underwater Sensor Networks", 978-1-4244-2677-5/08/$25.00 c 2008 IEEE
8. Stanley Barr, Benyuan Liu, and lie Wang. "Constructing Underwater Sensor Based Barriers Using Distributed Auctions", 978-1-4244-5239-2/09/$26.00 ©2009 IEEE
9. Yong Lin, Zhengyi Le, Fillia Makedon, "Accumulation Point Model for Barrier Coverage",978-1-4244-6314-5/09/$26.00 ©2009 IEEE.
10. Ai Chen, Santosh Kumar,"Local Barrier Coverage in Wireless Sensor Networks", 1536-1233/10/$26.00 _ IEEE 2010.
11. Li Zhang, Jian Tang, Weiyi Zhang, "Strong Barrier Coverage with Directional Sensors", 978-1-4244-4148-8/09/$25.00 IEEE ©2009.
12. M. E. Posner S. Kumar, T. H. Lai and P. Sinha. "Optimal sleep wakeup algorithms for barriers wireless sensors".In Fourth International Conference on Broadband Communications, Networks, and Systems, Raleigh, NC, 2007.
13. Santosh Kumar, Ten H. Lai, J´ozsef Balogh. "On k-Coverage in a Mostly Sleeping Sensor Network", MobiCom'04, Sept. 26-Oct. 1, 2004, Philadelphia, Pennsylvania, USA. Copyright 2004 ACM 1-58113-868-7/04/0009.
14. H. Zhang, and J.C. Hou, "Maintaining sensing coverage and connectivity in large sensor networks", in: Ad-hoc and Sensor Wireless Networks 1 (2005), pp. 89-124.
15. M. Lu, J. Wu, M. Cardei, and M. Li, "Energy-efficient connected coverage of discrete targets in wireless sensor networks", in: Proc. of the International Conference on Computer Networks and Mobile Computing, ICCNMC, Zhangjiajie, China, 2005, pp. 43-52.
16. B. Liu, O. Dousse, J. Wang, and A. Saipulla, "Strong Barrier Coverage of Wireless Sensor Networks," Proc. ACM MobiHoc, 2008
17. Raymond Mulligan and Habib M. Ammari "Coverage in Wireless Sensor Networks: A Survey.

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 12 Issue 11 Version 1.0 June 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Wireless Adhoc Networks Security Principles, Issues & Applications

By Ramesh Kait, Kuldeep Kherwal & C. Nelson Kennedy Babu
Singhania University Rajsthan

Abstract - Privacy and integrity of packets on WANetworks should be expected by the algorithmic mechanisms. This privacy and integrity is very much is to be mandated by regulations. In tradition the security is only based on cryptographic techniques which is not so much secure and leads to unsecure and unauthenticated information. As the packets of information are to be routed on networks so it needs some new security and digital signature based algorithm. A digital signature method provides the solution to many of these new concerns. So in this paper we will discuss new paradigm of digital signature based techniques along with merit & demerits, applications and issues related with it.

Keywords : *Digital Signature,Cryptography, Security, RSA , Hash Function.*

GJCST-E Classification: *C.2.1*

Strictly as per the compliance and regulations of:

Wireless Adhoc Networks Security Principles, Issues & Applications

Ramesh Kait [α], Kuldeep Kherwal [σ] & C. Nelson Kennedy Babu [ρ]

Abstract - Privacy and integrity of packets on WANetworks should be expected by the algorithmic mechanisms. This privacy and integrity is very much is to be mandated by regulations. In tradition the security is only based on cryptographic techniques which is not so much secure and leads to unsecure and unauthenticated information. As the packets of information are to be routed on networks so it needs some new security and digital signature based algorithm. A digital signature method provides the solution to many of these new concerns. So in this paper we will discuss new paradigm of digital signature based techniques along with merit & demerits, applications and issues related with it.

Keywords : Digital Signature, Cryptography, Security, RSA, Hash Function.

I. Introduction

With the advent of wireless network as packet radio networks in the 1970's, it became an interesting research subjects in computer world [1, 2, 5, 7, 12], and in these three fold decades tremendous improvement is made in the research. Wireless adhoc networks are a new paradigm of wireless communication for mobile hosts (which we call nodes). Wireless communication devices, could form an ad hoc network when they roam in a battlefield. Wireless networks can also be used for emergency, law enforcement, and rescue missions. Since an ad hoc network can be deployed rapidly with relatively low cost, it becomes an attractive option for commercial uses such as sensor networks or virtual classrooms.

II. Issues of Security

As security is a complex objective, in order to achieve this objective, the issues is to be clearly defined:

- **Authentication:** Are user who they say they are?
- **Access Privileges:** What applications and information can a particular user read, writes, or modify?
- **Accountability:** Did the person responsible for the information?
- **Traceability:** What is the change and review history of the information?

There can be a sure attack on the wireless adhoc network system because the attackers always think a one step ahead to the network designer, so there must be some security design to achieve the security objective.

III. Concept of Secure System Model

In order to maintain the security of wireless adhoc network using digital signature technique is very much suitable because it is based on mathematical formula and enables the unauthenticated person to break it very hard. A **digital signature/Scheme** is a mathematical scheme [5, 6, 8, 9] for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that it was not altered in transit. Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery/Tempering.

IV. Encryption for Privacy

Encryption refers to algorithmic schemes that encode plain text into non-readable form or Cipher text, providing privacy. The receiver of the encrypted text uses a "key" to decrypt the message, returning it to its original plain text form. The key is the trigger mechanism to the algorithm.

Until the advent of the Internet, encryption was rarely used by the public, but was largely a military tool. Today, with online marketing, banking, healthcare and other services, even the average householder is aware of encryption.

There are many types of encryption and not all of it is reliable. The same computer power that yields strong encryption can be used to break weak encryption schemes. Initially, 64-bit encryption was thought to be quite strong, but today 128-bit encryption is the standard with DES Schemes, and this will undoubtedly change again in the future. The **figure1.0** gives the process of the scheme how it works. There can be the two techniques of Cryptography can be used the description is as bellows

General Description of Symmetric (Private Key) Cryptography also known as most popular Symmetric

Author α : Department of Computer Science & Applications Kurukshetra University Kurukshetra. E-mail : rameshkait@kuk.ac.in
Author σ : Research Scholar, Singhania University Rajasthan. E-mail : ks.kherwal@gmail.com
Author ρ : PG Computer Science & Engineering,Shri Sowdambiga College of Engineering, Aruppukottai,Tamilnadu. E-mail : cnkbabu63@yahoo.in

Key is also known as DES i.e. Data Encryption Standard is as

- *k* is the key agreed on beforehand by A and B
- *m* is the message to be sent from A to B
- *Ek* is the encryption algorithm using key *k*,
- *Dk* is the decryption algorithm using key *k*

A sender encrypts message *M* using *Ek* (*m*) and sends it to B Receiver,

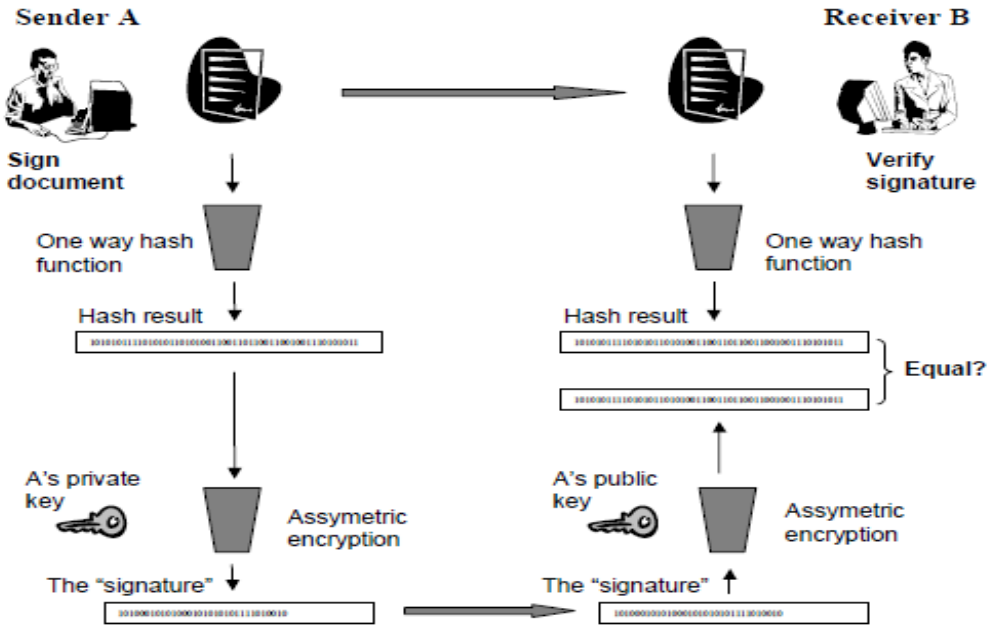


Fig. 1.0 : Digital Signature Processing Scheme

B decrypts using *Dk* (*Ek* (*m*)) and recovers the message *M* & incase of the Asymmetric (Public Key) Cryptography

- *m* is the message to be sent from A and B,
- *Eb* is the encryption algorithm using B's public key,
- *Db* is the decryption algorithm using B's private key.

A sender encrypts the message *m* using *Eb* (*m*) and transmits the results to B,

B decrypts using *Db* (*Eb* (*m*)) and recovers the message *m.*

As the above figure 1.0 shows that the digital signature is formed in two ways. First, A computes the hash value of her message; next, she encrypts the hash value with her private key. Upon receipt of the digital signature, B recovers the hash value calculated by A by decrypting the digital signature with A's public key. B can then apply the hash function to A's original message, which he has already decrypted. If the resultant hash value is not the same as the value supplied by A, then B knows that the message has been altered; if the hash values are the same, B should believe that the message he received is identical to the one that A sent.

This scheme also provides Non repudiation since it proves that A sent the message; if the hash value recovered by B using A's public key proves that the message has not been altered, then only A could have created the digital signature. B also has proof that he is the intended receiver; if he can correctly decrypt the message, then he must have correctly decrypted the session key meaning that his is the correct private key. Symmetric key (also called private key or secret key) cryptography [7, 8] uses the same key to encrypt and decrypt. The name "private key" derives from the need to keep the key private. A major challenge associated with symmetric key cryptosystems is the secure distribution of keys. Asymmetric key encryption (also called public key encryption) uses two keys: a public and a private key. Data encrypted with one key can be decrypted only with the other key. Asymmetric cryptography solves the challenge of secure distribution of secret keys.

Anyone with the public key can use it to perform a validity check of digital signatures created by the private key. Only a digital signature created by the appropriate private key decrypts and validates properly with the public key. If a different private key was used to sign the data, the validity check fails. If the contents of digitally signed data or the digital signature have been tampered with or are corrupted, the validity check also fails. Valid digital signatures can be used to perform the following functions:

1st Authenticate online entities, 2nd Verify the genuineness or origin of digital data and, 3rd Ensure the integrity of digital data against tampering.

Advantage of Digital signature is eliminating the possibility of committing fraud by an imposter signing since the digital signature cannot be altered, this makes forging the signature impossible. Beside this it helps in legal requirement and message integrity also. But implementation of this scheme is costly.

Disadvantage of encrypting all data to provide a digital signature is impractical for three reasons:

- The cipher text signature is the same size as the corresponding plaintext, so message sizes are doubled, consuming large amounts of bandwidth and storage space.
- Public key encryption is slow and places heavy computational loads on computer processors, so network and computer performance can be significantly degraded and to overcome these issues we use Digital signature using RSA.

V. Hash Function

A hash function takes a block of data, generally called the message, and returns a fixed-size string, which can be called the hash, hash value or message digest. The main reason for creating a hash value of a message is that any accidental or intentional change to it will result in a completely different hash value. Hashes are not unique. A good hash function should produce message digests that are impossible to brute force in a reasonable amount of time. The hash function should also have statistically evenly distributed collisions. This is called strong collision resistance.

Some properties of a good cryptographic hash function are:

- It is easy to compute the hash value for any given message.
- It is very difficult to find a message that has a given hash.
- It is also very difficult to modify a message without the hash being changed.
- It is not possible to find two different messages with the same hash.
- It can apply to any block size of data.
- It should produce a fixed-length of output data

Hash algorithms that are in common use today are:

- *Message Digest (MD) algorithms:* A series of byte-oriented algorithms that produce a 128-bit hash value from an arbitrary-length message.
- *Secure Hash Algorithm (SHA):* Algorithm for NIST's Secure Hash Standard (SHS). SHA-1 produces a 160-bit hash value
- *RIPEMD :* A series of message digests and 128-bit hash functions.
- *HAVAL (Hash of Variable Length) :* a hash algorithm with many levels of security. It can create hash values that are 128, 160, 192, 224, or 256 bits in length.
- *Whirlpool :* A relatively new hash function .It operates on messages less than 2^{256} bits in length, and produces a message digest of 512 bits.

VI. One Way Hash Function

The main role of hash function is in provision of digital signature. Hash functions are faster than digital signature. One-way chains are an important cryptographic primitive in many security applications. As one-way hash functions are very efficient to verify, they recently became increasingly popular for designing security protocols for resource-constrained mobile devices and sensor networks, as their low-powered processors can compute a one-way function within milliseconds, but would require tens of seconds or up to minutes to generate or verify a traditional digital signature [1]. A one way function is a mathematical function that is significantly easier to perform in one direction .Despite the computational efficiency of one-way functions, one-way hash function is still challenging to use in resource-constrained environments, such as on small mobile devices or sensor networks. Especially some of the proposed sensor networks have significant resource limitations, as they use minimal hardware to lower the energy consumption [2]. Generally all modern hash algorithms produce hash values of 128 bits and higher .Sometime called Trapdoor functions also.

VII. Fully Hash Function

The Full Domain Hash (FDH) is an RSA-based signature [9, 12, 13] scheme that follows the *hash-and-sign* paradigm. It is more secure than one way hash function. In the RSA digital signature process, the private key is used to encrypt only the message digest. The encrypted message digest becomes the digital signature and is attached to the original data. To verify the contents of digitally signed data, the recipient generates a new message digest from the data that was received, decrypts the original message digest with the originator's public key, and compares the decrypted digest with the newly generated digest. If the two digests match, the integrity of the message is verified. The identity of the originator also is confirmed because the public key can decrypt only data that has been encrypted with the corresponding private key. RSA rely upon ``Key Certification Authority'' (CA) that is responsible for issuing and/or certifying keys. The primary role of a key certification authority is to provide assurance that a user's public key is accurate. It is used in most of applications around the world.

Advantage of RSA is that it can recover the message digest from signature.

Disadvantage of RSA is that, it's a time consuming process and create a problem when M> n situation arise, where M is message and n is Block length.

For resolve this problem we should use Hash and sign at a time. There are several reasons to sign such a hash (or message digest) instead of the whole document.

- *For efficiency:* The signature will be much shorter and thus save time since hashing is generally much faster than signing in practice.
- *For compatibility:* Messages are typically bit strings, but some signature schemes operate on other domains (such as, in the case of RSA, numbers modulo a composite number N). A hash function can be used to convert an arbitrary input into the proper format.
- *For integrity*. Without the hash function, the text "to be signed" may have to be split (separated) in blocks small enough for the signature scheme to act on them directly. However, the receiver of the signed blocks is not able to recognize if all the blocks are present and in the appropriate order.

RSA is used in verification than signing because RSA public exponent is usually smaller than RSA private exponent. this is desirable because a message is signed by individual only once but check for verification several times .hence , RSA signature verification is faster .RSA allow both the public and private key to be used for encryption. If a message is encrypted with someone's private key it can only be decrypted with the corresponding public key. This feature can be used to create digital signatures

VIII. Proposed Plan for Security Mechanisms

We proposed solution for the authenticated broadcasting in wireless network to achieve many security goals for many applications that has to be achieved. Some of the measures that can be incorporated are:

- **One way Hash Function:** it is like checksum of a block of text and is secure in, that it is impossible to generate the same hash function value without knowing the correct algorithm and key. It should use for generate digital fingerprints and for encrypt password for operating system.
- **FDH (Full hash function):** FDH is a RSA based signature scheme included hash and sign at a time and use key certification authority for key management.
- **Digital Signature:** External attack can be checked using confidentiality of routing information and also by authentication and integrity assurance features. Digital signature is used for protecting data form compromised nodes.

IX. Conclusion

Hash functions, for example, are well-suited for ensuring data integrity because any change made to the contents of a message will result in the receiver calculating a different hash value than the one placed in the transmission by the sender. Since it is highly unlikely that two different messages will yield the same hash value, data integrity is ensured to a high degree of confidence. The value of hash function is should be long enough to protect attacks. Secret key cryptography, on the other hand, is ideally suited to encrypting messages, thus providing privacy and confidentiality. The sender can generate a *session key* on a per-message basis to encrypt the message; the receiver, of course, needs the same session key to decrypt the message. Asymmetric schemes can also be used for non-repudiation and user authentication; if the receiver can obtain the session key encrypted with the sender's private key, then only this sender could have sent the message. Public-key cryptography could, theoretically, also be used to encrypt messages although this is rarely done because secret-key cryptography operates about 1000 times faster than public-key cryptography. In last , we suggest for Hash and RSA scheme combination. Further improvement is PKI public key infrastructure is key management to ensure safe public key i.e. signature verification key. It improves WANetworks system effectiveness and efficiency and is the solution for the problem, how to ensure public key signature verification.

X. Bibliography

1. M. Brown, D. Cheung, D. Hankerson, J. Hernandez, M. Kirkup, and A. Menezes. PGP in constrained wireless devices. In Proceedings of the 9th USENIX Security Symposium, pages 247-261. USENIX, August 2000.
2. J. M. Kahn, R. H. Katz, and K. S. Pister, "Mobile networking for smart dust", In ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom'99), Seattle, WA, August99.
3. Weimerskirch A, Westhoff D, "Zero common-knowledge authentications for pervasive networks" In: Selected Areas in Cryptography. (2003) 73–87
4. O'Shea G, Roe M, "Child-proof authentication for mipv6 (cam)" SIGCOMM Computer. Communication Rev. 31 (2001) 4–8
5. Montenegro, G., Castelluccia, C, "Statistically unique and cryptographically verifiable (sucv) identifiers and addresses" In: Proceedings of the Network and Distributed System Security Symposium (NDSS). (2002)
6. Shamir, A, "Identity-based cryptosystems and signature schemes" In: Proceedings of CRYPTO '84, Springer-Verlag (1984) 47–53

7. Boneh, D., Franklin, M, "Identity-based encryption from the weil pairing" In: Proceedings of CRYPTO 2001, Springer-Verlag (2001) 213–229
8. Cocks, C, "An identity based encryption scheme based on quadratic residues" In: Proceedings of IMA 2001, Springer-Verlag (2001) 360–363.
9. Jochen Schiller. , Mobile Communications, Addison-Wesley 2000.
10. Krishna Moorthy Sivalingam, "Tutorial on Mobile Ad Hoc Networks", 2003.
11. Elizabeth M. Royer and Chai-Keong Toh, "A review of current routing protocols for adhoc mobile wireless networks" Technical report, University of California and Georgia Institute of Technology, USA, 1999.
12. Mobile Ad Hoc Networking Working Group – AODV, http://www.ietf.org/rfc/rfc3561.txt
13. Mobile Ad Hoc Networking Working Group – DSR, http://www.ietf.org/rfc/rfc4728.txt.

Global Journals Inc. (US) Guidelines Handbook 2012

www.GlobalJournals.org

FELLOW OF ASSOCIATION OF RESEARCH SOCIETY IN COMPUTING (FARSC)

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

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

MEMBER OF ASSOCIATION OF RESEARCH SOCIETY IN COMPUTING (MARSC)

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

AUXILIARY MEMBERSHIPS

ANNUAL MEMBER

- Annual Member will be authorized to receive e-Journal GJMBR for one year (subscription for one year).
- The member will be allotted free 1 GB Web-space along with subDomain to contribute and participate in our activities.
- A professional email address will be allotted free 500 MB email space.

PAPER PUBLICATION

- The members can publish paper once. The paper will be sent to two-peer reviewer. The paper will be published after the acceptance of peer reviewers and Editorial Board.

Process of submission of Research Paper

The Area or field of specialization may or may not be of any category as mentioned in 'Scope of Journal' menu of the GlobalJournals.org website. There are 37 Research Journal categorized with Six parental Journals GJCST, GJMR, GJRE, GJMBR, GJSFR, GJHSS. For Authors should prefer the mentioned categories. There are three widely used systems UDC, DDC and LCC. The details are available as 'Knowledge Abstract' at Home page. The major advantage of this coding is that, the research work will be exposed to and shared with all over the world as we are being abstracted and indexed worldwide.

The paper should be in proper format. The format can be downloaded from first page of 'Author Guideline' Menu. The Author is expected to follow the general rules as mentioned in this menu. The paper should be written in MS-Word Format (*.DOC,*.DOCX).

The Author can submit the paper either online or offline. The authors should prefer online submission.Online Submission: There are three ways to submit your paper:

(A) (I) First, register yourself using top right corner of Home page then Login. If you are already registered, then login using your username and password.

(II) Choose corresponding Journal.

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

(B) If you are using Internet Explorer, then Direct Submission through Homepage is also available.

(C) If these two are not convenient, and then email the paper directly to dean@globaljournals.org.

Offline Submission: Author can send the typed form of paper by Post. However, online submission should be preferred.

Preferred Author Guidelines

MANUSCRIPT STYLE INSTRUCTION (Must be strictly followed)

Page Size: 8.27" X 11'"

- Left Margin: 0.65
- Right Margin: 0.65
- Top Margin: 0.75
- Bottom Margin: 0.75
- Font type of all text should be Swis 721 Lt BT.
- Paper Title should be of Font Size 24 with one Column section.
- Author Name in Font Size of 11 with one column as of Title.
- Abstract Font size of 9 Bold, "Abstract" word in Italic Bold.
- Main Text: Font size 10 with justified two columns section
- Two Column with Equal Column with of 3.38 and Gaping of .2
- First Character must be three lines Drop capped.
- Paragraph before Spacing of 1 pt and After of 0 pt.
- Line Spacing of 1 pt
- Large Images must be in One Column
- Numbering of First Main Headings (Heading 1) must be in Roman Letters, Capital Letter, and Font Size of 10.
- Numbering of Second Main Headings (Heading 2) must be in Alphabets, Italic, and Font Size of 10.

You can use your own standard format also.
Author Guidelines:

1. General,

2. Ethical Guidelines,

3. Submission of Manuscripts,

4. Manuscript's Category,

5. Structure and Format of Manuscript,

6. After Acceptance.

1. GENERAL

Before submitting your research paper, one is advised to go through the details as mentioned in following heads. It will be beneficial, while peer reviewer justify your paper for publication.

Scope

The Global Journals Inc. (US) welcome the submission of original paper, review paper, survey article relevant to the all the streams of Philosophy and knowledge. The Global Journals Inc. (US) is parental platform for Global Journal of Computer Science and Technology, Researches in Engineering, Medical Research, Science Frontier Research, Human Social Science, Management, and Business organization. The choice of specific field can be done otherwise as following in Abstracting and Indexing Page on this Website. As the all Global

Journals Inc. (US) are being abstracted and indexed (in process) by most of the reputed organizations. Topics of only narrow interest will not be accepted unless they have wider potential or consequences.

2. ETHICAL GUIDELINES

Authors should follow the ethical guidelines as mentioned below for publication of research paper and research activities.

Papers are accepted on strict understanding that the material in whole or in part has not been, nor is being, considered for publication elsewhere. If the paper once accepted by Global Journals Inc. (US) and Editorial Board, will become the copyright of the Global Journals Inc. (US).

Authorship: The authors and coauthors should have active contribution to conception design, analysis and interpretation of findings. They should critically review the contents and drafting of the paper. All should approve the final version of the paper before submission

The Global Journals Inc. (US) follows the definition of authorship set up by the Global Academy of Research and Development. According to the Global Academy of R&D authorship, criteria must be based on:

1) Substantial contributions to conception and acquisition of data, analysis and interpretation of the findings.

2) Drafting the paper and revising it critically regarding important academic content.

3) Final approval of the version of the paper to be published.

All authors should have been credited according to their appropriate contribution in research activity and preparing paper. Contributors who do not match the criteria as authors may be mentioned under Acknowledgement.

Acknowledgements: Contributors to the research other than authors credited should be mentioned under acknowledgement. The specifications of the source of funding for the research if appropriate can be included. Suppliers of resources may be mentioned along with address.

Appeal of Decision: The Editorial Board's decision on publication of the paper is final and cannot be appealed elsewhere.

Permissions: It is the author's responsibility to have prior permission if all or parts of earlier published illustrations are used in this paper.

Please mention proper reference and appropriate acknowledgements wherever expected.

If all or parts of previously published illustrations are used, permission must be taken from the copyright holder concerned. It is the author's responsibility to take these in writing.

Approval for reproduction/modification of any information (including figures and tables) published elsewhere must be obtained by the authors/copyright holders before submission of the manuscript. Contributors (Authors) are responsible for any copyright fee involved.

3. SUBMISSION OF MANUSCRIPTS

Manuscripts should be uploaded via this online submission page. The online submission is most efficient method for submission of papers, as it enables rapid distribution of manuscripts and consequently speeds up the review procedure. It also enables authors to know the status of their own manuscripts by emailing us. Complete instructions for submitting a paper is available below.

Manuscript submission is a systematic procedure and little preparation is required beyond having all parts of your manuscript in a given format and a computer with an Internet connection and a Web browser. Full help and instructions are provided on-screen. As an author, you will be prompted for login and manuscript details as Field of Paper and then to upload your manuscript file(s) according to the instructions.

To avoid postal delays, all transaction is preferred by e-mail. A finished manuscript submission is confirmed by e-mail immediately and your paper enters the editorial process with no postal delays. When a conclusion is made about the publication of your paper by our Editorial Board, revisions can be submitted online with the same procedure, with an occasion to view and respond to all comments.

Complete support for both authors and co-author is provided.

4. MANUSCRIPT'S CATEGORY

Based on potential and nature, the manuscript can be categorized under the following heads:

Original research paper: Such papers are reports of high-level significant original research work.

Review papers: These are concise, significant but helpful and decisive topics for young researchers.

Research articles: These are handled with small investigation and applications

Research letters: The letters are small and concise comments on previously published matters.

5.STRUCTURE AND FORMAT OF MANUSCRIPT

The recommended size of original research paper is less than seven thousand words, review papers fewer than seven thousands words also.Preparation of research paper or how to write research paper, are major hurdle, while writing manuscript. The research articles and research letters should be fewer than three thousand words, the structure original research paper; sometime review paper should be as follows:

Papers: These are reports of significant research (typically less than 7000 words equivalent, including tables, figures, references), and comprise:

(a)Title should be relevant and commensurate with the theme of the paper.

(b) A brief Summary, "Abstract" (less than 150 words) containing the major results and conclusions.

(c) Up to ten keywords, that precisely identifies the paper's subject, purpose, and focus.

(d) An Introduction, giving necessary background excluding subheadings; objectives must be clearly declared.

(e) Resources and techniques with sufficient complete experimental details (wherever possible by reference) to permit repetition; sources of information must be given and numerical methods must be specified by reference, unless non-standard.

(f) Results should be presented concisely, by well-designed tables and/or figures; the same data may not be used in both; suitable statistical data should be given. All data must be obtained with attention to numerical detail in the planning stage. As reproduced design has been recognized to be important to experiments for a considerable time, the Editor has decided that any paper that appears not to have adequate numerical treatments of the data will be returned un-refereed;

(g) Discussion should cover the implications and consequences, not just recapitulating the results; conclusions should be summarizing.

(h) Brief Acknowledgements.

(i) References in the proper form.

Authors should very cautiously consider the preparation of papers to ensure that they communicate efficiently. Papers are much more likely to be accepted, if they are cautiously designed and laid out, contain few or no errors, are summarizing, and be conventional to the approach and instructions. They will in addition, be published with much less delays than those that require much technical and editorial correction.

The Editorial Board reserves the right to make literary corrections and to make suggestions to improve briefness.

It is vital, that authors take care in submitting a manuscript that is written in simple language and adheres to published guidelines.

Format

Language: The language of publication is UK English. Authors, for whom English is a second language, must have their manuscript efficiently edited by an English-speaking person before submission to make sure that, the English is of high excellence. It is preferable, that manuscripts should be professionally edited.

Standard Usage, Abbreviations, and Units: Spelling and hyphenation should be conventional to The Concise Oxford English Dictionary. Statistics and measurements should at all times be given in figures, e.g. 16 min, except for when the number begins a sentence. When the number does not refer to a unit of measurement it should be spelt in full unless, it is 160 or greater.

Abbreviations supposed to be used carefully. The abbreviated name or expression is supposed to be cited in full at first usage, followed by the conventional abbreviation in parentheses.

Metric SI units are supposed to generally be used excluding where they conflict with current practice or are confusing. For illustration, 1.4 l rather than 1.4 × 10-3 m3, or 4 mm somewhat than 4 × 10-3 m. Chemical formula and solutions must identify the form used, e.g. anhydrous or hydrated, and the concentration must be in clearly defined units. Common species names should be followed by underlines at the first mention. For following use the generic name should be constricted to a single letter, if it is clear.

Structure

All manuscripts submitted to Global Journals Inc. (US), ought to include:

Title: The title page must carry an instructive title that reflects the content, a running title (less than 45 characters together with spaces), names of the authors and co-authors, and the place(s) wherever the work was carried out. The full postal address in addition with the e-mail address of related author must be given. Up to eleven keywords or very brief phrases have to be given to help data retrieval, mining and indexing.

Abstract, used in Original Papers and Reviews:

Optimizing Abstract for Search Engines

Many researchers searching for information online will use search engines such as Google, Yahoo or similar. By optimizing your paper for search engines, you will amplify the chance of someone finding it. This in turn will make it more likely to be viewed and/or cited in a further work. Global Journals Inc. (US) have compiled these guidelines to facilitate you to maximize the web-friendliness of the most public part of your paper.

Key Words

A major linchpin in research work for the writing research paper is the keyword search, which one will employ to find both library and Internet resources.

One must be persistent and creative in using keywords. An effective keyword search requires a strategy and planning a list of possible keywords and phrases to try.

Search engines for most searches, use Boolean searching, which is somewhat different from Internet searches. The Boolean search uses "operators," words (and, or, not, and near) that enable you to expand or narrow your affords. Tips for research paper while preparing research paper are very helpful guideline of research paper.

Choice of key words is first tool of tips to write research paper. Research paper writing is an art.A few tips for deciding as strategically as possible about keyword search:

- One should start brainstorming lists of possible keywords before even begin searching. Think about the most important concepts related to research work. Ask, "What words would a source have to include to be truly valuable in research paper?" Then consider synonyms for the important words.
- It may take the discovery of only one relevant paper to let steer in the right keyword direction because in most databases, the keywords under which a research paper is abstracted are listed with the paper.
- One should avoid outdated words.

Keywords are the key that opens a door to research work sources. Keyword searching is an art in which researcher's skills are bound to improve with experience and time.

Numerical Methods: Numerical methods used should be clear and, where appropriate, supported by references.

Acknowledgements: Please make these as concise as possible.

References

References follow the Harvard scheme of referencing. References in the text should cite the authors' names followed by the time of their publication, unless there are three or more authors when simply the first author's name is quoted followed by et al. unpublished work has to only be cited where necessary, and only in the text. Copies of references in press in other journals have to be supplied with submitted typescripts. It is necessary that all citations and references be carefully checked before submission, as mistakes or omissions will cause delays.

References to information on the World Wide Web can be given, but only if the information is available without charge to readers on an official site. Wikipedia and Similar websites are not allowed where anyone can change the information. Authors will be asked to make available electronic copies of the cited information for inclusion on the Global Journals Inc. (US) homepage at the judgment of the Editorial Board.

The Editorial Board and Global Journals Inc. (US) recommend that, citation of online-published papers and other material should be done via a DOI (digital object identifier). If an author cites anything, which does not have a DOI, they run the risk of the cited material not being noticeable.

The Editorial Board and Global Journals Inc. (US) recommend the use of a tool such as Reference Manager for reference management and formatting.

Tables, Figures and Figure Legends

Tables: Tables should be few in number, cautiously designed, uncrowned, and include only essential data. Each must have an Arabic number, e.g. Table 4, a self-explanatory caption and be on a separate sheet. Vertical lines should not be used.

Figures: Figures are supposed to be submitted as separate files. Always take in a citation in the text for each figure using Arabic numbers, e.g. Fig. 4. Artwork must be submitted online in electronic form by e-mailing them.

Preparation of Electronic Figures for Publication

Even though low quality images are sufficient for review purposes, print publication requires high quality images to prevent the final product being blurred or fuzzy. Submit (or e-mail) EPS (line art) or TIFF (halftone/photographs) files only. MS PowerPoint and Word Graphics are unsuitable for printed pictures. Do not use pixel-oriented software. Scans (TIFF only) should have a resolution of at least 350 dpi (halftone) or 700 to 1100 dpi (line drawings) in relation to the imitation size. Please give the data for figures in black and white or submit a Color Work Agreement Form. EPS files must be saved with fonts embedded (and with a TIFF preview, if possible).

For scanned images, the scanning resolution (at final image size) ought to be as follows to ensure good reproduction: line art: >650 dpi; halftones (including gel photographs) : >350 dpi; figures containing both halftone and line images: >650 dpi.

Color Charges: It is the rule of the Global Journals Inc. (US) for authors to pay the full cost for the reproduction of their color artwork. Hence, please note that, if there is color artwork in your manuscript when it is accepted for publication, we would require you to complete and return a color work agreement form before your paper can be published.

Figure Legends: Self-explanatory legends of all figures should be incorporated separately under the heading 'Legends to Figures'. In the full-text online edition of the journal, figure legends may possibly be truncated in abbreviated links to the full screen version. Therefore, the first 100 characters of any legend should notify the reader, about the key aspects of the figure.

6. AFTER ACCEPTANCE

Upon approval of a paper for publication, the manuscript will be forwarded to the dean, who is responsible for the publication of the Global Journals Inc. (US).

6.1 Proof Corrections

The corresponding author will receive an e-mail alert containing a link to a website or will be attached. A working e-mail address must therefore be provided for the related author.

Acrobat Reader will be required in order to read this file. This software can be downloaded

(Free of charge) from the following website:

www.adobe.com/products/acrobat/readstep2.html. This will facilitate the file to be opened, read on screen, and printed out in order for any corrections to be added. Further instructions will be sent with the proof.

Proofs must be returned to the dean at dean@globaljournals.org within three days of receipt.

As changes to proofs are costly, we inquire that you only correct typesetting errors. All illustrations are retained by the publisher. Please note that the authors are responsible for all statements made in their work, including changes made by the copy editor.

6.2 Early View of Global Journals Inc. (US) (Publication Prior to Print)

The Global Journals Inc. (US) are enclosed by our publishing's Early View service. Early View articles are complete full-text articles sent in advance of their publication. Early View articles are absolute and final. They have been completely reviewed, revised and edited for publication, and the authors' final corrections have been incorporated. Because they are in final form, no changes can be made after sending them. The nature of Early View articles means that they do not yet have volume, issue or page numbers, so Early View articles cannot be cited in the conventional way.

6.3 Author Services

Online production tracking is available for your article through Author Services. Author Services enables authors to track their article - once it has been accepted - through the production process to publication online and in print. Authors can check the status of their articles online and choose to receive automated e-mails at key stages of production. The authors will receive an e-mail with a unique link that enables them to register and have their article automatically added to the system. Please ensure that a complete e-mail address is provided when submitting the manuscript.

6.4 Author Material Archive Policy

Please note that if not specifically requested, publisher will dispose off hardcopy & electronic information submitted, after the two months of publication. If you require the return of any information submitted, please inform the Editorial Board or dean as soon as possible.

6.5 Offprint and Extra Copies

A PDF offprint of the online-published article will be provided free of charge to the related author, and may be distributed according to the Publisher's terms and conditions. Additional paper offprint may be ordered by emailing us at: editor@globaljournals.org .

the search? Will I be able to find all information in this field area? If the answer of these types of questions will be "Yes" then you can choose that topic. In most of the cases, you may have to conduct the surveys and have to visit several places because this field is related to Computer Science and Information Technology. Also, you may have to do a lot of work to find all rise and falls regarding the various data of that subject. Sometimes, detailed information plays a vital role, instead of short information.

2. Evaluators are human: First thing to remember that evaluators are also human being. They are not only meant for rejecting a paper. They are here to evaluate your paper. So, present your Best.

3. Think Like Evaluators: If you are in a confusion or getting demotivated that your paper will be accepted by evaluators or not, then think and try to evaluate your paper like an Evaluator. Try to understand that what an evaluator wants in your research paper and automatically you will have your answer.

4. Make blueprints of paper: The outline is the plan or framework that will help you to arrange your thoughts. It will make your paper logical. But remember that all points of your outline must be related to the topic you have chosen.

5. Ask your Guides: If you are having any difficulty in your research, then do not hesitate to share your difficulty to your guide (if you have any). They will surely help you out and resolve your doubts. If you can't clarify what exactly you require for your work then ask the supervisor to help you with the alternative. He might also provide you the list of essential readings.

6. Use of computer is recommended: As you are doing research in the field of Computer Science, then this point is quite obvious.

7. Use right software: Always use good quality software packages. If you are not capable to judge good software then you can lose quality of your paper unknowingly. There are various software programs available to help you, which you can get through Internet.

8. Use the Internet for help: An excellent start for your paper can be by using the Google. It is an excellent search engine, where you can have your doubts resolved. You may also read some answers for the frequent question how to write my research paper or find model research paper. From the internet library you can download books. If you have all required books make important reading selecting and analyzing the specified information. Then put together research paper sketch out.

9. Use and get big pictures: Always use encyclopedias, Wikipedia to get pictures so that you can go into the depth.

10. Bookmarks are useful: When you read any book or magazine, you generally use bookmarks, right! It is a good habit, which helps to not to lose your continuity. You should always use bookmarks while searching on Internet also, which will make your search easier.

11. Revise what you wrote: When you write anything, always read it, summarize it and then finalize it.

12. Make all efforts: Make all efforts to mention what you are going to write in your paper. That means always have a good start. Try to mention everything in introduction, that what is the need of a particular research paper. Polish your work by good skill of writing and always give an evaluator, what he wants.

13. Have backups: When you are going to do any important thing like making research paper, you should always have backup copies of it either in your computer or in paper. This will help you to not to lose any of your important.

14. Produce good diagrams of your own: Always try to include good charts or diagrams in your paper to improve quality. Using several and unnecessary diagrams will degrade the quality of your paper by creating "hotchpotch." So always, try to make and include those diagrams, which are made by your own to improve readability and understandability of your paper.

15. Use of direct quotes: When you do research relevant to literature, history or current affairs then use of quotes become essential but if study is relevant to science then use of quotes is not preferable.

16. Use proper verb tense: Use proper verb tenses in your paper. Use past tense, to present those events that happened. Use present tense to indicate events that are going on. Use future tense to indicate future happening events. Use of improper and wrong tenses will confuse the evaluator. Avoid the sentences that are incomplete.

17. Never use online paper: If you are getting any paper on Internet, then never use it as your research paper because it might be possible that evaluator has already seen it or maybe it is outdated version.

18. **Pick a good study spot:** To do your research studies always try to pick a spot, which is quiet. Every spot is not for studies. Spot that suits you choose it and proceed further.

19. Know what you know: Always try to know, what you know by making objectives. Else, you will be confused and cannot achieve your target.

20. Use good quality grammar: Always use a good quality grammar and use words that will throw positive impact on evaluator. Use of good quality grammar does not mean to use tough words, that for each word the evaluator has to go through dictionary. Do not start sentence with a conjunction. Do not fragment sentences. Eliminate one-word sentences. Ignore passive voice. Do not ever use a big word when a diminutive one would suffice. Verbs have to be in agreement with their subjects. Prepositions are not expressions to finish sentences with. It is incorrect to ever divide an infinitive. Avoid clichés like the disease. Also, always shun irritating alliteration. Use language that is simple and straight forward. put together a neat summary.

21. Arrangement of information: Each section of the main body should start with an opening sentence and there should be a changeover at the end of the section. Give only valid and powerful arguments to your topic. You may also maintain your arguments with records.

22. Never start in last minute: Always start at right time and give enough time to research work. Leaving everything to the last minute will degrade your paper and spoil your work.

23. Multitasking in research is not good: Doing several things at the same time proves bad habit in case of research activity. Research is an area, where everything has a particular time slot. Divide your research work in parts and do particular part in particular time slot.

24. Never copy others' work: Never copy others' work and give it your name because if evaluator has seen it anywhere you will be in trouble.

25. Take proper rest and food: No matter how many hours you spend for your research activity, if you are not taking care of your health then all your efforts will be in vain. For a quality research, study is must, and this can be done by taking proper rest and food.

26. Go for seminars: Attend seminars if the topic is relevant to your research area. Utilize all your resources.

27. Refresh your mind after intervals: Try to give rest to your mind by listening to soft music or by sleeping in intervals. This will also improve your memory.

28. Make colleagues: Always try to make colleagues. No matter how sharper or intelligent you are, if you make colleagues you can have several ideas, which will be helpful for your research.

29. **Think technically:** Always think technically. If anything happens, then search its reasons, its benefits, and demerits.

30. Think and then print: When you will go to print your paper, notice that tables are not be split, headings are not detached from their descriptions, and page sequence is maintained.

31. Adding unnecessary information: Do not add unnecessary information, like, I have used MS Excel to draw graph. Do not add irrelevant and inappropriate material. These all will create superfluous. Foreign terminology and phrases are not apropos. One should NEVER take a broad view. Analogy in script is like feathers on a snake. Not at all use a large word when a very small one would be

sufficient. Use words properly, regardless of how others use them. Remove quotations. Puns are for kids, not grunt readers. Amplification is a billion times of inferior quality than sarcasm.

32. Never oversimplify everything: To add material in your research paper, never go for oversimplification. This will definitely irritate the evaluator. Be more or less specific. Also too, by no means, ever use rhythmic redundancies. Contractions aren't essential and shouldn't be there used. Comparisons are as terrible as clichés. Give up ampersands and abbreviations, and so on. Remove commas, that are, not necessary. Parenthetical words however should be together with this in commas. Understatement is all the time the complete best way to put onward earth-shaking thoughts. Give a detailed literary review.

33. Report concluded results: Use concluded results. From raw data, filter the results and then conclude your studies based on measurements and observations taken. Significant figures and appropriate number of decimal places should be used. Parenthetical remarks are prohibitive. Proofread carefully at final stage. In the end give outline to your arguments. Spot out perspectives of further study of this subject. Justify your conclusion by at the bottom of them with sufficient justifications and examples.

34. After conclusion: Once you have concluded your research, the next most important step is to present your findings. Presentation is extremely important as it is the definite medium though which your research is going to be in print to the rest of the crowd. Care should be taken to categorize your thoughts well and present them in a logical and neat manner. A good quality research paper format is essential because it serves to highlight your research paper and bring to light all necessary aspects in your research.

Informal Guidelines of Research Paper Writing

Key points to remember:

- Submit all work in its final form.
- Write your paper in the form, which is presented in the guidelines using the template.
- Please note the criterion for grading the final paper by peer-reviewers.

Final Points:

A purpose of organizing a research paper is to let people to interpret your effort selectively. The journal requires the following sections, submitted in the order listed, each section to start on a new page.

The introduction will be compiled from reference matter and will reflect the design processes or outline of basis that direct you to make study. As you will carry out the process of study, the method and process section will be constructed as like that. The result segment will show related statistics in nearly sequential order and will direct the reviewers next to the similar intellectual paths throughout the data that you took to carry out your study. The discussion section will provide understanding of the data and projections as to the implication of the results. The use of good quality references all through the paper will give the effort trustworthiness by representing an alertness of prior workings.

Writing a research paper is not an easy job no matter how trouble-free the actual research or concept. Practice, excellent preparation, and controlled record keeping are the only means to make straightforward the progression.

General style:

Specific editorial column necessities for compliance of a manuscript will always take over from directions in these general guidelines.

To make a paper clear

· Adhere to recommended page limits

Mistakes to evade

- Insertion a title at the foot of a page with the subsequent text on the next page

- Separating a table/chart or figure - impound each figure/table to a single page
- Submitting a manuscript with pages out of sequence

In every sections of your document

· Use standard writing style including articles ("a", "the," etc.)

· Keep on paying attention on the research topic of the paper

· Use paragraphs to split each significant point (excluding for the abstract)

· Align the primary line of each section

· Present your points in sound order

· Use present tense to report well accepted

· Use past tense to describe specific results

· Shun familiar wording, don't address the reviewer directly, and don't use slang, slang language, or superlatives

· Shun use of extra pictures - include only those figures essential to presenting results

Title Page:

Choose a revealing title. It should be short. It should not have non-standard acronyms or abbreviations. It should not exceed two printed lines. It should include the name(s) and address (es) of all authors.

Abstract:

The summary should be two hundred words or less. It should briefly and clearly explain the key findings reported in the manuscript--must have precise statistics. It should not have abnormal acronyms or abbreviations. It should be logical in itself. Shun citing references at this point.

An abstract is a brief distinct paragraph summary of finished work or work in development. In a minute or less a reviewer can be taught the foundation behind the study, common approach to the problem, relevant results, and significant conclusions or new questions.

Write your summary when your paper is completed because how can you write the summary of anything which is not yet written? Wealth of terminology is very essential in abstract. Yet, use comprehensive sentences and do not let go readability for briefness. You can maintain it succinct by phrasing sentences so that they provide more than lone rationale. The author can at this moment go straight to

shortening the outcome. Sum up the study, with the subsequent elements in any summary. Try to maintain the initial two items to no more than one ruling each.

- Reason of the study - theory, overall issue, purpose
- Fundamental goal
- To the point depiction of the research
- Consequences, including definite statistics - if the consequences are quantitative in nature, account quantitative data; results of any numerical analysis should be reported
- Significant conclusions or questions that track from the research(es)

Approach:

- Single section, and succinct
- As a outline of job done, it is always written in past tense
- A conceptual should situate on its own, and not submit to any other part of the paper such as a form or table
- Center on shortening results - bound background information to a verdict or two, if completely necessary
- What you account in an conceptual must be regular with what you reported in the manuscript
- Exact spelling, clearness of sentences and phrases, and appropriate reporting of quantities (proper units, important statistics) are just as significant in an abstract as they are anywhere else

Introduction:

The **Introduction** should "introduce" the manuscript. The reviewer should be presented with sufficient background information to be capable to comprehend and calculate the purpose of your study without having to submit to other works. The basis for the study should be offered. Give most important references but shun difficult to make a comprehensive appraisal of the topic. In the introduction, describe the problem visibly. If the problem is not acknowledged in a logical, reasonable way, the reviewer will have no attention in your result. Speak in common terms about techniques used to explain the problem, if needed, but do not present any particulars about the protocols here. Following approach can create a valuable beginning:

- Explain the value (significance) of the study
- Shield the model - why did you employ this particular system or method? What is its compensation? You strength remark on its appropriateness from a abstract point of vision as well as point out sensible reasons for using it.
- Present a justification. Status your particular theory (es) or aim(s), and describe the logic that led you to choose them.
- Very for a short time explain the tentative propose and how it skilled the declared objectives.

Approach:

- Use past tense except for when referring to recognized facts. After all, the manuscript will be submitted after the entire job is done.
- Sort out your thoughts; manufacture one key point with every section. If you make the four points listed above, you will need a least of four paragraphs.
- Present surroundings information only as desirable in order hold up a situation. The reviewer does not desire to read the whole thing you know about a topic.
- Shape the theory/purpose specifically - do not take a broad view.
- As always, give awareness to spelling, simplicity and correctness of sentences and phrases.

Procedures (Methods and Materials):

This part is supposed to be the easiest to carve if you have good skills. A sound written Procedures segment allows a capable scientist to replacement your results. Present precise information about your supplies. The suppliers and clarity of reagents can be helpful bits of information. Present methods in sequential order but linked methodologies can be grouped as a segment. Be concise when relating the protocols. Attempt for the least amount of information that would permit another capable scientist to spare your outcome but be cautious that vital information is integrated. The use of subheadings is suggested and ought to be synchronized with the results section. When a technique is used that has been well described in another object, mention the specific item describing a way but draw the basic

principle while stating the situation. The purpose is to text all particular resources and broad procedures, so that another person may use some or all of the methods in one more study or referee the scientific value of your work. It is not to be a step by step report of the whole thing you did, nor is a methods section a set of orders.

Materials:

- Explain materials individually only if the study is so complex that it saves liberty this way.
- Embrace particular materials, and any tools or provisions that are not frequently found in laboratories.
- Do not take in frequently found.
- If use of a definite type of tools.
- Materials may be reported in a part section or else they may be recognized along with your measures.

Methods:

- Report the method (not particulars of each process that engaged the same methodology)
- Describe the method entirely
- To be succinct, present methods under headings dedicated to specific dealings or groups of measures
- Simplify - details how procedures were completed not how they were exclusively performed on a particular day.
- If well known procedures were used, account the procedure by name, possibly with reference, and that's all.

Approach:

- It is embarrassed or not possible to use vigorous voice when documenting methods with no using first person, which would focus the reviewer's interest on the researcher rather than the job. As a result when script up the methods most authors use third person passive voice.
- Use standard style in this and in every other part of the paper - avoid familiar lists, and use full sentences.

What to keep away from

- Resources and methods are not a set of information.
- Skip all descriptive information and surroundings - save it for the argument.
- Leave out information that is immaterial to a third party.

Results:

The principle of a results segment is to present and demonstrate your conclusion. Create this part a entirely objective details of the outcome, and save all understanding for the discussion.

The page length of this segment is set by the sum and types of data to be reported. Carry on to be to the point, by means of statistics and tables, if suitable, to present consequences most efficiently.You must obviously differentiate material that would usually be incorporated in a study editorial from any unprocessed data or additional appendix matter that would not be available. In fact, such matter should not be submitted at all except requested by the instructor.

Content

- Sum up your conclusion in text and demonstrate them, if suitable, with figures and tables.
- In manuscript, explain each of your consequences, point the reader to remarks that are most appropriate.
- Present a background, such as by describing the question that was addressed by creation an exacting study.
- Explain results of control experiments and comprise remarks that are not accessible in a prescribed figure or table, if appropriate.
- Examine your data, then prepare the analyzed (transformed) data in the form of a figure (graph), table, or in manuscript form.

What to stay away from

- Do not discuss or infer your outcome, report surroundings information, or try to explain anything.
- Not at all, take in raw data or intermediate calculations in a research manuscript.

- Do not present the similar data more than once.
- Manuscript should complement any figures or tables, not duplicate the identical information.
- Never confuse figures with tables - there is a difference.

Approach

- As forever, use past tense when you submit to your results, and put the whole thing in a reasonable order.
- Put figures and tables, appropriately numbered, in order at the end of the report
- If you desire, you may place your figures and tables properly within the text of your results part.

Figures and tables

- If you put figures and tables at the end of the details, make certain that they are visibly distinguished from any attach appendix materials, such as raw facts
- Despite of position, each figure must be numbered one after the other and complete with subtitle
- In spite of position, each table must be titled, numbered one after the other and complete with heading
- All figure and table must be adequately complete that it could situate on its own, divide from text

Discussion:

The Discussion is expected the trickiest segment to write and describe. A lot of papers submitted for journal are discarded based on problems with the Discussion. There is no head of state for how long a argument should be. Position your understanding of the outcome visibly to lead the reviewer through your conclusions, and then finish the paper with a summing up of the implication of the study. The purpose here is to offer an understanding of your results and hold up for all of your conclusions, using facts from your research and generally accepted information, if suitable. The implication of result should be visibly described. Infer your data in the conversation in suitable depth. This means that when you clarify an observable fact you must explain mechanisms that may account for the observation. If your results vary from your prospect, make clear why that may have happened. If your results agree, then explain the theory that the proof supported. It is never suitable to just state that the data approved with prospect, and let it drop at that.

- Make a decision if each premise is supported, discarded, or if you cannot make a conclusion with assurance. Do not just dismiss a study or part of a study as "uncertain."
- Research papers are not acknowledged if the work is imperfect. Draw what conclusions you can based upon the results that you have, and take care of the study as a finished work
- You may propose future guidelines, such as how the experiment might be personalized to accomplish a new idea.
- Give details all of your remarks as much as possible, focus on mechanisms.
- Make a decision if the tentative design sufficiently addressed the theory, and whether or not it was correctly restricted.
- Try to present substitute explanations if sensible alternatives be present.
- One research will not counter an overall question, so maintain the large picture in mind, where do you go next? The best studies unlock new avenues of study. What questions remain?
- Recommendations for detailed papers will offer supplementary suggestions.

Approach:

- When you refer to information, differentiate data generated by your own studies from available information
- Submit to work done by specific persons (including you) in past tense.
- Submit to generally acknowledged facts and main beliefs in present tense.

Administration Rules Listed Before Submitting Your Research Paper to Global Journals Inc. (US)

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

Segment Draft and Final Research Paper: You have to strictly follow the template of research paper. If it is not done your paper may get rejected.

- The **major constraint** is that you must independently make all content, tables, graphs, and facts that are offered in the paper. You must write each part of the paper wholly on your own. The Peer-reviewers need to identify your own perceptive of the concepts in your own terms. NEVER extract straight from any foundation, and never rephrase someone else's analysis.

- Do not give permission to anyone else to "PROOFREAD" your manuscript.

- Methods to avoid Plagiarism is applied by us on every paper, if found guilty, you will be blacklisted by all of our collaborated research groups, your institution will be informed for this and strict legal actions will be taken immediately.)
- To guard yourself and others from possible illegal use please do not permit anyone right to use to your paper and files.

Criterion for Grading a Research Paper (Compilation) by Global Journals Inc. (US)

Please note that following table is only a Grading of "Paper Compilation" and not on "Performed/Stated Research" whose grading solely depends on Individual Assigned Peer Reviewer and Editorial Board Member. These can be available only on request and after decision of Paper. This report will be the property of Global Journals Inc. (US).

Topics	Grades		
	A-B	**C-D**	**E-F**
Abstract	Clear and concise with appropriate content, Correct format. 200 words or below	Unclear summary and no specific data, Incorrect form Above 200 words	No specific data with ambiguous information Above 250 words
Introduction	Containing all background details with clear goal and appropriate details, flow specification, no grammar and spelling mistake, well organized sentence and paragraph, reference cited	Unclear and confusing data, appropriate format, grammar and spelling errors with unorganized matter	Out of place depth and content, hazy format
Methods and Procedures	Clear and to the point with well arranged paragraph, precision and accuracy of facts and figures, well organized subheads	Difficult to comprehend with embarrassed text, too much explanation but completed	Incorrect and unorganized structure with hazy meaning
Result	Well organized, Clear and specific, Correct units with precision, correct data, well structuring of paragraph, no grammar and spelling mistake	Complete and embarrassed text, difficult to comprehend	Irregular format with wrong facts and figures
Discussion	Well organized, meaningful specification, sound conclusion, logical and concise explanation, highly structured paragraph reference cited	Wordy, unclear conclusion, spurious	Conclusion is not cited, unorganized, difficult to comprehend
References	Complete and correct format, well organized	Beside the point, Incomplete	Wrong format and structuring

Index

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