Online ISSN : 0975-4172
Print ISSN : 0975-4350
DOI : 10.17406/GJCST

Global Journal

of Computer Science and Technology: E

Network, Web & Security

Highlights

Mobile Ad Hoc Networks

Quality of IT Enabled Services

Towards Configured Intrusion

Contemporary Standards Features

Discovering Thoughts, Inventing Future

Volume 16 Issue 4 Version 0.1

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

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

Volume 16 Issue 4 (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® Headquarters
945th Concord Streets,
Framingham Massachusetts Pin: 01701,
United States of America
USA Toll Free: +001-888-839-7392
USA Toll Free Fax: +001-888-839-7392

Offset Typesetting

Global Journals Incorporated
2nd, Lansdowne, Lansdowne Rd., Croydon-Surrey,
Pin: CR9 2ER, United Kingdom

Packaging & Continental Dispatching

Global Journals
E-3130 Sudama Nagar, Near Gopur Square,
Indore, M.P., Pin: 452009, 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: *investors@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)

Integrated Editorial Board
(Computer Science, Engineering, Medical, Management, Natural Science, Social Science)

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 Issue

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 16 Issue 4 Version 1.0 Year 2016
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Towards Configured Intrusion Detection Systems

By Gagan Deep Sharma & Vivek Kumar
GGSIP University

Abstract- This paper studies the challenges in the current intrusion detection system and comparatively analyzes the active and passive response systems. The paper studies the existing IDS and their usefulness in detecting and preventing attacks in any type of network and control traffic with the performance of the system to be improved. The study also evaluates the emerging avenues in Intrusion Detection System and explores the possible future avenues in intrusion detection scheme. It is observed that the detection-based systems have started to gain popularity in the IT security domain. The paper highlights the need to implement an appropriately configured IDS since an optimally configured IDS deters hackers, thus, reducing the need for investigation by security experts for security violations.

Keywords: *Intrusion detection system, response systems, detection-based systems, configured IDS, security violations.*

GJCST-E Classification : *C.2.1 C.2.2*

Strictly as per the compliance and regulations of:

Towards Configured Intrusion Detection Systems

Gagan Deep Sharma [α] & Vivek Kumar [σ]

Abstract- This paper studies the challenges in the current intrusion detection system and comparatively analyzes the active and passive response systems. The paper studies the existing IDS and their usefulness in detecting and preventing attacks in any type of network and control traffic with the performance of the system to be improved. The study also evaluates the emerging avenues in Intrusion Detection System and explores the possible future avenues in intrusion detection scheme. It is observed that the detection-based systems have started to gain popularity in the IT security domain. The paper highlights the need to implement an appropriately configured IDS since an optimally configured IDS deters hackers, thus, reducing the need for investigation by security experts for security violations.

Keywords: Intrusion detection system, response systems, detection-based systems, configured IDS, security violations.

I. Introduction

Data systems and computer networks are central in modern social club. The more data stored and processed, the more significant it is to secure computer systems. Widespread use and proliferation of computer network has increased the attacks on new age information systems. These attacks are attempts to take illegal/unauthorized access to information available with an intention of misusing the same. These attacks result in major financial loss to organizations in the form of mistrust of customers, loosing goodwill. Any set of processes that attempt to compromise the integrity, confidentiality, or availability of a computer resource, is known as intrusion *(Zamboni, 2001)*. Generally an intruder is defined as a system, program or person who tries to and may become successful to stop into an information system or perform an action legally not allowed *(Graham, 2000)*.

The act of detecting actions that try to compromise the integrity, confidentiality, or availability of a computer resource can be referred as intrusion detection *(Zamboni, 2001)*. Intrusion Detection (ID) refers to all processes used in discovering unauthorized uses of network or computer devices through specifically designed software with a sole purpose of detecting unusual or abnormal activity. *Denning (1987)* proposes intrusion detection as an approach to counter, the information processing system and networking attacks and misuses *(Denning, 1987 and Botha & Solms, 2004)*.

Intrusion detection is carried out by an intrusion detection scheme. There are many commercial intrusion detection systems available and most of these commercial implementations are relatively ineffective and insufficient, which gives rise to the need for research on more dynamic intrusion detection schemes. An intrusion detection system is a device or software application that monitors network and/or system actions for malicious actions or policy violations and produces reports *(Scarfone and Mell, 2007)*. IDS is also understood as an instrument that complements a spacious scope of users used to experience some tier of protection *(Vigna et al, 2002)*.

For an IDS to be efficient, it must run continuously adapt to behavioral alterations and large sums of data, be configurable, do not apply too much memory resources of the machine and after system failures, be reusable without new learning *(Zamboni, 1998)*.

Traditional methods for intrusion detection are based on extensive knowledge of attack signatures that are provided by human experts. The signature database has to be manually revised for each new type of intrusion that is discovered. A significant limitation of signature-based methods is that they cannot detect novel attacks. In addition, once a new attack is discovered and its signature developed, often there is a substantial latency in its deployment. These limitations have led to an increasing interest in intrusion detection techniques based upon data mining, which generally fall into one of two categories: misuse detection and anomaly detection.

To prevent attacks or reduce their severity, many solutions exist, but no one can be considered satisfactory and all over. The intrusion detection schemes are one of the most efficient solution. Their purpose is to recognize intrusions or intrusion attempts by users or abnormal behavior by the identification of an onslaught from the stream network data. Different methods and approaches are available in the design of intrusion detection systems.

There are a variety of tools providing a certain level of comfort with acceptable risks used in the defence and surveillance of computer networks. Defence-in-Depth is a term encompassing

Author α: University School of Management Studies, GGSIP University, New Delhi. e-mail: angrishgagan@gmail.com
Author σ: Bureau Veritas Consumer Products Services India, Noida, Uttar Pradesh, India. e-mail: bhardwaj.vivekkumar@gmail.com

comprehensive analyst training, hardware deployed in strategic positions and a strong security policy necessary for achieving this objective. There are tools available to reach this goal. The aggregation of data comes from routers, the host itself, firewalls, virus scanners and IDS, the tool strictly designed to catch known attacks (SANS Institute, 2001).

Since the introduction of IDS, Cyber-attacks have been a real threat. With their wide variety and specialty, they can have catastrophic consequences. To prevent attacks or reduce their severity, many solutions exist, but no one can be considered satisfactory and complete. The intrusion detection systems are among the most effective solution. Their role is to recognize intrusions or intrusion attempts by users or abnormal behavior by the recognition of an attack from the stream network data.

Anderson (1972) delineates the fact the United States Air Force [USAF] "became increasingly aware of computer security problems. This problem feels virtually in every aspect of USAF operations and governance".

USAF faces the daunting tasks of providing shared use of their computer systems, which contained various levels of classifications in a need to know environment with a user base holding various levels of security clearance. Thirty years ago, this created a grave problem that is still with us today. The problem remains: "How to safely secure separate classification domains on the same network without compromising security?" *(Anderson, 1972)*.

Denning (1984) and Neumann (1986) undertake the R&D project with the first model of a real-time IDS. This prototype was named the Intrusion Detection Expert System (IDES). This IDES was initially a rule-based expert system trained to detect known malicious activity.

Some of the most common terms in context of IDS are as follows:

(a) Host-Based
(b) Network-Based
(c) Anomaly Detection Model
(d) Misuse Detection Model

These models are used as terms in Intrusion Detection user and research community. People from different areas have researched and developed few systems to deal with these kind of issues *(SANS Institute, 2001)*

a) Why should Intrusion Detection Systems be used?

Intrusion detection allows organizations to protect their systems from the threats that come with increasing network connectivity and reliance on information systems. Passed on the grade and nature of modern network security threats, the question to security professionals should not be whether to use intrusion detection, but which intrusion detection features and capabilities to employ.

IDSs have gained acceptance as a necessary addition to every organization's security infrastructure. Despite the documented contributions intrusion detection technologies make to system security, in many organizations one must still justify the acquisition of IDSs *(Bace and Mell, 2001)* There are several compelling reasons to acquire and use IDSs:

(a) To prevent problem behaviors by increasing the perceived danger of discovery and punishment for those who would assault or otherwise misuse the scheme.
(b) To detect attacks and other security violations that are not prevented by other protection criteria.
(c) To identify and handle with the preambles to attacks (commonly viewed as network probes and other "doorknob rattling" activities).
(d) To document the existing threat to an establishment.
(e) To act as quality control for security design and administration, especially of large and complex enterprises.
(f) To provide useful information about intrusions that do take place, allowing improved diagnosis, recovery, and correction of causative factors.

b) Major types of IDSs

IDSs have various types, characterized by different monitoring and analysis approaches. Each approach has inherent advantages and disadvantages. Furthermore, all approaches can be described in terms of a generic process model for IDSs. *(Bace & Mell, 2001)*

Many IDSs *(Bace & Mell, 2001)* can be described in terms of three fundamental functional components:

- Information Sources – the different sources of event information used to determine whether an intrusion has taken place. These roots can be traced from different stages of the system, with network, host, and application monitoring. On this basis, the following types of IDS have been observed –

o *Network-based IDSs:* The majority of commercial intrusion detection systems is network based. These IDSs detect attacks by capturing and analyzing network packets. Listening on a network segment or switch, one network-based IDS can monitor the network traffic affecting multiple hosts that are connected to the network segment, thereby protecting those hosts. Network-based IDSs often consist of a set of single-purpose sensors or hosts placed at various points in a network. These units monitor network traffic, performing local analysis of that traffic and reporting attacks to a central management console. As the sensors are limited to running the IDS, they can be more easily secured against attack. Many of these detectors are designed to function in "stealth" mode, in

parliamentary procedure to attain it more unmanageable for an assailant to influence their presence and placement.

- *Host-based IDSs:* Host-based IDSs operate on information collected from within an individual computer system (Application-based IDSs are actually a subset of host-based IDSs). This vantage point allows host based IDSs to analyze activities with great reliability and precision, determining exactly which processes and users are involved in a particular attack on the operating system. Furthermore, unlike network based IDSs, host-based IDSs can "see" the outcome of an attempted attack, as they can directly access and monitor the data files and system processes usually targeted by attacks. Host-based IDSs normally utilize information sources of two types, operating system audit trails, and system logs. Operating system audit trails are usually generated at the innermost (kernel) level of the operating system, and are therefore more detailed and better protected than system logs. However, system logs are much less obtuse and a lot smaller than audit trails, and are furthermore far easier to grasp. Some server-based IDSs are designed to sustain a centralized IDS management and accounting infrastructure that can tolerate a single management console to pass over many hosts. Others generate messages in formats that are compatible with network management systems.
- *Application-based IDSs:* Application-based IDSs are a special subset of host-based IDSs that analyze the events transpiring within a software application. The most common information sources used by application-based IDSs are the application's transaction log files. The ability to interface with the application directly, with significant domain- or application-specific knowledge included in the analysis engine, allows application-based IDSs to detect suspicious behavior due to authorized users exceeding their mandate. This is because such problems are more likely to appear in the interaction between the user, the data, and the application.

- Analysis – the part of intrusion detection systems that actually organizes and makes sense of the events derived from the information sources, deciding when those events indicate that intrusions are occurring or have already taken place. The most common analysis approaches are misuse detection and anomaly detection. The following forms of IDS are observed on this basis –

- *Misuse Detection:* Misuse detectors analyze system activity, looking for events or sets of events that match a predefined pattern of events that describe a known attack. As the patterns corresponding to known attacks are called signatures, misuse detection is sometimes called "signature-based detection." The most common form of misuse detection used in commercial products specifies each pattern of events corresponding to an attack as a separate signature. Nevertheless, in that respect are more sophisticated approaches to doing misuse detection (called "state-based" analysis techniques) that can leverage a single signature to find groups of approaches.
- *Anomaly Detection:* Anomaly detectors identify abnormal, unusual behavior (anomalies) on a host or network. They operate on the assumption that attacks are different from "normal" (legitimate) activity and can therefore be detected by systems that distinguish these conflicts. Anomaly detectors construct profiles representing normal behavior of users, hosts, or network connections. These profiles are built from historical information accumulated over a period of normal functioning. The detectors then collect event data and use a variety of measures to determine when monitored activity deviates from the norm.

- Response – the set of actions that the system takes once it detects intrusions. These are typically grouped into active and passive measures, with active measures involving some automated intervention on the part of the system, and passive measures involving reporting IDS findings to humans, who are then expected to take action based on those reports. The forms of IDS under this section are as under –

- *Active IDS:* Active IDS responses are automated actions taken when certain types of intrusions are detected. In that respect are three categories of active responses.

  - *Collect additional information over time:* In the IDS case, this might involve increasing the level of sensitivity of information sources (for instance, turning up the number of events logged by an operating system audit trail, or increasing the sensitivity of a network monitor to capture all packets, not just those targeting a particular port or target system.) Collecting additional information is helpful for several reasons. The additional information collected can help resolve the detection of the attack. (Assisting the system in diagnosing whether an attack did or did not take place.) This option also allows the organization to gather information that can be used to support investigation and apprehension of the attacker, and to support criminal and civil legal remedies.
  - *Technological Change and the Environment:* Another active response is to stop an attack in advance and then block subsequent access by the assailant. Typically, IDSs do not possess the power

to stop a specific person's access, but instead block Internet Protocol (IP) addresses from which the attacker seems to be doing. It is very difficult to block a determined and knowledgeable attacker, but IDSs can often deter expert attackers or stop novice hackers by (a) injecting TCP reset packets into the attacker's connection to the victim system, thereby terminating the connection ; (b) reconfiguring routers and firewalls to block packets from the attacker's apparent location (IP address or site); (c) reconfiguring routers and firewalls to block the network ports, protocols, or services being used by an attacker; (d) in extreme situations, re-configuring routers and firewalls to sever all connections that use certain network interfaces.

- *Take Action Against the Intruder:* Some who follow intrusion detection discussions, particularly in information warfare circles, consider that the first option in active response is to call for action against the trespasser. The most aggressive form of this response involves launching attacks against or attempting to actively gain information about the attacker's host or site. However tempting it might be, this response is ill advised. Due to legal ambiguities about civil liability, this option can represent a bigger peril that the attack it is designated to stop. The first reason for approaching this option with a large deal of carefulness is that it may be illegal. Furthermore, as many attackers use false network addresses when attacking systems, it carries with it a high risk of causing damage to innocent Internet sites and users. Finally, strike back can escalate the attack, provoking an attacker who originally thought just to browse a site to contain more aggressive activity.

o *Passive IDS:* Passive IDS responses provide information to system users, relying on humans to take subsequent action based on that information. Many commercial IDSs rely solely on passive responses.

- *Alerts and Notifications:* Alerts and notifications are generated by IDSs to inform users when attacks are discovered. Most commercial IDSs allow users a large deal of latitude in finding out how and when alarms are generated and to whom they are exhibited. The most usual kind of alarm is an onscreen alert or popup window. This is displayed on the IDS console or on other systems as specified by the user during the configuration of the IDS. The information provided in the alarm message varies widely, ranging from a notification that an intrusion has taken place to extremely detailed messages outlining the IP addresses of the source and target of the attack, the specific attack tool used to gain access, and the outcome of the attack. Another set of options that are of utility to large or distributed organizations are those involving remote notification of alarms or alerts. These allow organizations to configure the IDS so that it sends alerts to cellular phones and pagers carried by incident response teams or system security personnel.

- *SNMP Traps and Plug-ins:* Some commercial IDSs are designed to generate alarms and alerts, reporting them to a network management system. These uses SNMP traps and messages to post alarms and alerts to central network management consoles, where they can be serviced by network operations personnel. Several benefits are associated with this reporting scheme, including the ability to adapt the entire network infrastructure to respond to a detected attack, the ability to shift the processing load associated with an active response to a system other than the one being targeted by the attack, and the ability to use common communications channels. *(Bace and Mell, 2001)*

c) IDS Framework/ Architecture

Various intrusion detection system (IDS) frameworks/architectures have evolved over a period of time. These broadly include the following.

- The STAT Framework – The Web STAT intrusion detection system has been developed using the STAT framework *(Vigna et al., 2002)*. The framework provides the implementation of a domain-independent analysis engine that can be extended in a well-defined way to perform intrusion detection analysis in specific application domains. The STAT framework centres around an intrusion modeling technique that characterizes attacks in terms of transitions between the security states of a system. This approach is supported by the STATL attack modeling language. The STATL language provides constructs to represent an attack as a composition of states and transitions. States are used to characterize different snapshots of a system during the evolution of an attack. Obviously, it is not feasible to represent the complete state of a system (e.g., volatile memory, file system); therefore, a STATL scenario uses variables to record just those parts of the system state that are needed to define an attack signature (e.g., the value of a counter or the source of an HTTP request). A transition has an associated action that is a specification of the event that can cause the scenario to move to a new state. For example, an action can be the opening of a TCP connection or the execution of a CGI script. The space of possible relevant actions is constrained by a transition assertion, which is a filter condition on the events that can possibly match the action. For example, an assertion can require that a TCP connection be opened with a specific destination port or that a CGI application be invoked with specific parameters. It is possible for several

occurrences of the same attack to be active at the same time. A STATL attack scenario, therefore, has an operational semantics in terms of a set of instances of the same scenario specification. The scenario specification represents the scenario's definition and global environment, and a scenario instance represents a particular attack that is currently in progress.

The STAT Core module is the run-time for the STATL language. The Core implements the concepts of state, transition, instance, timer, etc. In addition, the STAT Core is responsible for obtaining events from the target environment, and matching this event stream against the actions and assertions corresponding to transitions in the active attack scenarios. The STATL language and the Core runtime are domain independent. They do not support any domain-specific features, which may be necessary to perform intrusion detection analysis in particular domains or environments. For example, network events such as an IP packet or the opening of a TCP connection cannot be represented in STATL natively. Therefore, the STAT framework provides a number of mechanisms to extend the STATL language and the runtime to match the characteristics of a specific target domain.

In summary, a STAT-based sensor is created by developing a language extension that describes the particular domain of the application, an event provider that retrieves information from the environment and produces STAT events, and attack scenarios that describe attacks in terms of state transition models of STAT events. In addition, it is possible to create response libraries that are specific to a certain domain. The response functions in the library can be dynamically associated with the states modeled in the attack scenarios.

- Distributed Intrusion Detection System (DIDS) – DIDS is the second major IDS system having evolved in recent times (Snapp et. al., 2003). The DIDS architecture combines distributed monitoring and data reduction with centralized data analysis. This approach is unique among current IDS's. The components of DIDS are the DIDS director, a single host monitor per host. and a single LAN monitor for each broadcast LAN segment in the monitored network. DIDS can potentially handle hosts without monitors since the LAN monitor can report on the network activities of such hosts. The host and LAN monitors are primarily responsible for the collection of evidence of unauthorized or suspicious activity, while the DIDS director is primarily responsible for its evaluation. Reports are sent independently and asynchronously from the host and LAN monitors to the DIDS director through a communications infrastructure.

High level communication protocols between the components are based on the ISO Common Management Information Protocol (CMIP) recommendations, allowing for future inclusion of CMIP management tools as they become useful. The architecture also provides for bidirectional communication between the DIDS director and any monitor in the configuration. This communication consists primarily of notable events and anomaly reports from the monitors. The director can also make requests for more detailed information from the distributed monitors via a "GET" directive, and issue commands to have the distributed monitors modify their monitoring capabilities via a "SET" directive. A large amount of low level filtering and some analysis is performed by the host monitor to minimize the use of network bandwidth in passing evidence to the director.

The DIDS director consists of three major components that are all located on the same dedicated workstation. Because the components are logically independent processes, they could be distributed as well. The communications manager is responsible for the transfer of data between the director and each of the host and the LAN monitors. It accepts the notable event records from each of the host and LAN monitors and sends them to the expert system. On behalf of the expert system or user interface, it is also able to send requests to the host and LAN monitors for more information regarding a particular subject. The expert system is responsible for evaluating and reporting on the security state of the monitored system. It receives the reports from the host and the LAN monitors, and, based on these reports, it makes inferences about the security of each individual host, as well as the system as a whole. The expert system is a rule-based system with simple learning capabilities. The director's user interface allows the System Security Officer (SSO) interactive access to the entire system. The SSO is able to watch activities on each host, watch network traffic (by setting "wire-taps"), and request more specific types of information from the monitors.

The host monitor is currently installed on Sun SPARC stations running SunOS 4.0.x with the Sun C2 security package. Through the C2 security package, the operating system produces audit records for virtually every transaction on the system. These transactions include file accesses, system calls, process executions, and logins. The contents of the Sun C2 audit record are: record type, record event, time, real user ID, audit user ID, effective user ID, real group ID, process ID, error code, return value, and label.

All possible transactions fall into one of a finite number of events formed by the cross product of the actions and the domains, and each event may also succeed or fail. Note that no distinction is made between files, directories or devices, and that all of these are treated simply as objects. Not every action is applicable to every object; for example, the terminate action is applicable only to processes. The choice of

these domains and actions is somewhat arbitrary in that one could easily suggest both finer and coarser grained partitions. However, they capture most of the interesting behavior for intrusion detection and correspond reasonably well with what other researchers in this field have found to be of interest. By mapping an infinite number of transactions to a finite number of events, not only can the operating system dependencies be removed, but also restrict the number of permutations that the expert system will have to deal with. The concept of the domain is one of the keys to detecting abuses. Using the domain allows us to make assertions about the nature of a user's behavior in a straightforward and systematic way. Although this leads to loss of some details provided by the raw audit information, that is more than made up for by the increase in portability, speed, simplicity, and generality.

The LAN monitor uses heuristics in an attempt to identify the likelihood that a particular connection represents intrusive behavior. These heuristics consider the capabilities of each of the network services, the level of authentication required for each of the services, the security level for each machine on the network, and signatures of past attacks. The abnormality of a connection is based on the probability of that particular connection occurring and the behavior of the connection itself. Upon request, the LAN monitor is also able to provide a more detailed examination of any connection, including capturing every character crossing the network (i.e., a wire-tap). This capability can be used to support a directed investigation of a particular subject or object. Like the host monitor, the LAN monitor forwards relevant security information to the director through its LAN agent.

DIDS utilizes a rule-based (or production) expert system. The expert system is currently written in Prolog, and much of the form of the rule base comes from Prolog and the logic notation that Prolog implies. The expert system uses rules derived from the hierarchical Intrusion Detection Model (IDM). The IDM describes the data abstractions used in inferring an attack on a network of computers. That is, it describes the transformation from the distributed raw audit data to high level hypotheses about intrusions and about the overall security of the monitored environment. In abstracting and correlating data from the distributed sources, the model builds a virtual machine which consists of all the connected hosts as well as the network itself. This unified view of the distributed system simplifies the recognition of intrusive behavior which spans individual hosts. The model is also applicable to the trivial network of a single computer.

- Intrusion Detection System for Cloud Computing – Cloud computing provides application and storage services on remote servers *(Shelke, Sontakke, Gawande, 2012).* The clients do not have to worry about its maintenance and software or hardware up-gradations. Cloud model works on the „concept of virtualization" of resources, where a hypervisor server in cloud data center hosts a number of clients on one physical machine. Deploying HIDS in hypervisor or host machine would allow the administrator to monitor the hypervisor and virtual machines on that hypervisor. But with the rapid flow of high volume of data as in cloud model, there would be issues of performance like overloading of VM hosting IDS and dropping of data packets. Also if host is compromised by an offending attack the HIDS employed on that host would be neutralized. In such a scenario, a network based IDS would be more suitable for deployment in cloud like infrastructure. NIDS would be placed outside the VM servers on bottle neck of network points such as switch, router or gateway for network traffic monitoring to have a global view of the system. Such NIDS would still be facing the issue of large amount of data through network access rate in cloud environment. To handle a large number of data packets flow in such an environment a multi-threaded IDS approach has been proposed in this paper. The multi-threaded IDS would be able to process large amount of data and could reduce the packet loss. After an efficient processing the proposed IDS would pass the monitored alerts to a third party monitoring service, who would in turn directly inform the cloud user about their system under attack. The third party monitoring service would also provide expert advice to cloud service provider for mis-configurations and intrusion loop holes in the system. The cloud user accesses its data on remote servers at service provider's site over the cloud network. User requests and actions are monitored and logged through a multi-threaded NIDS. The alert logs are readily communicated to cloud user with an expert advice for cloud service provider.

Proposed multi-threaded NIDS model for distributed cloud environment is based on three modules: capture & queuing module, analysis/ processing module and reporting module. The capture module, receives the in-bound and out-bound (ICMP, TCP, IP, UDP) data packets. The captured data packets are sent to the shared queue for analysis. The analysis and process module receives data packets from the shared queue and analyze it against signature base and a pre-defined rule set. Each process in a shared queue can have multiple threads which work in a collaborative fashion to improve the system performance. The main process will receive TCP, IP, UDP and ICMP packets and multiple threads would concurrently process and match those packets against pre-defined set of rules. Through an efficient matching and analysis the bad

packets would be identified and alerts generated. Reporting module would read the alerts from shared queue and prepares alert reports. The third party monitoring and advisory service having experience and resources would immediately generate a report for cloud user's information and sends a comprehensive expert advisory report for cloud service provider. Figure above depicts the flow chart of proposed multi-threaded Cloud IDS.

- An implementation of intrusion detection system using genetic algorithm – *Hoque, Mukit and Bikas (2012)* identify the following problems with the existing systems.

o *Snort:* A free and open source network intrusion detection and prevention system, was created by Martin Roesch in 1998 and now developed by Sourcefire. In 2009, Snort entered InfoWorld's Open Source Hall of Fame as one of the "greatest open source software of all time". Through protocol analysis, content searching, and various pre-processors, Snort detects thousands of worms, vulnerability exploit attempts, port scans, and other suspicious behavior.

o *OSSEC:* An open source host-based intrusion detection system, performs log analysis, integrity checking, rootkit detection, time-based alerting and active response. In addition to its IDS functionality, it is commonly used as a SEM/SIM solution. Because of its powerful log analysis engine, ISPs, universities and data centers are running OSSEC HIDS to monitor and analyze their firewalls, IDSs, web servers and authentication logs.

o *OSSIM:* The goal of Open Source Security Information Management, OSSIM is to provide a comprehensive compilation of tools which, when working together, grant network/security administrators with a detailed view over each and every aspect of networks, hosts, physical access devices, and servers. OSSIM incorporates several other tools, including Nagios and OSSEC HIDS.

o *Bro:* An open-source, Unix-based network intrusion detection system Bro detects intrusions by first parsing network traffic to extract its application-level semantics and then executing event-oriented analyzers that compare the activity with patterns deemed troublesome.

o *Fragroute/Fragrouter:* A network intrusion detection evasion toolkit. Fragrouter helps an attacker launch IP-based attacks while avoiding detection. It is part of the NIDS bench suite of tools by Dug Song.

o *BASE:* The Basic Analysis and Security Engine, BASE is a PHP-based analysis engine to search and process a database of security events generated by various IDSs, firewalls and network monitoring tools. A Genetic Algorithm (GA) is a programming technique that mimics biological evolution as a problem-solving strategy. It is based on Darwinian's principle of evolution and survival of fittest to optimize a population of candidate solutions towards a predefined fitness. When using GA for solving various problems three factors will have vital impact on the effectiveness of the algorithm and also of the applications. These include:

- the fitness function;
- the representation of individuals;
- the GA parameters. The determination of these factors often depends on applications and/or implementation.

The present paper aims to understand the emerging avenues in Intrusion Detection System, as to what all models, architectures are available for detecting intrusions and how to prevent those intrusions to occur in any network traffic. The paper further focuses on challenges in the current intrusion detection system while also comparatively analyzing the Active and Passive Response Systems. Finally, the paper explores the possible future avenues in intrusion detection scheme.

II. Findings and Discussion

IDS is an emerging trend in network security as intrusions are increasing day by day due to internet availability with high level of usage among people across the globe. With improvements in the network is required to protect one`s information lying unsecured over the internet and should not be revealed to unauthorized people or groups. Cloud computing is another emerging trend which has shot up demand of security over free network, i.e. Internet *(Shelke et. al, 2012).*

On the basis of analysis done from available systems in Intrusion Detection proposed by people in different geographical areas, different network or environment requires a different level of security and infrastructure is another concern to implement IDS or related services.

Currently, networked computer systems play an ever more major function in our fellowship and its economic system. They have become the targets of a wide array of malicious threats that invariably turn into real intrusions. This is the reason computer security has become a vital concern for network practitioner. Too often, intrusions cause disaster inside LANs and the time and cost to renovate the damage can grow to extreme proportions. Instead of using passive measures to repair and patch security hole once they have been exploited, it is more efficient to take up a proactive measure to intrusions *(Gomez, Dasgupta, 2002).*

Intrusion Detection Systems (IDS) are primarily focused on identifying probable incidents, monitoring

information about them, tries to stop them, and reporting them to security administrators in real-time environment, and those that exercise audit data with some delay (non-real-time). The latter approach would in turn delay the instance of detection. In addition, organizations apply IDSs for other reasons, such as classifying problems with security policies, documenting existing attacks, and preventing individuals from violating security policies. IDSs have become a basic addition to the security infrastructure of almost every organization *(Hassan, 2013).* A usual Intrusion Detection System is demonstrated in Figure 1 below.

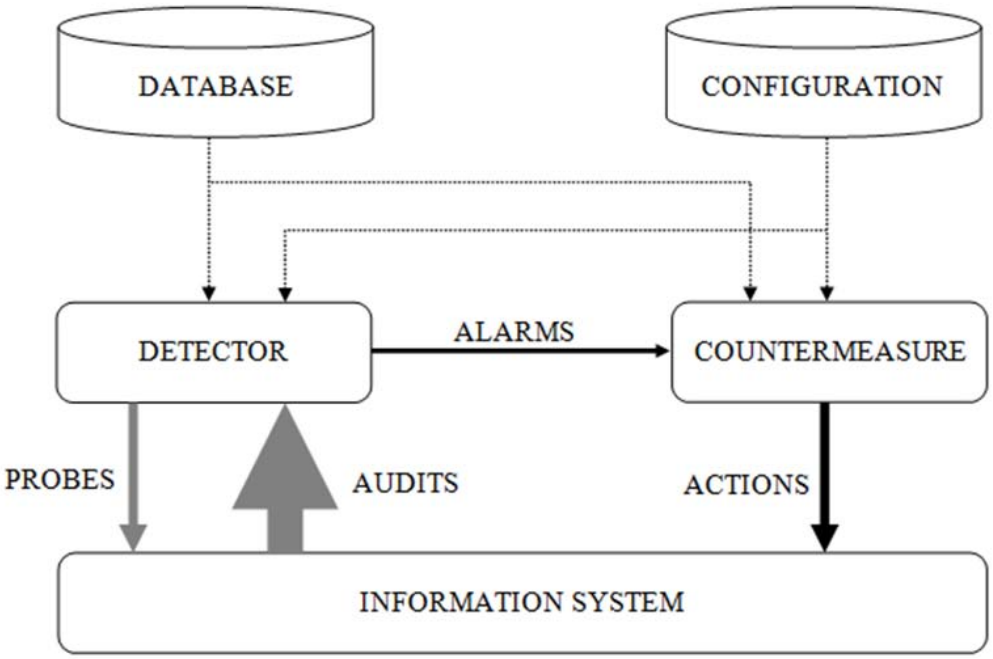

Figure 1

Note: The arrow lines symbolize the amount of information flowing from one component to another

Very Simple Intrusion Detection System

One of the major problems encountered by IDS is large number of false positive alerts that is the alerts that are mistakenly analyzed normal traffic as security violations. An ideal IDS does not produce false or inappropriate alarms. In practice, signature based IDS found to produce more false alarms than expected. This is due to the very general signatures and poor built in verification tool to authenticate the success of the attack. The large amount of false positives in the alert logs generates the course of taking corrective action for the true positives, i.e. delayed, successful attacks, and labor intensive.

The normal and the abnormal intrusive activities in networked information processing systems are hard to forecast as the limits cannot be easily explained. This prediction process may generate false alerts in many anomaly based intrusion detection schemes. However, with the introduction of fuzzy logic, the false alarm rate in determining intrusive activities can be minimized; a set of fuzzy rules (noncrisp fuzzy classifiers) can be employed to identify the normal and abnormal behavior in computer networks, and fuzzy inference logic can be applied over such rules to determine when an intrusion is in progress. The primary problem with this procedure is to make good fuzzy classifiers to detect intrusions *(Tillapart, 2002).*

The intrusion detection strategies concern four primary issues. First is the dataset that is captured from network communications. The second is Genetic Algorithms (GA) which use mutation, recombination, and selection applied to a population of individuals in order to evolve iteratively better and better solutions and a way to generate fuzzy rules to characterize normal and abnormal behavior of network systems. The third is to generate alerts and reports for malicious traffic behavior, and the fourth is the maintenance of the ids for observation of placement of sensors, and qualified trained intrusion analysts so that the latest malicious traffic is being detected.

The following future trends are clearly visible in intrusion detection systems.

- *Genetic Algorithm (GA):* GA is a programming technique that uses biological evolution as a problem solving strategy. It is based on Darwinian's theory of evolution and survival of fittest to make effective a population of candidate result near a predefined fitness. The proposed GA based

intrusion detection system holds two modules where each acts in a dissimilar stage. In the training stage, a set of classification rules are produced from network audit data using the GA in an offline background. In the intrusion detection phase, the generated rules are employed to classify incoming network connections in the real-time environment. Once the rules are generated, the intrusion detection system becomes simple, experienced and efficient one.

GA applies an evolution and natural selection that employs a chromosome-like data structure and evolve the chromosomes by means of selection, recombination and mutation operators. The process generally starts with randomly generated population of chromosomes, which signify all possible solution of a problem that are measured candidate solutions. From each chromosome different positions are set as bits, characters or numbers. These positions are regarded as genes. An evaluation function is employed to find the decency of each chromosome according to the required solution; this function is known as "Fitness Function". During the process of evaluation "Crossover" is applied to have natural reproduction and "Mutation" is applied to mutation of species. For survival and combination the selection of chromosomes is partial towards the fittest chromosomes *(Hassan, 2013).*

- *Fuzzy Logic:* A fuzzy expert system consists of three different types of entities: fuzzy sets, fuzzy variables and fuzzy rules. The membership of a fuzzy variable in a fuzzy set is determined by a function that produces values within the interval [0, 1]. These functions are called membership functions. Fuzzy variables are divided into two groups: antecedent variables, that are assigned with the input data of the fuzzy expert system and consequent variables, that are assigned with the results computed by the system.

The fuzzy rules determine the link between the antecedent and the consequent fuzzy variables, and are often defined using natural language linguistic terms. For instance, a fuzzy rule can be" if the temperature is cold and the wind is strong then wear warm clothes", where temperature and wind are antecedent fuzzy variables, wear is a consequent fuzzy variable and cold, strong and warm clothes are fuzzy sets *(Hassan, 2013).*

The process of a fuzzy system has three steps. These steps are Fuzzification, Rule Evaluation, and Defuzzification. In the fuzzification step, the input crisp values are transformed into degrees of membership in the fuzzy sets. The degree of membership of each crisp value in each fuzzy set is determined by plugging the value into the membership function associated with the fuzzy set. In the rule evaluation step, each fuzzy rule is assigned with a strength value. The strength is determined by the degrees of memberships of the crisp input values in the fuzzy sets of antecedent part of the fuzzy rule. The defuzzification stage transposes the fuzzy outputs into crisp values.

III. Conclusion

The study focused on studying existing IDS and their usefulness in detecting and preventing attacks in any type of network and control traffic with the performance of the system to be improved as well. It is found that intrusion has different meaning and scenarios defining need of attack detection and prevention of attacks.

Deterrence is the key to the value of IDS. The benefit of deploying an IDS depends on how much it prevents hackers from committing intrusions. Although IDSs are classified as detective controls because they detect attacks that were not prevented, they implicitly act as preventive controls by changing the behavior of attackers in the first place, and thus eliminating attacks.

The presence of a network-based IDS can put hackers on notice that their actions may lead to legal action. Host-based systems provide very similar deterrent effect. People who know that their actions may be monitored are less likely to commit misuse.

Optimally configured IDSs always provide non-negative value to their adopters. By using the out-of-box configuration, firms may be taking the easy way out, but they may be hurting themselves. Current widespread complaint against IDSs is that they produce many false alarms: False positives are tremendous time wasters and drive up operational labor costs.

IDS developers should also pay close attention to the configuration issue. They should design IDSs that are easy to configure, especially in light of high false positive rates associated with IDSs. Most vendors do not provide these data. Various groups, including academic institutions, research labs, and commercial organizations, have tested commercial and government sponsored IDS products.

All the IT security concerns are integral part of security programs and therefore, should be carefully designed and deployed. Recently, organizations realized that it is impossible to eliminate all security risks. As a result, detection based systems have started to gain popularity in the IT security domain. Today, IDSs are the most popular detective controls. Although IDS has been the fastest-growing security product in the market for the last few years, the security community is uncertain about their value.

An improperly configured IDS may encourage more hacking, resulting in a higher loss for the firm. An optimally configured IDS deters hackers, thus, reducing the need for investigation by security experts for security violations. To firms that are using default configuration

or that have not adopted an IDS because of doubts about its value, our results provide incentives to implement an appropriately configured IDS.

IV. Limitations and Future Research Directions

As with all models, the model parameters were common knowledge to the firm and users. One region that looks particularly interesting is games with incomplete information, in which either the assembly or the user is unsure about the other's payoffs. This perspective allows incorporation of uncertainty about the nature of the game being played.

It may be more realistic to consider a multiperiod model in which the firm revises its estimates every period based on its observations of the hacker's strategy in previous periods. Such learning has been analyzed in game theory.

Security experts take appropriate actions after receiving alarms from IDSs. This approach, also called passive response, is the current trend in commercial IDSs. Another response option is to let the IDS take an action without human intervention (active response). Current IDSs provide little or no guidance to security management once an attack has been identified.

IDSs are here to stay, with billion dollar firms supporting the development of commercial security products and driving hundreds of millions in annual sales. Nevertheless, they remain hard to configure and operate and often can't be effectively utilized by the very novice security personnel who demand to benefit from them most.

References Références Referencias

1. Anderson, J. P. (1972). Computer Security Technology Planning Study Volume II. *Electronic Systems Division (AFSC)*.
2. Bace, R., & Mell, P. (2001). NIST special publication on intrusion detection systems. *National Institute of Standards and Technology, CA*.
3. Balasubramaniyan, J. S., Garcia-Fernandez, J. O., Isacoff, D., Spafford, E., & Zamboni, D. (1998). An Architecture for Intrusion Detection Using Autonomous. *Paper, COAST Technical Report, Purdue University*.
4. Botha, M., & Solms, R. v. (2004). Utilizing Neural Networks For Effective Intrusion Detection. *Port Elizabeth Technikon, South Africa*.
5. Denning, D. E. (1987). An Intrusion Detection Model.
6. Gomez , J., & Dasgupta, D. (2002). Evolving Fuzzy Classifiers for Intrusion Detection. *IEEE*.
7. Graham, R. (2000, January 07). *FAQ: Network Intrusion Detection Systems.* Retrieved from www.robertgraham.com.
8. Hassan, M. M. (2013). Current Studies on Intrusion Detection System, Genetic Algorithm And Fuzzy Logic. *International Journal of Distributed and Parallel Systems*.
9. Hoque, M. S., Mukit, M., & Bikas, M. N. (2012). An Implementation of Intrusion Detection System using Genetic Algorithm. *International Journal of Network Security & Its Applications (IJNSA)*.
10. Institute, S. (2001). Understanding Intrusion Detection Systems. *SANS Institute*.
11. Scarfone, K., & Mell, P. (2007). Intrusion Detection and Prevention Systems. *National Institute of Standards and Technology Special Publication*.
12. Shelke, M. K., Sontakke, M., & Gawande, D. D. (2012). Intrusion Detection System for Cloud Computing. *International Journal of Scientific & Technology Research*.
13. Snapp, S. R., Brentano, J., Dias, G. V., Goan, T. L., Heberlein, L. T., Ho, C.-L., et al. (2002). DIDS (Distributed Intrusion Detection System) - Motivation, Architecture, and An Early Prototype. *University of California, Davis*.
14. Tillapart, P., Thumthawatworn, T., & Santiprabhob, P. (2002). Fuzzy Intrusion Detection System. *Thesis, Assumption University,Bangkok*.
15. Vigna, G., Robertson, W., Kher, V., & Kemmerer, R. A. (2002). A Stateful Intrusion Detection System forWorld-Wide Web Servers. *University of California, Santa Barbara*.
16. Zamboni, D. (2001). Using internal sensors for computer intrusion detection. *Center for Education and Research in Information Assurance and Security, Purdue University*.

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 16 Issue 4 Version 1.0 Year 2016
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Performance Evaluation of ALOHA-CS MAC Protocol

By Mst. Rubina Aktar
Bangladesh University of Engineering and Technology

Abstract- The main task of a MAC protocol is to prevent simultaneous transmissions or resolve transmission collisions of data packets while providing energy efficiency, low channel access delays and fairness among the nodes in a network [1]. The Aloha protocol is a fully decentralized medium access control protocol. This protocol was introduced to improve the utilization of the shared medium by synchronizing the transmission of devices. The performance of the Carrier sense Pure ALOHA is evaluated in this paper on the basis of throughout of the system and the average number of retransmission needed for the successful transmission of a packet. Performance criteria are analyzed with change of offered load of the system. The simulation is a Monte Carlo based one on the MATLAB platform.

Keywords: MAC protocol; pure ALOHA; carrier sense Pure ALOHA; throughput; random access technique.

GJCST-E Classification : C.2.2

Strictly as per the compliance and regulations of:

Performance Evaluation of ALOHA-CS MAC Protocol

Mst. Rubina Aktar

Abstract- The main task of a MAC protocol is to prevent simultaneous transmissions or resolve transmission collisions of data packets while providing energy efficiency, low channel access delays and fairness among the nodes in a network [1]. The Aloha protocol is a fully decentralized medium access control protocol. This protocol was introduced to improve the utilization of the shared medium by synchronizing the transmission of devices. The performance of the Carrier sense Pure ALOHA is evaluated in this paper on the basis of throughout of the system and the average number of retransmission needed for the successful transmission of a packet. Performance criteria are analyzed with change of offered load of the system. The simulation is a Monte Carlo based one on the MATLAB platform.

Keywords: MAC protocol; pure ALOHA; carrier sense Pure ALOHA; throughput; random access technique.

I. Introduction

Medium Access Control (MAC) protocols are collection of algorithms for solving the problem of sharing a single channel by multiple transmitting nodes. The problems can be solved by partitioning the channel, or by allowing random access of the transmitting nodes or by hybrid algorithms [2]. The performance of any algorithm or protocol is evaluated on the basis of some factors: average time of a packet spent in the transmission queue, throughput- fraction of channel capacity for useful data transmission, fairness to the transmitting nodes, stability and robustness against channel fading, power consumption, support for multimedia etc. Pure ALOHA is a random access protocol for solving the problem for sharing a single channel by multiple transmitting. In this paper, the performance of carrier sense Pure ALOHA protocol is analyzed on the basis throughput and the average number of retransmission of the packets. The paper is organized as follows: Random access technique for sharing a single access point is introduced is section II. In section III, the mathematical formulation of Pure ALOHA technique is show. In Section IV, the system model is introduced, simulation techniques are discussed and the results are analyzed.

II. Random Access Technique

In Random access technique, no portion of the channel is kept fixed for any transmitting node, rather the channel is allocated to the transmitting nodes on a random basis. When a packet comes to the transmitting nodes it checks whether the channel is free. If it is free, the node sends the packet through the packet. In case of the channel being occupied, the packet is retransmitted after a random interval according to some algorithms for retransmission. It specifies how to detect collision and how to recover from collisions.

III. The Pure Aloha Technique

For analyzing Aloha in communication, let all packets have same length L and required T seconds for transmission. This can be visualized in Fig .1. The figure 1 shows three stations A, B and C that have sent packets. At first packet A send a time t_o, If packet B send any time between time $t_o - T$ and t_o, then end of packet collides with beginning of packet A . If packet C sends any time between time t_o and $t_o + T$, starts of packet C collides with end of packet A.

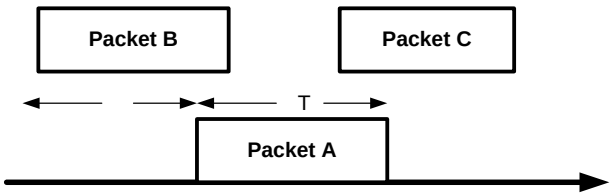

Fig. 1 : Pure Aloha

Collisions occur if packet transmissions overlap by any amount of time. Since all the packet overlap with part of another, no transmission was successful.

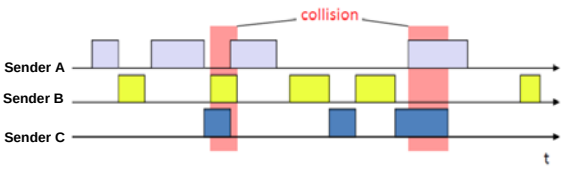

Fig. 2 : Aloha collisions

The transmission of a packet is successful if the packet does not collide with other packets at the destination.

In Pure ALOHA the vulnerable period- the time interval during which the packets are susceptible to collisions with transmissions from other users is considered to be twice the transmission length of each packet. For the study of pure ALOHA it is assumed that all the packets have same packet length, channel data

Author: Dept. of Electrical and Electronic Engineering Bangladesh University of Engineering and Technology Dhaka, Bangladesh.
e-mail: rubi07eee@gmail.com

rate is fixed and the users generate new packet at random time interval.

The number of packet generated per unit time follows Poisson's distribution:

$$\Pr[k] = \frac{\lambda^k e^{-\lambda}}{k!} \quad (1)$$

Where, k is number of packet generated per unit time, λ is the only parameter of the Poisson's distribution i.e. the average number of packet generated per unit time [3].

The performance of the system is characterized by throughput S of the system.

$$S = \begin{bmatrix} Average\ number\ of\ Packet \\ generated\ within \\ packet\ transmission\ time, T_p \end{bmatrix} \begin{bmatrix} Probability\ of \\ no\ collision \end{bmatrix}$$

Here,

$$\begin{matrix} Probability\ of \\ no\ collision \end{matrix} = \begin{matrix} Probability\ of \\ generating\ no\ packet \\ within\ vulnerable\ time, 2T_p \end{matrix}$$

$$= \Pr[0] = \frac{(2\lambda T_p)^0 e^{-2\lambda T_p}}{0!} = e^{-2\lambda T_p}$$

$$S = (\lambda T_p) e^{-2\lambda T_p} = G e^{-2G} \quad (2)$$

Here, G is the offered load. When offered load is 0.5, the throughput is maximum and maximum throughput for pure ALOHA is 18.7%. But here we uses Carrier Sense (CS) ALOHA, which senses whether the channel is free before transmission so the throughput is greater than throughput for normal (without carrier sensing) pure ALOHA.

IV. Protocal Discption and Model

Carrier sense ALOHA is different from others ALOHA. It extends the carrier sensing function to include all packets regardless of whether the sensing device is the recipient or not. Aloha is predecessor to carrier sense multiple excess systems used in many broadcast system. Thus ALOHA depends on the ability of a node to detect or learn that a collision has occurred [4]. Here the evaluation is considered a wireless local area network having N nodes and a single access point which is shown in Fig .1. The four nodes are competing to gain the access of AP for transmitting their data packets. The MAC protocol used for sharing the AP is ALOHA with carrier sense (ALOHA-CS). Therefore, a node with a new data packet immediately senses the carrier. If the carrier is idle, the node transmits the packet immediately. If the carrier is busy, transmission of the packet is delayed by an integer number of packet duration. After retransmission try by the maximum allowed times, a packet will be dropped.

The simulation has been performed on a MATLAB based Monte-Carlo simulation platform. Here, a wireless local area network (LAN) with a single access point (AP) and four nodes competing to gain the access of AP for transmitting their data packets is considered which is illustrated in Fig. 3.

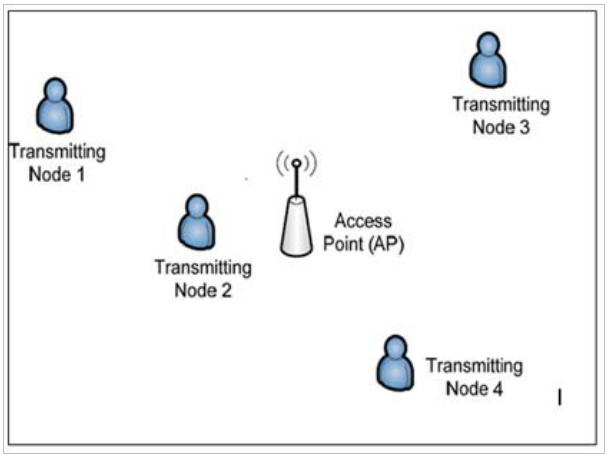

Fig. 3 : Access Point and Trasnmitting Nodes inside LAN

V. Simulation and Result

a) Random Packet generation

Packet from each transmitting node is generating according to Poisson's distribution, so the time interval between each packet is an exponential distribution with mean 1 */ no of packet generation in unit time.* Exponentially distributed random numbers are generated in MATLAB for representing packet access in the access point. All the packets are equally probable to come from any of the transmitting nodes; so they are distributed among the transmitting nodes using uniforms integer random number generator from 1 to 4. A packet in access point can be retransmitted packet or a fresh packet, where a packet can be retransmitted not more than 8 times.

b) Throughput Analysis

Throughput is defined as the ratio of the successfully transmitted packet per sec to the number of packet generated per sec. In pure ALOHA a node can start transmission at any time. In slotted ALOHA, all nodes have synchronized clocks marking frame boundary times (the clock period is the time for one frame transmission) and a node wishing to transmit does so at the start of the next frame slot. In both cases, a node transmits without checking the state of the channel [5].

The throughput which is defined as the portion of channel bandwidth for successful transmission i.e. percentage of successful transmission of total transmission is calculated and plotted for three different packet lengths: 2000, 4000 and 10000 bits in Fig.4.

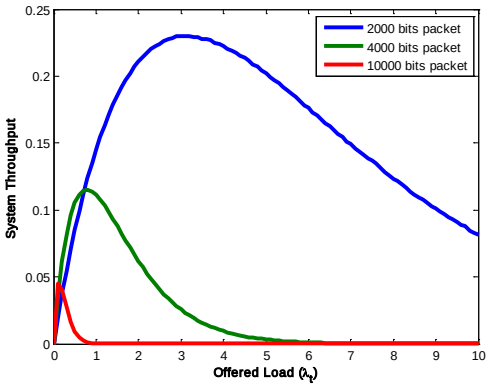

Fig. 4 : System Throughput Vs. Offered Load (λ_t)

Fig.4 indicates that throughput of packet length 4000 is higher than packet length 10000 and throughput of packet length 2000 is higher than packet length 4000.

c) Average No. of Retransmission

The Average number of retransmission is also calculated for the three packet lengths which increases with offered load as expected.

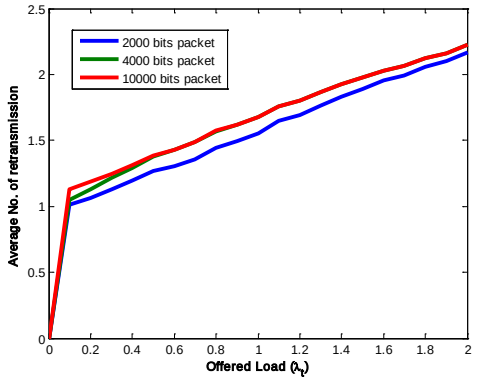

Fig. 5 : Average No. of Retransmission Vs. Offered Load (λ_t)

For a given critical limit of the new packet generation rate, the number of transmission control is not needed for a stable operation. The reason is that if the new packet generation rate is below a certain limit, the probability of success is very high because of the lower aggregate traffic generation rate [6]. The probability of retransmission is very low in that situation. Therefore, the aggregate traffic generation is lower even with the higher maximum allowable number of transmissions. The aggregate traffic generation rate increases with the multiplication of the retransmission probability and number of transmissions, for a given new packet generation rate[7]. If the retransmission probability becomes very low because of higher success probability, the multiplication of retransmission probability and the number of transmissions also become very low. Hence, the aggregate traffic generation rate becomes almost the same as the new packet generation rate. Thus, the throughput also remains almost constant regardless of the augmentation of number of transmissions. This lower aggregate traffic generation rate is not sufficient to make the system unstable. This critical limit of the new packet generation rate depends on the number of users and the type of capture.Fig.5 shows that the number of retransmission vs offered load. The average number of retransmission increases as the offered load increases.

VI. Conclusion

Aloha-CS is simpler and more scalable, as it only needs a small amount of memory, and does not rely on additional control messages. Aloha-CS, on the other hand, requires the use of additional packets, which serve as advance notification to neighboring nodes, so that they can avoid transmitting packets that could result in collisions. The Aloha-CS needs to collect and store more information, therefore it requires more resources. Due to the need to select a suitable lag time for a given network setting, the scheme is less scalable as it needs to check if its lag time is still appropriate whenever there are any significant topology changes. However, the extra cost allows the Aloha-CS to achieve much better throughput and collision avoidance. Throughput maximizes for a definite offered load and average number of retransmission increases with offered load as expected.

References Références Referencias

1. N. Abramson, “The Aloha system – another alternative for computer communications”, AFIPS Conference Proceedings, vol. 36, 1970, pp.295-298.
2. V. Rodoplu and M. K. Park, “An energy-efficient MAC protocol for underwater wireless acoustic networks”, in *Proc. MTS/IEEE OCEANS'05*.
3. T. S. Rappaport, “Wireless Communicaions – Principles and Practice” ,Second Edition, Pearson Education, 2002.
4. J. Kong, J. hong Cui, D. Wu, and M. Gerla, “Building underwater ad-hoc Networks and sensor networks for large scale real-time aquatic applications”, in *Proceedings of MILCOM*, 2005.
5. L. Merakos and D. Kazakos, “On Retransmission Control Policies in Multiple-Access Communication Networks”, IEEE Transactions on Automatic Control, Vol. AC-30, No. 2, pp. 109–117, 1985.
6. E. Paolini, G. Liva, and M. Chiani “High Throughput Random Access via Codes on Graphs: Coded Slotted ALOHA’’ in Proc. 2011 IEEE Int. Conf. Commun., Kyoto, Japan, Jun. 2011.
7. G. Ferrari and O. Tonguz, “Performance of Ad Hoc Wireless Networks With Aloha and PR-CSMA MAC Protocols”, IEEE Global Telecommunications Conference, San Francisco, USA, vol. 5, pp. 2824 – 2829, December 2003.

This page is intentionally left blank

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 16 Issue 4 Version 1.0 Year 2016
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Quality of IT Enabled Services in Higher Education Institutions in Saudi Arabia

By Romana Aziz & Basit Shahzad
Prince Sultan University

Abstract- The delivery of education has improved over time by using the IT enabled services, especially in the higher education institutes. The role of the IT enabled services to disseminate effective teaching has increased over time and still improving with a great pace with emerging needs of the students and the teachers. This research paper is focused to identify and investigate the quality of IT enabled services in the higher education institutes in Saudi Arabia. The study was conducted at two model higher education institutions from public and private sector. Mixed research method has been used to attain the information and to identify the convergence of the information. It was identified that the quality of IT enabled services in better in the public sector institution ascompared to the private sector institution.

Keywords: quality of education, quality of IT enabled services, education Saudi Arabia.

GJCST-E Classification : K.4.2

Strictly as per the compliance and regulations of:

Quality of IT Enabled Services in Higher Education Institutions in Saudi Arabia

Romana Aziz [α] & Basit Shahzad [σ]

Abstract- The delivery of education has improved over time by using the IT enabled services, especially in the higher education institutes. The role of the IT enabled services to disseminate effective teaching has increased over time and still improving with a great pace with emerging needs of the students and the teachers. This research paper is focused to identify and investigate the quality of IT enabled services in the higher education institutes in Saudi Arabia. The study was conducted at two model higher education institutions from public and private sector. Mixed research method has been used to attain the information and to identify the convergence of the information. It was identified that the quality of IT enabled services in better in the public sector institution ascompared to the private sector institution.

Keywords: quality of education, quality of IT enabled services, education Saudi Arabia.

I. Introduction

Access to education is a fundamental right of each child and making this access better is an obligation of the government. The emergence of IT and its utilization in the education sector has helped the students at all levels, to improve their capability to learn and without need to memorizing text but by learning the conceptual grounds and theories. Thus, IT has played its role in making the teaching and learning, not only interesting but also effective in the recent years. The role of IT Enabled Services (ITES) has been vital in the higher education institutes as well and now, as the baseline of the ITES has been established at most institutes it is becoming important to evaluate the quality of ITES at different institutes. In this paper, we focus on two higher education institutions from public and private sector. We have chosen universities in Saudi Arabia as the study is focused to make a comparison of the ITES in Saudi universities.

Considering the nature of the study, two leading universities, one each from government and private sector was selected to participate in the study as they exist in same city. The public sector university (referred as A in the rest of this paper)was established in the fifties and is one of the oldest university in the kingdom while the private sector university (referred as B in the rest of this paper) was established in the nineties. It is also important to mention that the current student enrolment at the private university is around 3,500 while the public sector university has 10 times mores enrolment, and so is the ratio in the staff of the universities. The purpose of this study is to compare the state of the ITES in the Saudi universities.

II. Literature Review

In order to compare the state of the art it is important to establish the parameters based on which the comparisons among the universities can be made for the quality of ITES. Some recent work has been carried out in this domain which is presented in the this section. Several researchers [1][2][3][4][5], including Alanezi and Yang have mentioned that the 'Accessibility' factor is vital in nature for measuring the quality of ITES. Tan and Burgess [5][1][4] have advocated the need for customization as a major player in the quantification of the ITES for the higher education while Parasuraman and George[1][6][2][7] are of the view that delivery of teaching and the efficiency of the ITES is also important.

Alanezi, Lin, Sedera and Swaid[1][8][9][10] have identified the importance and have advocated the existence of the factors like functionality and information quality. Both these factors form the core of ITES and are valuable in their nature and existence. Zeithaml [2] has found that some factors like response time, service usability, system integrity and trust are important factors in the quantification of the quality measurement. These factors govern the environmental factors and responsiveness of the system and are vital to measure the quality of the system instead of functionality of the system. Tan, George and Burgess [1][4][7] have advocated the presence of security as an integral factor to measure the quality of ITES. Apart from that, some researchers like Burgess [5] have considered that the factors like site design, service usability and service reliability have a great value in the measurement of the quality of the ITES. Aziz [11] in her research shortlisted these seventeen items to evaluate the quality of the ITES in the higher education. The shortlisting was done from more than 100 elements based on the recurrence, relevance and importance which was determined by the expert opinion. The factor, its description and the citation of the survey is given in Table 1.

Author α: College of Computer & Information Sciences, Prince Sultan University, Riyadh, Saudi Arabia. e-mail: raziz@psu.edu.sa
Author σ: College of Computer & Information Sciences, King Saud University, Riyadh, Saudi Arabia. e-mail: basit.shahzad@gmail.com

Table 1 : Factors to measure ITES quality

No	Factor	Description	
1	Accessibility	Accessibility is the degree to which the user can access the required service	[1][2][3][4][5]
2	Customization	The ability to configure the ITES according to requirement	[5][1][4]
3	Delivery of teaching	It deals with the ways and quality of the teaching.	[7]
4	Efficiency	How quickly the required services are available.	[1][6][2][7]
5	Functionality	It describes that what specific tasks can be performed by using the system	[1][8]
6	Information quality	By what level the available information suits the user.	[9][10]
7	Interoperability	Access to multiple service	[4]
8	Privacy	The level to which a person is secure in performing his tasks without being public.	[7][6][1]
9	Response time	The time between the request and availability of the information	[2]
10	Security	Security factor reflects the adequacy of security features implemented in the ITES.	[7][1][4]
11	Service reliability	Service reliability is the percentage of time the ITES is available for use without failure.	[5]
12	Service usability	Service usability factor refers to the degree to which the users find it easy to use the various ITES.	[2]
13	Site design	Site design factor measures the quality of site design in terms of user satisfaction and ease of use.	[5]
14	System integrity	The provision of consistent information at all times.	[2]
15	Trust	How reliable, efficient and responsive a system is.	[2]
16	Usefulness	Usefulness is the degree to which the users find it easier to do their work via the ITES.	[5]
17	User support	User support factor refers to the degree to which the ITES department personnel are willing to serve the users in case their help and support is required.	[3]

The findings by Aziz [11] form the basis of this study. The findings are contemporary in nature and discuss an evolutionary paradigm of emerging state of the art from the authors of immense repute [12, 13]. Ahead of this a considerably sound and current methodology to affirm the findings was used that increase the trust to use this findings of the publication as a base of this research.

III. Methodology

This study is a mixed method research [14, 15], that has been completed by triangulating the qualitative and quantitative results. The survey was conducted on 300 individuals in each institute and the results were collected. The purpose of the survey was to ask the users about the quality of IT enabled services at their respective institute, against the different factors attained after the comprehensive literature review. Likert scale [16] was used to rank the responses on a scale of 1-5, i.e. from poor to excellent, hence, the column 1 in each response list has the weightage 1, the 2nd column has the weightage 2 and column 3 has the weightage of 3 and so on. Once the sums are accumulated they are divided by the number of total respondents to get the weighted average and this activity is run for both institutes separately. After that the comparison among the results is made by considering each factor to identify that in which area a specific institute is performing better. A qualitative study has been conducted on the same lines where four respondents were interviewed (two from each university) and were asked to identify the standards of the IT enabled service in their respective institutes based on the factors and considering the cotemporary situations[17-24]. In this research we follow the partially mixed sequential dominant status paradigm where the qualitative findings follow the quantitative findings and are dominant. This paradigm is followed in research studies that are centric to evaluate the technology education [25-31].

IV. Quantitative Study

Considering the scale of the survey it is important to maximize the responses, however it is notable that the responses have to be precise and should come from the experienced users[17, 32]. In order to achieve this the means given in Table 2 are used to spread the survey and collect the responses. The effectiveness of these means is given in Table 3 while Figure 1 illustrates the spread of survey call.

Table 2 : Means of Sending Survey and responsiveness

No.	Mean of	Count	Responses	%
1	Paper	10	10	*100*
2	Web Link	500	398	*80*
3	Skype Text	20	10	*50*
4	Google Talk	50	30	*60*
5	Phone call	60	40	*67*
6	Text	40	36	*90*
7	Facebook	96	64	*67*
Total		776	588	*75*

Table 3 : Effectiveness of each mean by percentage

No.	Mean of Sending Survey	Count	Responses	Average Response
1	Paper Survey	10	10	*1.7%*
2	Web Link	500	398	*67.6%*
3	Skype Text Request	20	10	*1.7%*
4	Google Talk Link Forwarding	50	30	*5.1%*
5	Phone call Requests	60	40	*6.8%*
6	Text message Requests	40	36	*6.12%*
7	Facebook messaging	96	64	*10.8%*

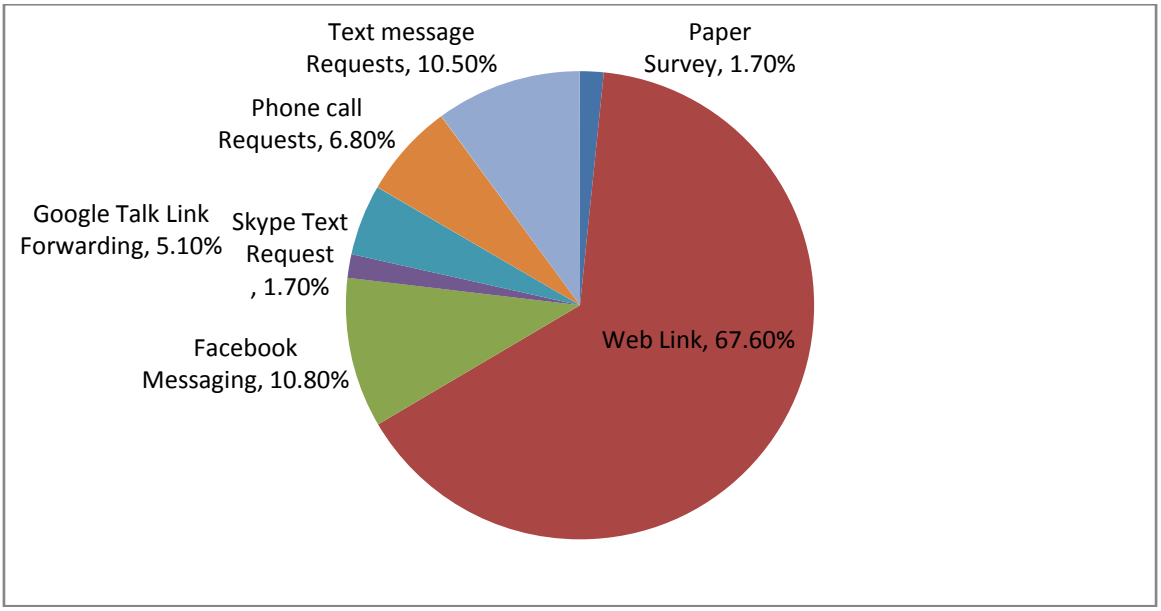

Figure 1 : Proportionate spread of the survey call

The Survey reached to 776 while 588 out of them responded. Following statistics in Table 4 are used for this survey.

Table 4 : Statistics for the survey conduct

Measure	Number
Confidence Level	99%
Confidence Interval	3
Population accessed	776
Sample Size	548
percentage	50

**The actual population size is unknown [9]*

Confidence level demonstrates the level of confidence that we have on the response to be correct and precise. Usually a confidence level of 95% is used in the research although 99% is used. The confidence interval determines the amount of acceptable results, and is always presented with the ± symbol. If the threshold value is 67 and the confidence interval is 5, it will allow considering values from 62-72 as legitimate. Since the survey has been conducted in two different institute to compare the state of the art of IT enabled services, almost half of the responses came from each institute. A 5-level Likert scale has been used in this research that ranges from poor to excellent. The range is from 1-5 on a quantitative scale. The value for poor is 1 and value for excellent is 5. Every response that choses the 'poor' against some item is multiplied by 1 while the selections like 'somewhat acceptable' is multiplied by2, the choice 'acceptable' is multiplied by 3, the choice 'very good' is multiplied by 4, and the choice 'excellent' is multiplied by 5. The average weighted response is achieved by divining the weighted response over the total number of respondents. It is further important that some questions were not answered by some individuals. For institute A, 261 respondents have responded while some 325 respondents responded for the institute B.

Table 5 : Survey response statistics from institute A

Items	Poor	Somewhat Acceptable	Acceptable	Very Good	Excellent	Average Weighted Response
Accessibility	0	42	270	492	135	3.60
Customization	0	48	972	1584	315	3.41
Delivery of teaching	3	24	252	504	90	3.59
Efficiency	0	36	216	516	180	3.72
Functionality	0	30	278	384	255	3.67
Information quality	3	36	234	504	165	3.65
Interoperability	3	42	331	384	90	3.78
Privacy	3	36	341	492	105	3.88
Response time	3	24	261	456	165	3.65
Security	0	42	243	420	90	3.53
Service reliability	0	24	234	336	165	3.67
Service usability	0	24	297	348	225	3.68
Site design	0	6	234	552	120	3.75
System integrity	0	36	279	456	105	3.56
Trust	0	42	405	348	75	3.37
Usefulness	0	30	297	372	210	3.65
User support	0	36	252	348	225	3.68

Table 6 : Survey response statistics from institute B

Items	Poor	Somewhat acceptable	Acceptable	Very Good	Excellent	Average Weighted Response
Accessibility	12	102	531	312	75	3.17
Customization	0	126	540	228	75	2.94
Delivery of teaching	42	120	531	156	15	2.69
Efficiency	9	132	495	216	120	3.06
Functionality	6	138	504	288	75	3.06
Information quality	21	72	414	384	150	3.24
Interoperability	30	96	432	264	120	3.02
Privacy	24	138	177	120	75	1.70
Response time	9	108	477	288	135	3.17
Security	18	132	468	228	120	3.01
Service reliability	18	138	468	204	75	2.92
Service usability	24	108	441	288	60	2.98
Site design	21	144	477	192	90	2.91
System integrity	18	180	450	168	60	2.81
Trust	6	150	432	264	135	3.10
Usefulness	18	144	495	204	75	2.92
User support	12	144	468	228	90	2.99

Table 7 : Comparison of Institute A and B for quality of ITES

Items	AWR (Average Weighted Response) Somewhat acceptable		Better on Quantitative Scale
	Institute A	Institute B	
Accessibility	3.60	3.17	Institute-A
Customization	3.41	2.94	Institute-A
Delivery of teaching	3.59	2.69	Institute-A
Efficiency	3.72	3.06	Institute-A
Functionality	3.67	3.06	Institute-A
Information quality	3.65	3.24	Institute-A
Interoperability	3.78	3.02	Institute-A
Privacy	3.88	1.70	Institute-A
Response time	3.65	3.17	Institute-A
Security	3.53	3.01	Institute-A
Service reliability	3.67	2.92	Institute-A
Service usability	3.68	2.98	Institute-A
Site design	3.75	2.91	Institute-A
System integrity	3.56	2.81	Institute-A
Trust	3.37	3.10	Institute-A
Usefulness	3.65	2.92	Institute-A
User support	3.68	2.99	Institute-A

V. Qualitative Study and Triangulation

Table 5 and Table 6 summarize the survey response statistics from institute A and B respectively. The results shown in Table 7 , clearly demonstrate that the quality of ITES is better in institute A as compared to institute B in all the factors. Considering these results a qualitative study was formulated where four interviews were conducted to gain an insight of the ITES in the respective institutes. The outcome is given in Table 8. Along with the illustrative description of the ITES quality items, the interviewees preferred to give the absolute numbers in measuring the quality. Four interviews were conducted in total Two interviews were conducted in institute A while rest two were conducted at institute B. The summary of the results is presented in Table 8 which clearly demonstrates that the interviewees (like the survey respondents) believed that the quality of ITES is better in institute A as compared to institute B. In the survey, institute A was observed having lead in the quality factors while in the interviews institute A leads in 12 out of 17 factors, equal in 4, and lags in 1 factor. Figures 2 and 3 depict the quantitative and qualitative analysis respectively.

Table 8 : Outcome of the 4 interviews

Items	Qualitative Response		Better on Quantitative Scale
	Institute A	Institute B	
Accessibility	4	3.5	Institute-A
Customization	3.5	3.5	-
Delivery of teaching	3	2.5	Institute-A
Efficiency	4	2.5	Institute-A
Functionality	3.5	3.5	-
Information quality	4	3.5	Institute-A
Interoperability	4.5	3	Institute-A
Privacy	4	2.5	Institute-A
Response time	3	3.5	Institute-B
Security	4	2.5	Institute-A
Service reliability	4.5	3	Institute-A
Service usability	4	3.5	Institute-A
Site design	4	3	Institute-A
System integrity	4	2.5	Institute-A
Trust	3.5	3.5	-
Usefulness	3.5	3.5	-
User support	4.5	3.5	Institute-A

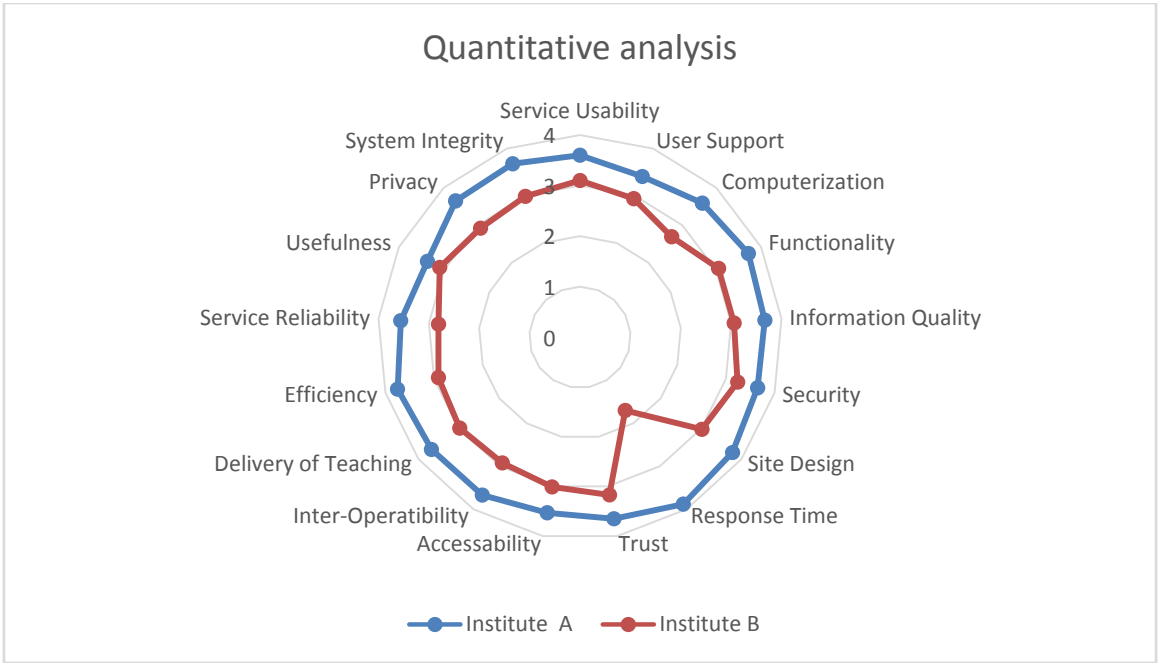

Figure 2 : Quantitative analysis of ITES

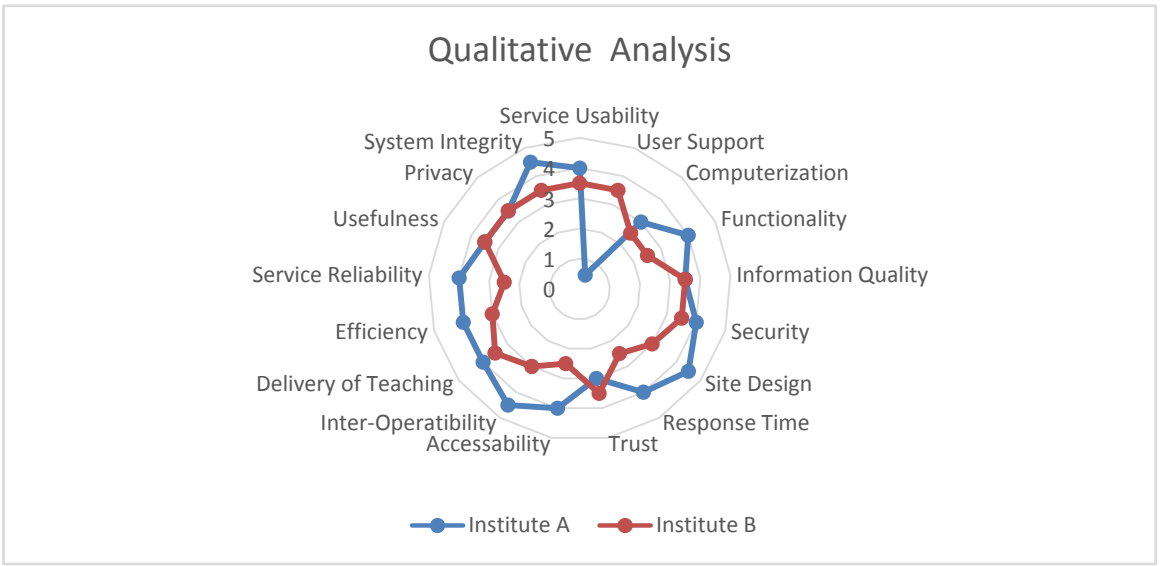

Figure 3 : Qualitative analysis of ITES

In triangulation process, it is observed that whether the findings of the qualitative method and the quantitative methods converge to similar results? The triangulation process is shown in Table 9.

Table 9 : Triangulation of Qualitative and quantitative results

Items	AWR Somewhat acceptable		Better on Quantitative Scale			Better on Qualitative Scale	Triangulation Results
	Institute A	Institute B		Institute A	Institute B		
Accessibility	3.60	3.17	Institute-A	4	3.5	Institute-A	Institute-A
Customization	3.41	2.94	Institute-A	3.5	3.5	Equal	Equal
Delivery of teaching	3.59	2.69	Institute-A	3	2.5	Institute-A	Institute-A
Efficiency	3.72	3.06	Institute-A	4	2.5	Institute-A	Institute-A
Functionality	3.67	3.06	Institute-A	3.5	3.5	Equal	Equal
Information quality	3.65	3.24	Institute-A	4	3.5	Institute-A	Institute-A
Interoperability	3.78	3.02	Institute-A	4.5	3	Institute-A	Institute-A
Privacy	3.88	1.70	Institute-A	4	2.5	Institute-A	Institute-A
Response time	3.65	3.17	Institute-A	3	3.5	Institute-B	Institute-B
Security	3.53	3.01	Institute-A	4	2.5	Institute-A	Institute-A
Service reliability	3.67	2.92	Institute-A	4.5	3	Institute-A	Institute-A
Service usability	3.68	2.98	Institute-A	4	3.5	Institute-A	Institute-A
Site design	3.75	2.91	Institute-A	4	3	Institute-A	Institute-A
System integrity	3.56	2.81	Institute-A	4	2.5	Institute-A	Institute-A
Trust	3.37	3.10	Institute-A	3.5	3.5	Equal	Equal
Usefulness	3.65	2.92	Institute-A	3.5	3.5	Equal	Equal
User support	3.68	2.99	Institute-A	4.5	3.5	Institute-A	Institute-A

VI. Discussion

There are 17 factors for measuring the quality of ITES in the institutes in Saudi Arabia. Two intuitions, one government and one private university was selected for this purpose in the capital city of Riyadh. The results of the study demonstrate that the quality of the ITES is better in institute A as compared to B. After the completion of the triangulation process the results have not changed much from the initial process, since the findings were very much consistent in the quantitative and qualitative methods. For the factors like 'accessibility', 'delivery of teaching', 'efficiency', 'information quality', 'inter-operability', 'privacy', 'security', 'service reliability', 'service usability', 'site design', 'system integrity', and 'user support' the results of the qualitative and quantitative findings were same. For the factors 'customization', 'functionality, 'trust', and 'usefulness'. the qualitative findings are different from the quantitative findings where in the survey it was established that the institute A is better as compared to institute B but in the interview it was established that both institutes have same standing. It was mentioned in the methodology section that the qualitative findings will have the dominance on the quantitative findings, therefore the qualitative results are observed in case of a disagreement among the qualitative and quantitative findings. Since the results of the qualitative finding demonstrate that the state-of-art of two institutions for these four factors is not different therefore the qualitative findings hold. For one factor 'response time' in the quantitative findings it was observed that the institute A is better in comparison while the results of the qualitative findings are otherwise, but for the reasons mentioned above, the qualitative results are held.

VII. Conclusion

It can be summarized that the in order to compare the state-of-art of ITES in Saudi universities 17 factors were identified. Two institutions were compared based on quantitative and qualitative data, and the results have shown that institute A leads with better score on 12 factors while for four factors the scores were equal, while institute B leads only in one factor. It can be concluded that the state-of-art of ITES is much better in institute A as compared to institute B. Institute B needs to be more concerned in improving the quality of the ITES, especially in the areas of accessibility, information security, privacy, and user support. While Institute A needs to improve in customization, usefulness, response time, and trust.

VIII. Acknowledgement

The authors thank Prince Sultan University in the Kingdom of Saudi Arabia for funding this project in the year 2013-2014 under number IBRP-CFW-2013-11-14.

References Références Referencias

1. M. A. Alanezi, A. Kamil, and S. Basri, "A proposed instrument dimensions for measuring e-government service quality," *International Journal of u-and e-Service,* vol. 3, pp. 1-18, 2010.
2. V. A. Zeithaml, A. Parasuraman, and A. Malhotra, "Conceptual Framework for understanding e-service quality: Implications for future research and managerial practice," 2000.
3. Z. Yang, S. Cai, Z. Zhou, and N. Zhou, "Development and validation of an instrument to measure user perceived service quality of information presenting web portals," *Information & Management,* vol. 42, pp. 575-589, 2005.
4. C.-W. Tan, I. Benbasat, and R. T. Cenfetelli, "IT-mediated customer service content and delivery in electronic governments: An empirical investigation of the antecedents of service quality," *MIS quarterly,* vol. 37, pp. 77-109, 2013.
5. L. Burgess, "A conceptual framework for understanding and measuring perceived service quality in net-based customer support systems," in *CollECTeR LatAm Conference, Santiago, Chile*, 2004, pp. 13-15.
6. A. Parasuraman, V. A. Zeithaml, and A. Malhotra, "ES-QUAL a multiple-item scale for assessing electronic service quality," *Journal of service research,* vol. 7, pp. 213-233, 2005.
7. A. George and G. G. Kumar, "Impact of service quality dimensions in internet banking on customer satisfaction," *DECISION,* vol. 41, pp. 73-85, 2014.
8. H.-F. Lin, "Determining the relative importance of mobile banking quality factors," *Computer Standards & Interfaces,* vol. 35, pp. 195-204, 2013.
9. D. Sedera and G. Gable, "A factor and structural equation analysis of the enterprise systems success measurement model," *ICIS 2004 Proceedings,* p. 36, 2004.
10. S. I. Swaid and R. T. Wigand, "Measuring the quality of e-service: Scale development and initial validation," *Journal of Electronic Commerce Research,* vol. 10, pp. 13-28, 2009.
11. B. Shahzad and R. Aziz, "Factors for Measurement of ITES Quality for Higher Education Institutions in Saudi Arabia," *Global Journal of Computer Science and Technology,* vol. 15, pp. 1-10, 2015.
12. B. Shahzad and E. Alwagait, "Utilizing Technology in Education Environment: A Case Study," in *Information Technology: New Generations (ITNG), 2013 Tenth International Conference on*, 2013, pp. 299-302.
13. S. Livingstone, "Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression," *New media & society,* vol. 10, pp. 393-411, 2008.

14. D. A. Abowitz and T. M. Toole, "Mixed method research: Fundamental issues of design, validity, and reliability in construction research," *Journal of Construction Engineering and Management,* vol. 136, pp. 108-116, 2009.
15. J. C. Greene, V. J. Caracelli, and W. F. Graham, "Toward a conceptual framework for mixed-method evaluation designs," *Educational evaluation and policy analysis,* vol. 11, pp. 255-274, 1989.
16. J. W. Lee, P. S. Jones, Y. Mineyama, and X. E. Zhang, "Cultural differences in responses to a Likert scale," *Research in nursing & health,* vol. 25, pp. 295-306, 2002.
17. J. W. Creswell., "Research Design: Qualitative, Quantitative, and Mixed Methods Approaches," *Sage Publications,* , 2009.
18. J. Ritchie, J. Lewis, C. M. Nicholls, and R. Ormston, *Qualitative research practice: A guide for social science students and researchers*: Sage, 2013.
19. G. Goldkuhl, "Pragmatism vs interpretivism in qualitative information systems research," *European Journal of Information Systems,* vol. 21, pp. 135-146, 2012.
20. S. Q. Qu and J. Dumay, "The qualitative research interview," *Qualitative Research in Accounting & Management,* vol. 8, pp. 238-264, 2011.
21. L. I. Meho, "E-mail interviewing in qualitative research: A methodological discussion," *Journal of the American society for information science and technology,* vol. 57, pp. 1284-1295, 2006.
22. C. Weston, T. Gandell, J. Beauchamp, L. McAlpine, C. Wiseman, and C. Beauchamp, "Analyzing interview data: The development and evolution of a coding system," *Qualitative sociology,* vol. 24, pp. 381-400, 2001.
23. C. E. Hill, K. D. Loch, D. Straub, and K. El-Sheshai, "A qualitative assessment of Arab culture and information technology transfer," *Journal of Global Information Management (JGIM),* vol. 6, pp. 29-38, 1998.
24. P. Burnard, "A method of analysing interview transcripts in qualitative research," *Nurse education today,* vol. 11, pp. 461-466, 1991.
25. Y. Al-Ohali, A. A. Al-Oraij, and B. Shahzad, "KSU News Portal: A Case Study," *International Conference on Internet Computing (ICOMP'11),* 2011.
26. B. Shahzad and A. Alwagait, "Does a Change in Weekend Days Have an Impact on Social Networking Activity?," *Journal of Universal Computer Science,* vol. 20, pp. 2068-2079, 2015.
27. E. Alwagait, B. Shahzad, and S. Alim, "Impact of social media usage on students academic performance in Saudi Arabia," *Computers in Human Behavior,* vol. 51, pp. 1092-1097, 2015.
28. B. Shahzad, E. Alwagait, and S. Alim, "Impact of Change in Weekend Days on Social Networking Culture in Saudi Arabia," in *2014 International Conference on Future Internet of Things and Cloud (FiCloud)*, 2014, pp. 553-558.
29. B. Shahzad and J. Iqbal, "" Software Risk Management–Prioritization of frequently occurring Risk in Software Development Phases. Using Relative Impact Risk Model," *2nd International Conference on Information and Communication Technology (ICICT2007),* pp. 16-17, 2007.
30. B. Shahzad, J. Iqbal, Z. ul Haq, and S. Raza, "Distributed risk analysis using relative impact technique," *3rd Asian Conference on Intelligent Systems and Networks,* pp. 433-439, 2006.
31. B. Shahzad, T. Afzal, and R. Irfan, "Enhanced risk analysis-relative impact factorization," in *Information and Communication Technologies, 2005. ICICT 2005. First International Conference on*, 2005, pp. 290-295.
32. A. M. S. Basit Shahzad, "Application of Quantitative Research Methods in Identifying Software Project Factors," *International Journal of Information Technology and Electrical Engineering,* vol. 1, pp. 30-33, 2012.

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 16 Issue 4 Version 1.0 Year 2016
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Cryptanalysis and Further Improvement of a Dynamic ID and Smart Card based Remote user Authentication Scheme

By Narendra Panwar
Uttarakhand Technical University

Abstract- Computer systems and their interconnections using networks have im-proved the dependence of both the organizations as well as the individuals on the stored information. This interconnection, in turn, has led to a heightened awareness of the need for data security and the protection of data and re- sources from electronic frauds, electronic eavesdropping, and network-based attacks. Consequently, cryptography and network security have evolved, leading to the development of smart cards to enforce network security. Re-cently, Rafael Martinez-Pelez and Rico-Novella Francisco [1] pointed out vul-nerabilities in Wang et al. [2] scheme. In this paper, we crypt-analyze Wanget al. scheme and demonstrated that our proposed scheme withstands thevulnerabilities pointed out by Francisco et al. and it completes all the re-cent security requirements of [3]. We implemented the proposed scheme in MATLAB and demonstrated that our proposed scheme is not vulnerable to the shortcomings pointed out by Francisco et al. in their scheme.

Keywords: *security, authentication, remote user, smart card.*

GJCST-E Classification : *C.2.3 C.2.5*

Strictly as per the compliance and regulations of:

Cryptanalysis and Further Improvement of a Dynamic ID and Smart Card based Remote user Authentication Scheme

Narendra Panwar

Abstract- Computer systems and their interconnections using networks have im-proved the dependence of both the organizations as well as the individuals on the stored information. This interconnection, in turn, has led to a heightened awareness of the need for data security and the protection of data and re- sources from electronic frauds, electronic eavesdropping, and network-based attacks. Consequently, cryptography and network security have evolved, leading to the development of smart cards to enforce network security. Re-cently, Rafael Martinez-Pelez and Rico-Novella Francisco [1] pointed out vul-nerabilities in Wang et al. [2] scheme. In this paper, we crypt-analyze Wanget al. scheme and demonstrated that our proposed scheme withstands thevulnerabilities pointed out by Francisco et al. and it completes all the re-cent security requirements of [3]. We implemented the proposed scheme in MATLAB and demonstrated that our proposed scheme is not vulnerable to the shortcomings pointed out by Francisco et al. in their scheme.

Keywords: security, authentication, remote user, smart card

I. Introduction

In 1981, a remote password authentication scheme was proposed by L. Lamport [4] over an insecure channel. Since then, several schemes [5], [6], [7], [8], [9], [10] have been proposed to address this problem for achieving more functionality and efficiency. In a traditional password scheme, each user has an identity and a secret password. If a person wants to log into a network system, they must submit their identity and the corresponding password.

Preprint submitted to Journal of Information Science and Applications May 31, 2016

To avoid storing a plain password table in a public network system, several scheme [4], [11], [12] have proposed a dictionary of verification tables to store each user ID and the corresponding one-way hash value of passwords in the remote system. In 2005, Chien et al.[9] pointed out that Das et al.[8] scheme cannot achieve user anonymity because an attacker can trace user with the static value. In 2010, Lee et al.[13] have analyzed the security of the smart card based user authentication scheme proposed by Lee and Chiu [14]. Their security analysis showed that scheme [9] does not achieve its main security goal of the two-factor security. To demonstrate this, they have shown that the scheme is vulnerable to an o_-line dictionary attack in which an attacker, who has obtained the secret values stored in the users smart card can easily find out its password. Besides reporting the security problem, they showed what really is causing the problem and how to fix it and they proposed a new and improved scheme than Lee and Chius scheme.

In 2012, Francisco et al. have shown security vulnerabilities like Denial of service, server spoong, impersonation in Wang et al. [2] scheme. We propose a scheme that can withstand the above mentioned attacks, we implemented and demonstrated the stated scheme using MATLAB. The paper is organized as follows.

In Section 2, we give a brief review on Wang et al.s scheme. We demon- strate the vulnerabilities of the scheme in Section 3. The proposed scheme and its security analysis are presented in section 4 and 5. Section 6 com- pares the performance of our proposed scheme with other related schemes. Finally, we conclude this paper in Section 7.

Author: e-mail: naren.rishikesh@gmail.com

Table 1: Notation Table

Symbol	Description
U_i	The User
S	The Remote Server
ID_i	Unique identity of U_i
PW_i	Unique password of U_i
S_k	The common session key
$\oplus$	The bitwise XOR operation
H(.)	A collision free one-way hash function such as SHA-256
x,y	Secret Keys of S

II. Review of Wang et al. Scheme

Wang et al. proposed a dynamic ID and smart card based remote user authentication scheme in which the remote server does not maintain a verification table and chooses the users password. Table 1 describes the notations used in this paper and Table 2 depicts review of Wang et al. scheme.

Table 2 : Wang et al scheme

User U_i	**Server S**
Registration Phase	
Select ID_i	Choose PW_i
Send ID_i to Server S	Compute A_i=H(PW_i)$\oplus$H(x)$\oplus$$ID_i$
	Store [A_i,y,H(.)] into Smart Card
	Sends PW_i and Smart Card to U_i through secure channel

Table 2 : Wang et al scheme

User U_i	**Server S**
Login Phase U_i keys in his/her ID_i and PW_i into smart card terminal and perform: CID_i=H(PW_i)⊕H(A_i⊕y⊕T)⊕ID_i Send M_i=[ID_i, CID_i, A_i,T] to S.	**Verification Phase** Verify T*-T ≤ Δ T, if time interval is incorrect then reject login request otherwise accept M_i and perform: H(PW_i)*=CID_i⊕H(A_i⊕y⊕T)⊕ID_i Compute ID_i*=H(PW_i)*⊕H(x)⊕A_i If ID_i*and ID_i are not equals, then reject login request otherwise S performs: Computes B= H(H(PW_i)*⊕y⊕T_2) Sends [B, T_2] to U_i
Server Verification Phase Verify T_2-T≤ ΔT, if the time interval is incorrect then U_i terminate phase, otherwise perform: Computes B*=H(H(PW_i)⨁y⨁T_2) If B*=B holds U_i confirms the identity of S.	

Table 2 : Wang et al scheme

User U_i	**Server S**
Password Change Phase U_i insert smart card into card reader and keys in his/her PW_i, new password NPW_i and performs: A_i*=A_i⊕H(PW_i)⊕H(NPW_i) Store A_i* into smart card with replacing A_i.	

III. Cryptanalysis of Wang et al. Scheme

In this section, we demonstrate that Wang et al. scheme is vulnerable to the followings attacks.

a) Denial-of-Service attack

There is no user id and password verification mechanism at client terminal. Therefore, if the user enters false identity ID_i^* it will compute CID_i^* and U_i send it to the server S as login request without verifying users identity.S computes

$$H(PWD_i)^*=CID_i^* \oplus H(A_i \oplus y \oplus T) \oplus ID_i^*$$

and

$$ID_i^{**}=H(PW_i)^* \oplus H(x) \oplus A_i.$$

Computed ID_i^{**} will never match to the ID_i^* received by the server from the user U_i. If such case happens unnecessary computing will be performed by the server, and it will lead to Denial-of-Service attack..

b) Impersonation attack

Wang et al.'s scheme cannot withstand impersonation attack. The attacker can create a valid login request message if he/she obtains $A_i^* H(x)$ and y. If a legitimate user with mal intent wishes to attack the server he/she can extract $H(x)$ from his/her card and can establish a valid session with the server and thus becoming an attacker using his/ her user privileges. Table 3 describes impersonation attack on Wang et al scheme.

Table 3 : Impersonation attack on Wang et al scheme

Legitimate User (Attacker) U_a	**Server S**
Using smart card Compute $H(x)=H(PW_a) \oplus A_a \oplus ID_a$ Intercept previous message $[ID_i, CID_i, A_i, T]$ of User U_i $H(PW_i)=A_i \oplus H(x) \oplus ID_i$ $CID_i^*=H(PW_i) \oplus H(A_i \oplus y \oplus T^*) \oplus ID_i$ Send $M_i=[ID_i, CID_i, A_i, T^*]$ to S	**Verification Phase** Verify $T^*-T \leq \Delta T$, if time interval is incorrect then reject login request otherwise accept M_i and perform: $H(PW_i)^*=CID_i \oplus H(A_i \oplus y \oplus T^*) \oplus ID_i$ Compute $ID_i^*=H(PW_i)^* \oplus H(x) \oplus A_i$ Here ID_i^* and ID_i are equals so login request accepted by the server and S performs: $B=H(H(PW_i)^* \oplus y \oplus T^{**})$ Sends $[B, T^{**}]$ to U_a

Table 3 : Impersonation attack on Wang et al scheme

Legitimate User (Attacker) U_a	**Server S**
Server Verification Verify $T^{**}-T^* \leq \Delta T$, now time interval is correct and U_a perform: $B^*=H(H(PW_i) \oplus y \oplus T^{**})$ Now session will successfully start between the legitimate attacker U_a and server S.	CID

c) Server spoofing attack

Wang et al. scheme is vulnerable to server spoofing attack which is shown in Table 4. In this scheme,S needs to know y and H(x) for verifying the legitimacy of each user. If the attacker is a legitimate user U_a he/she can impersonate as S to cheat U_i because he/she knows y and H(x). After the user U_i receives the acknowledgement message [B,T**] he/she will compute $B^*=H(PW_i) \oplus y \oplus T^{**}$ and checks whether or not B^* is equal to B In this case, U_i will believe that the attacker is the legitimate S, and will establish a session key with S for further communication.

Table 4 : Server spoofing attack on Wang et al scheme

Legitimate User U_i	**Legitimate User (Attacker) U_a as S**
Login Phase	
U_i keys in his/her ID_i and PW_i into smart card terminal and perform:	
$CID_i=H(PW_i)\oplus H(A_i\oplus y\oplus T)\oplus ID_i$	**Intercept message M_i of User U_i**
Send $M_i=[ID_i,CID_i,A_i,T]$ to S.	$M_i=[ID_i,CID_i,A_i,T]$
	Compute $H(x)=H(PW_a)\oplus A_a\oplus ID_a$
	Compute $H(PW_i)=A_i\oplus H(x)\oplus ID_i$
	Computes $B=H(H(PW_i)\oplus y\oplus T^{**})$
	Sends $[B,T^{**}]$ to U_i
Server Verification	
Verify $T^{**}-T^*\leq \Delta T$, if time interval is correct then U_i perform:	
$B^*= H(H(PW_i)\oplus y\oplus T^{**})$	
Now the session will successfully start between legitimate user U_i and attacker user U_a.	

d) Password Change Phase Flaws

In the password change phase of Wang et al. scheme, we observe that an attacker user U_i can change password of any other legitimate user U_is, which is shown in Table 5.

Table 5 : Password change flaws of Wang et al scheme

Legitimate User U_l	**Attacker User U_a**
Login Phase	
U_l keys his/her ID_l and PW_l into smart card terminal and perform:	
Computes	
$CID_l=H(PW_l)\oplus H(A_l\oplus y\oplus T)\oplus ID_l$	
Send $M1=[ID_l,CID_l,A_l,T]$ to S.	
	Intercept message M_1 of User U_l
	$M1=[ID_l,CID_l,A_l,T]$
	Compute $H(x)=H(PW_a)\oplus A_a\oplus ID_a$
	Change password
	Compute $H(PW_l)=A_l\oplus H(x)\oplus ID_l$
	Attacker user U_a computes:
	$A_a{*}=A_l\oplus H(PW_l)\oplus H(NPW_l)$
	Store $A_l{*}$ into smart card replacing with A_l.

IV. Proposed Scheme

This section proposes a strong, secure authentication scheme which will with- stand the security vulnerabilities which leads to the aforementioned attacks.

a) Registration phase

In this phase, the user U_i registers with the remote server S through a secure channel to be a authentic user.

Step 1: U_i chooses his/her identity ID_i and password PW_i and computes $H(ID_i\|PW_i\|R_x$ where R_x random number generated by U_i. Then U_i sends the registration request $H(ID\|PW_i\|R_x)]$ to S.

Step 2: Upon receiving $[ID_i H(ID\|PW_i\|R_x]$ from , S veri_es the validity of and computes $VID_i=H(K\oplus ID_i)$

Step 3: S computes $N_i=VID_i\oplus H(ID_i\|PW_i\|R_x$ then captures current date and time in T and create a record $[ID_i,T]$ in its database.

Step 4: S stores $[H(.),N_i T]$into the smart card of U_i and sends the smart card through a secure channel to the user U_i

Step 5: Upon receiving the smart card fromS,U_istores into smart card and does not need to remember R_x after _nishing registration phase. Finally, U_i's, smart card contains $[H(.),N_i T,R_x]$

b) Login phase

In this phase, when an authentic user want to login to the remote server S, he/she must perform the following steps:

Step 1: U_i inserts his/her smart card into the card reader and inputs the identity $ID_i$and password PW_i The smart card computes $VID_i{*}=N_i\oplus H(ID_i\|PW_i\|R_x)$, where$R_x$ is retrieved from its memory space.

Step 2: The smart card computes $T=T+1$ and $M_1=(ID_i\|VID_i{*}\|R_x\|T)^2$ mod n and sends a login request M_1 to S

c) Authentication phase

Upon receiving the login request M1 from U_i, S performs the following steps:

Step 1: S reveals M_1 by using the Chinese Remainder Theorem (CRT) with p and q to obtainID_i VID_i R_x and T. Then S veri_es the revealed T with the stored T_i corresponding to ID_i. If T _ T, S replaces T_i with new time variable T in its database. Otherwise, S rejects U_i's, login request.

Step 2: If Step 1 holds, S computes$VID_i=H(K\oplus ID_i)$,and checks if computed VID_i equals received $VID_i{*}$. If it holds, S would successfully authenticate U_i. and computes the session key$S_k=H(VID_i\|R_x\|T)$shared with U_i.

Step 3: S computes$M_2=H(VID\|R_x$ and send it to U_i.

Step 4: Ui computes $M_2{*}=H(VIDikRx)$ and check if computed $M_2{*}$ equals received M_2. If it does not hold, Ui stops the session. Otherwise, Ui now successfully authenticate S and use $S_k=H(VID_i\|R_x\|T)$ shared session key with S for securing future communications.

d) Password change phase

In this phase, the user U_i inserts the smart card into device and inputs ID_i, original passwordPW_i, new password $PW_i{*}$ and $R_x{*}$, where $R_x{*}$ is a new random

number generated by U_i. Then, the smart card computes $B=H(ID_i\|PW_i\|R_x)$, $B^*=H(ID_i\|PW_i^*\|R_x^*)$ and $A_i=A_i\oplus B\oplus B^*$. Finally, the values A_i and R_x stored in U_i's, smart card are replaced with A and R_x^*, respectively. Here the password PW_i^* of user U_i has been changed to a new password PW_i^* with o_ine session.

V. Security Analysis

In this section, we analyzed the security of the proposed scheme and shown that our scheme is secure against the following well-known attacks. The security of our proposed authentication scheme is based on the secure hash function and the CRT. In the following steps, we analyzed the security of the proposed scheme to verify that the specified security requirements [3] are fulfilled.

a) Resistance to user anonymity attack

Suppose that the attacker intercepted U_i's, authentication messages. Then, the adversary cannot retrieve any static parameter from these messages, due to the CRT. Hence, the proposed scheme can preserve user anonymity.

b) Resistance to offine password guessing attack

Suppose that a malicious legitimate attacker user U_a has got U_i's, smart card, and the secret information $[H(.),N_i\ T$ and R_x can also be revealed under our assumption of the non-tamper resistant smart card. Even after gathering this information, the attacker has to at least guess both ID_i and PW_i, correctly at the same time, because it has been demonstrated that our scheme can provide identity protection. It is impossible to guess these two parameters correctly at the same time, and thus the proposed scheme can resist offine password guessing attack with smart card security breach.

c) Resistance to stolen verifier attack

In the proposed scheme no sensitive verifiers corresponding to the users are maintained by S. Therefore, the proposed scheme is free from the stolen verifier attack.

d) Resistance to user impersonation attack

As VID_i and N_i are protected by secure one-way hash function, any modification to these parameters of the legitimate user U_i's, will be detected by the server S. Because the attacker has no way of obtaining the values of ID_i PW_i and N_i cor-responding to user U_i he/she cannot fabricate the valid VID_i and Ni, Therefore, the proposed scheme is secure against user impersonation attack.

e) Resistance to server masquerading attack

In the proposed scheme, a malicious server S^* cannot compute the correct mes- sage $M_2=H(VID_i\|R_x$ without knowing U_i's, valid VID_i and R , S* has to break the secure one-way hash function to retrieve ID_i PW_i and R_x from $H(ID_i\|PW_i\|R_x)$. Therefore, the proposed scheme is free from server masquerading attack.

f) Resistance to replay attack

Our scheme can withstand replay attack because the authenticity of authentcation messages M_1 is verified by checking the time variable T.

g) Resistance to parallel session attack

If an adversary masquerade as legitimate user U_i by replaying a previously intercepted authentication message. The attacker cannot compute valid T because he does not know the values of $M_1=(ID_i\|VID_i\|R_x\|T)^2$ mod n corresponding to user U_i. Therefore, the resistance to parallel session attack can be guaranteed in our scheme.

h) Resistance to mutual authentication

In our scheme user U_i computes $M_2^*=H(VID_i\|R_x$ and veri_ed with received M_2. If it hold, U_i authenticate the server S veri_cation successfully and uses $S_k=H(VID_i\|R_x\|T$ shared session key with S for future communications.

i) Resistance to forward secrecy

Based on the dificulty of the one-way hash algorithm, any previously generated session keys cannot be revealed without knowledge of the VID_i R_x and T. As a result our scheme provides the property of forward secrecy.

VI. Computational Cost Analysis

In this scheme we have taken 1.0 unit average run time for a single one-way secure hash function operation. The proposed scheme requires lower computation overhead with comparison to other schemes, which is shown in the Table 6 and the Figure 1.

Table 6 : Computational cost analysis

Computational overhead/Scheme	A_1	A_2	A_3	A_4	A_5	Our Sch.
Computation overhead in the registration phase	5Th	5Th	3Th	3Th	2Th	2Th
Execution overhead in the registration phase	5.0	5.0	3.0	3.0	2.0	2.0
Computation overhead in the login phase	7Th	3Th	2Th	2Th	2Th	2Th
Execution overhead in the login phase	7.0	3.0	2.0	2.0	2.0	2.0
Computation overhead in the authentication phase	11Th	9Th	5Th	5Th	5Th	5Th
Execution overhead in the authentication phase	11.0	9.0	5.0	5.0	5.0	5.0
Total execution overhead	23.0	17.0	10.0	10.0	9.0	9.0

Schemes:A1: Mishra et al A2:Hao et al A3:Lee et al A4:Wen et al A5:Wang et al

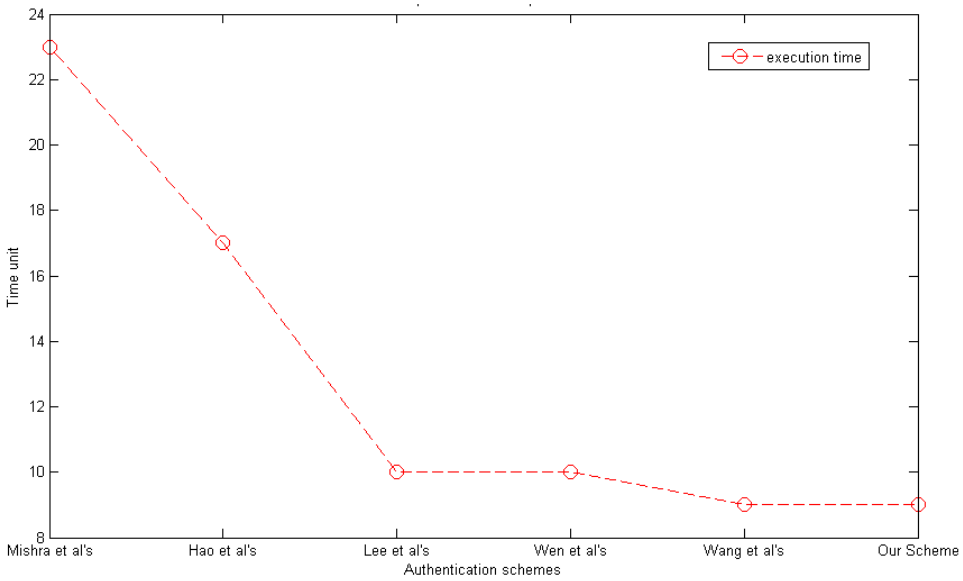

Figure 1 : Comparison of computational cost

VII. Conclusion

Wang et al.s scheme was proposed for resolving security issues presented in pre- vious work of [8]. However, we have discovered some security aws in their scheme making it vulnerable to various attacks such as impersonation, server spoofing and denial of service attack. Moreover, the scheme cannot withstand password change aws. As a remedy to the aforementioned weaknesses, we have presented an enhanced scheme, which overcome the vulnerabilities of [15] and [1] scheme.

References Références Referencias

1. R. Mart'nez-Pel_aez, F. Rico-Novella, Weaknesses of an eficient and secure dynamic ID-based remote user authentication scheme, Procedia Technology 3 (2012) 351{353. doi:10.1016/j.protcy.2012.03.038. URLhttp://linkinghub.elsevier.com/retrieve/pii/ S2212017312002678
2. J. D. Y. Y. Wang, J.Y. Liu, F.X. Xiao, A more eficient and secure dynamic ID-based remote user authentication scheme, Computer Communications 32 (2009) 583{585.
3. C. S. Tsai, C. C. Lee, M. S. Hwang, Password authentication schemes: Current status and key issues, in: International Journal of Network Security, Vol. 3, IEEE, 2006, pp. 101{115. doi:10.1109/ICM2CS. 2009.5397977.URL http://ieeexplore .ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5397977
4. L. Lamport, Password authentication with insecure communication, Communications of the ACM 24 (11) (1981) 770{772. doi:10.1145/358790.358797. URLhttp:// portal.acm.org/ citation.cfm? doid= 358790.358797

5. P. G.M.J, J. van Leeuwen, Authentication : A Concise Survey, Computers & Security 5 (1986) 243{250. doi:0167 4048/86.
6. H.-M. Sun, An eficient remote use authentication scheme using smart cards (2000). doi:10.1109/30.920446.
7. M. Kumar, New remote user authentication scheme using smart cards, in: IEEE Transactions on Consumer Electronics, Vol. 50, 2004, pp. 597{600. doi:10.1109/TCE.2004.1309433.
8. M. Das, V. Gulati, A. Saxena, A dynamic id-based remote user authentication scheme, IEEE Transactions on Consumer Electronics 50 (2) (2004) 629{631.arXiv:0410011,doi:10.1109/TCE.2004.1309441.
9. S.-W. Lee, H.-S. Kim, K.-Y. Yoo, Improvement of Chien et al.'s remote user authentication scheme using smart cards, Computer Standards & Interfaces27(2)(2005)doi:http://dx.doi.org/10.1016/j.csi.2004.02.002.URLhttp://www.sciencedirect.com/science/ article /pii/ S0920548904000170
10. Z.-Y. Wu, Y. Chung, F. Lai, T.-S. Chen, A Password-Based User Authentication Scheme for the Integrated EPR Information System, Journal of Medical Systems 36 (2) (2012) 631{638. doi:10.1007/s10916-010-9527-7.URL http://link.springer.com/ 10.1007/s10916-010-9527-7
11. C. C. Chang, S. J. Hwang, Cryptographic authentication of passwords, in: Security Technology, 1991. Proceedings. 25th Annual 1991 IEEE International Carnahan Conference on, 1991, pp. 126{130. doi:10.1109/CCST.1991.202203.
12. S.-M. Yen, Security of a one-time signature, Electronics Letters 33 (8) (1997) 677{679. doi:10.1049/el:19970460.
13. Y. Lee, H. Yang, D. Won, Attacking and Improving on Lee and Chiu ' s Authentication Scheme Using Smart Cards, Springer Berlin Heidelberg, Berlin, Heidelberg, 2010, Ch. Attacking, pp. 377{385.
14. Y.-C. Lee, Narn-Yih; Chiu, Improved remote authentication scheme with smart card, Computer Standards and Interfaces 27 (2) (2005) 177{180.
15. Y.-P. Liao, S.-S. Wang, A secure dynamic ID based remote user authentication scheme for multi-server environment, Computer Standards & Interfaces 31 (1)(2009) 24{29. doi:10.1016/j.csi.2007.10.007. URL http://dx.doi.org/10.1016/j.csi.2007.10.007http://linkinghub.elsevier.com/retrieve/pii/S09205489070010 3

This page is intentionally left blank

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 16 Issue 4 Version 1.0 Year 2016
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Energy Efficient Multicast Routing in Mobile Ad Hoc Networks: Contemporary Affirmation of Benchmarking Models in Recent Literature

By SK. Nagula Meera, D. Srinivasa Kumar & D. Srinivasa Rao
JNTU-Hyderabad

Abstract- The Mobile Ad hoc Networks playing critical role in network aided communication requirements. The features such as ad hoc and open architecture based connectivity and node mobility are elevating the mobile ad hoc networks as much as feasible to deploy and use. The direct communication between any of two nodes in this network is possible if target node is in the range of source node. If not, the indirect communication took place, which is usually referred as multi hop routing. The multi hop routing occurs as either a unicast model (one source node to one destination node), multicast model (one source node to multiple destination nodes) or multiple casting (manifold unicast routing). In these routing strategies, provision of service quality in multi hop routing is a challenging task. The optimal quality of service in routing, magnifies the delivery ratio, transmission rate, network life span and other expected characteristics of the ad hoc routing. Among the quality service provision factors minimal energy conservation is prime factor, which is since the nodes involved in routing are self-energized and if discharged early then the route will be destructed that causes discontinued routing. The energy consumption is more specific in multicast routing, hence it is grabbing the more attention of the current research contributions.

Keywords: multicast routing protocols, mobile ad hoc network (manet), energy efficient routing. tree based multicast route, mesh based multicast route, zone based multicast route, hybrid multicast route, residual energy.

GJCST-E Classification : C.2.1 C.2.2 C.2.3

Strictly as per the compliance and regulations of:

Energy Efficient Multicast Routing in Mobile Ad Hoc Networks: Contemporary Affirmation of Benchmarking Models in Recent Literature

SK. Nagula Meera [α], D. Srinivasa Kumar [σ] & D. Srinivasa Rao [ρ]

Abstract -The Mobile Ad hoc Networks playing critical role in network aided communication requirements. The features such as ad hoc and open architecture based connectivity and node mobility are elevating the mobile ad hoc networks as much as feasible to deploy and use. The direct communication between any of two nodes in this network is possible if target node is in the range of source node. If not, the indirect communication took place, which is usually referred as multi hop routing. The multi hop routing occurs as either a unicast model (one source node to one destination node), multicast model (one source node to multiple destination nodes) or multiple casting (manifold unicast routing). In these routing strategies, provision of service quality in multi hop routing is a challenging task. The optimal quality of service in routing, magnifies the delivery ratio, transmission rate, network life span and other expected characteristics of the ad hoc routing. Among the quality service provision factors minimal energy conservation is prime factor, which is since the nodes involved in routing are self-energized and if discharged early then the route will be destructed that causes discontinued routing. The energy consumption is more specific in multicast routing, hence it is grabbing the more attention of the current research contributions. In this regard this manuscript reviewed the contemporary literature and the significant contributions of energy efficient multicast routing strategies.

Keywords: multicast routing protocols, mobile ad hoc network (manet), energy efficient routing. tree based multicast route, mesh based multicast route, zone based multicast route, hybrid multicast route, residual energy.

I. Introduction

Mobile ad hoc networks (MANET) [1] is one of the critical class of network aided distributed communication. The features such as dynamic connectivity,less infrastructure ability of node mobility enables to establish network aided communication in civilian environments such as army communication in battle grounds, natural calamities handling and social media sharing between hand held and mobile devices. The direct communication between any devices of the MANET is possible only if receiver is in the range of sender. If receiver is not in the range of the sender, then the route can be established between sender and receiver by using the intermediate devices called nodes. The phenomenal growth in computer aided network communication demands instant access to any network in order to exchange digital data. The video conferences, digital data sharing between students in academic strategies, service search and information sharing in business enterprises and social media are the few examples to justify the demand of ad hoc network strategies. The constraints such as indefinite node density of a network, unpredictable mobility of the nodes, and other operational factors of a node such as egress and ingress capacity, residual energy levels compromised behavior of the nodesevincing that intermediate nodes selection to establish route between source and destination is a challenging task. Though the many contributions found in contemporary literature to establish optimal routes, they limited to one or two quality factors. Hence the quality provisioning in route discovery is still an open issue for current research domain. Multicasting is significantly sensitive to discover optimal routes, which since the load of transmission is significantly high and often intermediate nodes are necessarily transmit data to multiple nodes in order to transmit data to multiple target nodes. Hence the node life span is most critical to retain the multicast route to complete data transmission between one source to many destination nodes. Hence, this manuscript reviewed contemporary literature on energy efficient multicast routing strategies.

The paper is organized as follows. Section 2 describes nomenclature of the multicast routing strategies. Section 3 is the contemporary affirmation of the benchmarking energy efficient multicast routing models fund in recent literature. Section 4summarizing the manuscript contributions.

II. Nomenclature of the Multicast Routing Strategies

The categorization of the multicasting routing strategies are usually based on the topologies such as tree, mesh, zone and hybrid topologies are used to build multicast routes. Further these multicast routing models under divergent topologies are categorized

Author α: Research Scholar, Dept., of ECE, JNTU, Hyderabad, Telangana State, India. e-mail: nag.meera@gmail.com
Author σ: Professor & Principal, Hosur Institute of Technology & Science Beerpalli, Krishnagiri Dist, Tamilnadu.
Author ρ: Professor, Dept., of ECE, College of Engineering, JNTU, Hyderabad, Telangana State, India.

based on service provision strategies such as reliability, bandwidth usage, delay, bandwidth delay and power aware or energy efficient.

The tree based multicast routing protocols of these categories are subcategorized as source-rooted and core-rooted schemes according to the roots of the multicast trees. The source node acts as root node of the tree and maintains the topology related information and addresses of all nodes involved in multicast route, hence the model is evincing the constraints such as process, route maintenance and traffic overheads. The other category of tree based multicast routing models are core-rooted models, which is the set of subtrees and each sub tree behaves as source rooted trees. Each subtree is formed by a node involving multicasting as root node. The core-root tree based multicast routing strategies are optimal than source-root tree based multicast routing strategies but route stability is a questionable factor. Though the tree based multicast models are is establish but frequent destruction of the route due to node mobility is quite often that abandons the data transmission till the reformation of the tree happens.

The sub categories of the mesh based multicast routing models are also based on either core or central nodes, which are as similar as source and core root based multicast trees. But mesh based multicast routing models are node mobility resistant. Hence the route destruction due to node mobility is least significant in mesh based ulticast routing models.

The multicast models of the zone based topology partitions the network region as virtual zones. Further the nodes of each zone are used to core-root tree or core-point mesh. The node that considered as core-root or core-point is the zone head. The inter zone communication is done through the zone heads. The considerable advantage of the zone based multicasting models is, the node mobility needn't be tracked, instead, notifying zone change of the node is sufficient. The visible constraints of these zone based multicasting are overhead of zone formation, route discovery and route maintenance.

The hybrid models of multicast routing protocols are the combination of either all of tree, mesh and zone topologies or any of two.

The other considerable category of multicast routing protocols are hierarchical models. This category is often fall under hybrid models. This multicast routing protocols are set of connected multicast routing protocols of one or more of the types called tree, mesh and zone based topologies. The constraints specific to these topologies can be evinced even in hierarchical models.

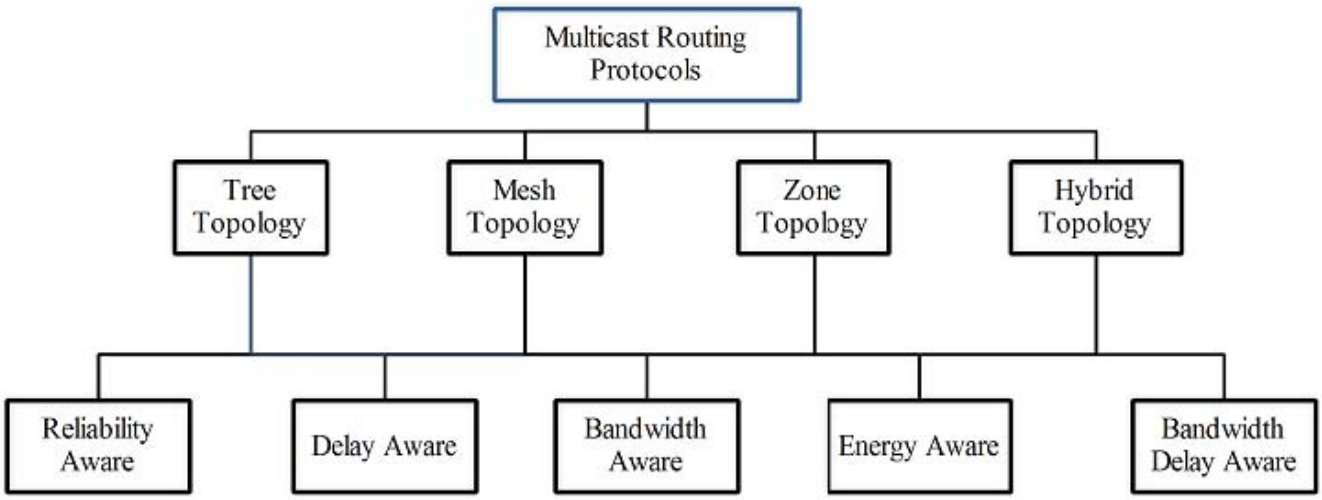

Figure 1 : Nomenclature of the multicast routing strategies for mobile ad hoc networks

The classification of the multicast routing strategies based on the tree, mesh, zone and hybrid topologies explores issues in multicast routing specific to reliability, delay, bandwidth usage, bandwidth delay, link stability and energy usage.

The context of this manuscript is reviewing energy efficient multicast routing protocols, hence the benchmarking energy efficient multicast routing protocols that fall in either of the category explored and found in contemporary literature are informed in detail in following section.

III. Contemporary Affirmation of Benchmarking QoS Multicast Routing Protocols

This section explores the some of the benchmarking energy efficient multicast routing models found in contemporary literature.

The minimum energy-per-bit for multicasting Wu et al., [2] defined a coding aware multicasting with minimal energy consumption. The objective of the

model is to minimize bit level energy consumption. In regrad to this network coding is adapted to in multicast routing. The empirical analysis of the model claimed the significance of the network coding to achieve bit level energy consumption to be minimal and construction of multicast tree that consumes overall energy as much as low. The considerable constraint is that if transmission distance increased between nodes then the energy consumption is complemented and often route destruction evinced if noise found during transmission.

Guo et al., [3] proposed an energy efficient multicast routing model for Wireless ad hoc networks with Omni antenna based neighbor node communication strategy. In case of source initiated multicast traffic, power saving capability achieved through the usage of adaptive antennas. In order to select nodes those transmit data as radio frequency with minimal usage of the energy, the mixed integer linear programming (MILP) is adapted here in this model. The experimental study noticed that, this model is highly adaptable only for low and midsize networks to achieve minimal energy consumption. The constraints observed for the model [2] even found in this model.

A distributed minimum energy multicast model [4] proposed for mobile ad hoc networks with nodes using Omni directional antennas. The objective of the proposal is to minimize the energy usage for radio frequency transmission. In order to build an energy efficient multicasting tree, this model is considering the factors such as managing distinct levels of energy usage, balancing the flooding in multicast tree and multicasting tree maintenance. The overall routing process is in two dimensions and those are achieving minimal energy consumption and continuous reformation of the multicast tree to avoid the route failure due to node mobility. The energy consumption in regard to radio frequency (RF) transmission is estimated by the distance between source and destination Omni directional antennas. The experimental study indicating that the model is out performed in Manets with low mobility nodes. The significant constraint of the model is that it is not considering the route lifespan (residual energy is not assessing), which causes often route destruction, also not considering the signal to noise ratio, hence the energy saving is not optimal if noise found in RF transmission medium.

Li et al., [5] proposed an Energy efficient multicast routing in ad hoc wireless networks that equipped with Node-Join-Tree, Tree-Join-Tree and directed Steiner tree based multicast tree building algorithms. An approximation algorithm is used to overcome the NP-Hard problem of the multicast tree formation [6]. The greedy approaches NJT (Node-Join-Tree) and TJT (Tree-Join-Tree) are used to perform optimal node joins to build multiple sub trees and optimal sub tree joins to build multicast tree respectively. Each neighbor node verification and each sub tree verification are the critical computational constraints observed in NJT and TJT respectively. In order to overcome this Steiner tree method is used to achieve greediness in node verification and subtree verification in respective NJT and TJT. The empirical study evincing optimal performance of this model in Manets with nodes with less transmission distance between them. The constraints noticed for models [2][3] are noticed even for this model.

Gua et al., [7] extended their earlier contributions [3][4] with basic energy-efficient multicast (BEEM) and distributed maximum lifetime multicast (DMLM), for increasing the lifetime of the network. Distinct energy usage scheme is adopted from [4], and node location identification is done by positioning system. The experimental study compared the performance of BEEM, DMLM and ODMRP in the context of maximal lifespan of the network. The comparison evinced that DMLM increased the network lifespan through minimal energy usage that compared to BEEM and ODMRP and the network lifespan observed under BEEM is much better than the ODMRP. The computational and process control overhead also found high in the order of DMLM, BEEM and ODMRP, which is considerable constraint of the proposal.

Shafigh et al., [8] proposed a mesh based multicast routing that selects nodes based on their residual energy. In order to this the proposed model is using fuzzy reasoning to segregate nodes with low residual energy and high residual energy. The proposed models is on demand multicasting model that uses fuzzy reasoning to select optimal nodes in order to build mesh based multicast route. The fitness function of the fuzzy logic is assessing the residual energy levels of the nodes capable to involve in route establishment. The empirical study compared the values obtained for metrics (such as PDR, control overhead, end-to-end delay) with the values obtained for ODMRP, which are evincing the phenomenal advantage of this model over ODMRP. The constraints observed are downfall in packet delivery ratio and energy usage is complimented against increase in control packet transmission, which is specific to dense networks.

Xiang et al. [9] proposed a multicast routing protocol, which is labeled as efficient geographic multicast protocol. This protocol builds zone based bidirectional multicast tree that dilutes the complexity of route discovery and maintenance. In order to this the overall network range is partitioned into virtual zones such that direct communication between any two nodes in a zone is possible. Each zone is equipped with a zone head and if node want to communicate to a node that exists in other zone then the source node seeks zone head role in order. Since the data transmission is zone level but node level, hence route maintenance is phenomenally very low, since the protocol rather monitoring the node mobility, it handles the zone

change of the nodes due to their mobility. The transmission over head is shared between all member nodes of the zone, hence transmission overhead also be found very low. The empirical study that compared PDR, control overhead and delay observed for this protocol with other benchmarking model called ODMRP and SPBM [10]. The empirical study results evincing that this model performance is optimal than other two. The minimal energy consumption and maximal residual energy are not considered to select a zone based multicast tree, which is a significant constraint to achieve maximum network lifespan.

Tavli et al., [11] devised a cross layer architecture based protocol for multicasting with minimal energy consumption, which is using time reservation strategy in multicasting. This protocol also balancing the other QoS factors that includes spatial reuse. This architecture used in this protocol is the combination of multicast mesh and multicast tree structures, where the multicast tree is active and that surrounded by the passive multicast mesh. The passive multicast mesh helps to handle the broken links in active multicast tree efficiently. This protocol is an extension to the earlier model called multi hop time reservation using adaptive control for energy efficiency [12]. This model switches idle nodes to sleep mode and also surpasses the recurrent data transmissions in order to achieve minimal energy conservation. The experimental study evincing the minimal energy consumption and delay that compared to other benchmarking model called ODMRP [13]. The considerable constraint this model is complex cross layer architecture.

Fareena et al [14] proposed a multicast routing model that limiting the overall energy consumption by selecting nodes based on their mobility speed and direction. This is a cross model of mesh and tree architectures. The density of neighbor count also considered in order to select nodes for multicast route building. The metrics node mobility speed and direction, neighbor count and residual energy of each node are used as critical factors by this model to devise energy efficient multicast route. Switching the idle nodes into sleep state is also boosting this model to minimize the energy consumption. The empirical study signifies that the model is optimal as the packet delivery ratio is high, energy consumption and end-to-end delay is low that compared to the ODMRP. The constraints are, control flow overhead and process overhead. The overall energy consumption observed for data packets and control packets transmission is not optimal.

Nasab et al. [15] proposed a multicast routing strategy to achieve minimum energy consumption. The devised model is using PSO (particle swarm optimization) [16] technique to discover the route with maximum residual energy, minimal energy consumption and end-to-end delay. The initial multicast tree that includes all nodes in the network is built by prims algorithm and further optimal multicast tree is discovered by applying PSO. The nodes involved in initial tree are considered as particles with the properties called mobility speed, position and direction of mobility. The PSO traverse these particles in order to select qualified particles. Further the optimal nodes are being selected from these qualified nodes through the fitness function, which is assessing the node fitness by their residual energy levels, energy consumption ratio. The experimental study evinced that the PSO model is the best fit model to derive energy efficient multicast tree that compared to traditional GA approach. The computational overhead observed for PSO is considerable constraint of the model, which is also lagging to achieve energy efficiency in noisy channels (signal to noise ratio is low in discovered multicast tree).
Varaprasad et al., [17] proposed a multicasting protocol that aimed to achieve maximum link stability and minimal energy consumption. Tis proposed model relied on two factors called residual energy of the battery and maximal relay scope. The establishment of route with the nodes having high residual energy and high relay capacity evinced reliable communication. This model is not considering the minimizing the energy consumption to enhance the network life span, which is found to be critical constraint of this model and other constraint is process load due to additional control traffic.

Lu et al., [18] proposed a multicast routing model, which is to achieve minimal energy consumption and minimal end-to-end delay. The route discovery strategy is an evolutionary model that uses genetic algorithm in route selection. In order to obtain the optimal multicast tree path, the proposed model is applying genetic evolutions on possible multicast trees discovered in route request phase. The cost function estimating the energy consumption ratio and end-to-end delay in order to notify the fitness of the resultant multicast trees of the GA crossovers. The empirical study of the model evinced the discovery of optimal multicast tree with minimal energy consumption and least end-to-end delay. The critical constraint of the proposal is computation overhead, since the genetic algorithm process complexity is not linear, hence the process complexity is complimented if network size is increased. The other constraint of the model is, it is not considering the overall multicast tree lifespan as a factor route selection.

The review of contemporary multicast routing with minimal energy consumption and maximal network lifespan models was done here in this section. The review evincing that the all of these models are found to be fit under the specific factors considered. All of these models are divergent at multicast route discovery process in order to achieve minimal energy consumption and maximal network lifespan. The common constraints of these models observed is limiting the performance if transmission influenced by

noise, computational overhead observed in route discovery phase and process overhead observed at route maintenance phase.

IV. Conclusion

This manuscript reviewed the energy efficient multicast routing strategies found in recent literature. The review evinced the context of the multicast routing protocols and the strategies followed in order to achieve energy efficient transmission and limits. The multicast routing models reviewed were fall in either of the routing topologies called tree, mesh, zone and hybrid topology, but common objective of all these protocols is multicast routing under minimal energy consumption and maximal network lifespan. The review of these models reveal that scalability issues such as compatibility to dense networks, nodes with high mobility and transmissions under noise in fluencesare not considered by most of the approaches. The assessment of the performance of all these models are at limited extent of QoS factors and heterogeneous factors of mobile ad hoc networks such as all-to-all multicast routing, many-to-many multicast routing and multiple unicast routing. Hence it is obvious to notify that a vast research scope to devise energy efficient multicast routing protocols.

References Références Referencias

1. Conti, M., & Giordano, S. (2014). Mobile ad hoc networking: milestones, challenges, and new research directions. Communications Magazine, IEEE,52(1), 85-96.
2. Wu, Y., Chou, P.A. and Kung, S-Y. (2005) 'Minimum-energy multicast in mobile ad hoc networks using network coding', IEEE Transactions on Communications, Vol. 53, No. 11, pp.1906–1918.
3. Guo, S. and Yang, O. (2006) 'Minimum-energy multicast in wireless ad hoc networks with adaptive antennas: MILP formulations and heuristic algorithms', IEEE Transactions on Mobile Computing, Vol. 5, No. 4, pp.333–346.
4. Guo, S. and Yang, O. (2007) 'Localized operations for distributed minimum energy multicast algorithm in mobile ad hoc networks', IEEE Transactions on Parallel and Distributed Systems, Vol. 18, No. 2, pp.186–198.
5. Li, D., Liu, Q., Hu, X. and Jia, X. (2007) 'Energy efficient multicast routing in ad hoc wireless networks', Science Direct, Computer Communications, Vol. 30, No. 18, pp.3746–3756.
6. Cagalj, M., Hubaux, J-P. andEnz, C. (2002) 'Minimum-energy broadcast in all-wireless networks: NP-completeness and distribution issues', Proc. ACM MobiCom, pp.172–182.
7. Guo, S. and Yang, O. (2008) 'Maximizing multicast communication lifetime in wireless mobile ad hoc networks', IEEE Transactions on Vehicular Technology, Vol. 57, No. 4, pp.2414–2425.
8. Shafigh, A.S., Abdollahi, K. and Kassler, A.J. (2010) 'Improving performance of on demand multicast routing by using fuzzy logic', IEEE International Conference on Wireless Communications, Networking and Information Security (WCNIS), pp.525–529.
9. Xiang, X., Wang, X. and Yang, Y. (2011) 'Supporting efficient and scalable multicasting over mobile ad hoc networks', IEEE Transactions on Mobile Computing, Vol. 10, No. 5, pp.544–559.
10. Transier, M., Füßler, H., Widmer, J., Mauve, M., &Effelsberg, W. (2007). A hierarchical approach to position-based multicast for mobile ad-hoc networks. Wireless Networks, 13(4), 447-460.
11. Tavli, B. and Heinzelman, W.B. (2011) 'Energy-efficient real-time multicast routing in mobile ad hoc networks', IEEE Transactions on Computers, Vol. 60, No. 5, pp.707–722. Transier, M., Fubler, H., Widmer, J., Mauve, M. and Effelsberg, W. (2007) 'A hierarchical approach to position-based multicast for mobile ad-hoc networks', Wireless Networks, Vol. 13, No. 4, pp.447–460.
12. Tavli, B. and Heinzelman, W. (2004) 'MH-TRACE: multi hop time reservation using adaptive control for energy efficiency', IEEE J. Selected Areas Comm., Vol. 22, No. 5, pp.942–953.
13. Lee, S.J., Su, W. and Gerla, M. (2002) 'On-demand multicast routing protocol in multihop wireless mobile networks', Mobile Networks and Applications, Vol. 7, No. 6, pp.441–453.
14. Fareena, N., ShunmugaPriya Mala, A. and Ramarca, K. (2012) 'Mobility based energy efficient multicast protocol for MANET', Proc. International Conference on Modelling Optimization and Computing, Vol. 38, pp.2473–2483.
15. Nasab, A.S., Derhami, V., Khanli, L.M. and Bidoki, A.M.Z. (2012) 'Energy-aware multicast routing in MANET based on particle swarm optimization', First World Conference on Innovation and Computer Sciences (INSODE 2011), Vol. 1, pp.434–438.
16. Eberhart, R.C. and Kennedy, J. (1995.) 'A new optimizer using particle swarm theory', IEEE 6th Symposium Micro Machine and Human Science.
17. Varaprasad, G. (2013) 'High stable power aware multicast algorithm for mobile ad hoc networks', IEEE Sensors Journal, Vol. 13, No. 5, pp.1442–1446.
18. Lu, T. and Zhu, J. (2013) 'Genetic algorithm for energy-efficient QoS multicast routing', IEEE Communications Letters, Vol. 17, No. 1, pp.31–34.
19. An and, J. and Srinath, D. (2009) 'Performance analysis of shared tree based multicast routing protocols for ad-hoc wireless networks',

International Journal of Engineering and Technology, Vol. 2, No. 1, pp.78–91.
20. Corson, M.S. and Macker, J. (1999) 'Mobile ad hoc networking (MANET): routing protocol performance issues and evaluation considerations', Internet Engineering Task Force, pp.1–12.
21. Diot, C., Dabbous, W. and Crowcroft, J. (1997) 'Multipoint communication: a survey of protocols, functions, and mechanisms', IEEE Journal on Selected Areas in Communications, Vol. 15, No. 3, pp.277–290.
22. Gossain, H., Cordeiro, C.D.M. and Agrawal, D.P. (2003) 'Multicast over wireless mobile ad hoc networks: present and future directions', IEEE Network, Vol. 17, No. 1, pp.52–59.
23. Guo, S. and Yang, O. (2004) 'Multicast lifetime maximization for energy-constrained wireless ad hoc networks with directional antennas', Proc. IEEE Globecom Conf., pp.4120–4124.
24. Ho, T., Medard, M., Effros, M. and Karger, D. (2003) 'On randomized network coding', Proc. 41st Allerton Annual Conference on Communication, Control and Computing.
25. Kamboj, P. and Sharma, A.K. (2010) 'Energy efficient multicast routing protocol for MANET with minimum control overhead (EEMPMO)', International Journal of Computer Applications, Vol. 8, No. 7, pp.1–11.
26. Klein, P.N. and Ravi, R. (1995) 'A nearly best-possible approximation algorithm for node-weighted Steiner trees', Journal of Algorithms, Vol. 19, No. 1, pp.104–114.
27. Lee, S.J., Su, W., Hsu, J., Gerla, M. and Bagrodia, R. (2000) 'A performance comparison study of ad hoc wireless multicast protocols', Proc. IEEE INFOCOM, Vol. 2, pp.565–574.
28. Liang, W. (2006) 'Approximate minimum-energy multicasting in wireless ad hoc networks', IEEE Transactions on Mobile Computing, Vol. 5, No. 4, pp.377–387.
29. Liang, W., Brent, R., Xu, Y. and Wang, Q. (2009) 'Minimum-energy all-to-all multicasting in wireless ad hoc networks', IEEE Transactions on Wireless Communications, Vol. 8, No. 11, pp.5490–5499.
30. Murthy, C.S.R. and Manoj, B.S. (2004) Ad Hoc Wireless Networks: Architectures and Protocols, 1st ed., Prentice Hall PTR, Upper Saddle River, NJ, USA.
31. Subramani, M. and Kuppusamy, S. (2011) 'Improving congestion control performance and fairness in multihop ad hoc network', International Journal of Networking and Virtual Organisations, Inderscience Publishers, Vol. 9, No. 1, pp.86–101.
32. Wang, B. and Gupta, S. K. S. (2003) 'On maximizing lifetime of multicast trees in wireless ad hoc networks', Proc. Int. Conf. Parallel Process., Kaohsiung, Taiwan, R.O.C., pp.333–340.
Wieselthier, J.E., Nguyen, G.D. and Ephremides, A. (2002a) 'Energy-limited wireless networking with directional antennas: the case of session-based multicasting', Proc. IEEE Infocom Conference., pp.190–199.
33. Wieselthier, J.E., Nguyen, G.D. and Ephremides, A. (2002b) 'Energy-aware wireless networking with directional antennas: the case of session-based broadcasting and multicasting', IEEE Trans. Mobile Computing, Vol. 1, No. 3, pp.176–191.
34. Zhang, J., Fan, P. and Letaief, K.B. (2008) 'Network coding for efficient multicast routing in wireless ad-hoc networks', IEEE Transactions on Communications, Vol. 56, No. 4, pp.598–607.

Global Journals Inc. (US) Guidelines Handbook 2016

www.GlobalJournals.org

FELLOW OF ASSOCIATION OF RESEARCH SOCIETY IN COMPUTING (FARSC)

Global Journals Incorporate (USA) is accredited by Open Association of Research Society (OARS), U.S.A and in turn, awards "FARSC" title to individuals. The 'FARSC' title is accorded to a selected professional after the approval of the Editor-in-Chief/Editorial Board Members/Dean.

- The "FARSC" is a dignified title which is accorded to a person's name viz. Dr. John E. Hall, Ph.D., FARSC or William Walldroff, M.S., FARSC.

FARSC accrediting is an honor. It authenticates your research activities. After recognition as FARSC, you can add 'FARSC' title with your name as you use this recognition as additional suffix to your status. This will definitely enhance and add more value and repute to your name. You may use it on your professional Counseling Materials such as CV, Resume, and Visiting Card etc.

The following benefits can be availed by you only for next three years from the date of certification:

FARSC designated members are entitled to avail a 40% discount while publishing their research papers (of a single author) with Global Journals Incorporation (USA), if the same is accepted by Editorial Board/Peer Reviewers. If you are a main author or co-author in case of multiple authors, you will be entitled to avail discount of 10%.

Once FARSC title is accorded, the Fellow is authorized to organize a symposium/seminar/conference on behalf of Global Journal Incorporation (USA).The Fellow can also participate in conference/seminar/symposium organized by another institution as representative of Global Journal. In both the cases, it is mandatory for him to discuss with us and obtain our consent.

You may join as member of the Editorial Board of Global Journals Incorporation (USA) after successful completion of three years as Fellow and as Peer Reviewer. In addition, it is also desirable that you should organize seminar/symposium/conference at least once.

We shall provide you intimation regarding launching of e-version of journal of your stream time to time. This may be utilized in your library for the enrichment of knowledge of your students as well as it can also be helpful for the concerned faculty members.

The FARSC can go through standards of OARS. You can also play vital role if you have any suggestions so that proper amendment can take place to improve the same for the benefit of entire research community.

As FARSC, you will be given a renowned, secure and free professional email address with 100 GB of space e.g. johnhall@globaljournals.org. This will include Webmail, Spam Assassin, Email Forwarders, Auto-Responders, Email Delivery Route tracing, etc.

The FARSC will be eligible for a free application of standardization of their researches. Standardization of research will be subject to acceptability within stipulated norms as the next step after publishing in a journal. We shall depute a team of specialized research professionals who will render their services for elevating your researches to next higher level, which is worldwide open standardization.

The FARSC member can apply for grading and certification of standards of their educational and Institutional Degrees to Open Association of Research, Society U.S.A. Once you are designated as FARSC, you may send us a scanned copy of all of your credentials. OARS will verify, grade and certify them. This will be based on your academic records, quality of research papers published by you, and some more criteria. After certification of all your credentials by OARS, they will be published on your Fellow Profile link on website https://associationofresearch.org which will be helpful to upgrade the dignity.

The FARSC members can avail the benefits of free research podcasting in Global Research Radio with their research documents. After publishing the work, (including published elsewhere worldwide with proper authorization) you can upload your research paper with your recorded voice or you can utilize chargeable services of our professional RJs to record your paper in their voice on request.

The FARSC member also entitled to get the benefits of free research podcasting of their research documents through video clips. We can also streamline your conference videos and display your slides/ online slides and online research video clips at reasonable charges, on request.

The FARSC is eligible to earn from sales proceeds of his/her researches/reference/review Books or literature, while publishing with Global Journals. The FARSC can decide whether he/she would like to publish his/her research in a closed manner. In this case, whenever readers purchase that individual research paper for reading, maximum 60% of its profit earned as royalty by Global Journals, will be credited to his/her bank account. The entire entitled amount will be credited to his/her bank account exceeding limit of minimum fixed balance. There is no minimum time limit for collection. The FARSC member can decide its price and we can help in making the right decision.

The FARSC member is eligible to join as a paid peer reviewer at Global Journals Incorporation (USA) and can get remuneration of 15% of author fees, taken from the author of a respective paper. After reviewing 5 or more papers you can request to transfer the amount to your bank account.

MEMBER OF ASSOCIATION OF RESEARCH SOCIETY IN COMPUTING (MARSC)

The ' MARSC ' title is accorded to a selected professional after the approval of the Editor-in-Chief / Editorial Board Members/Dean.
The “MARSC” is a dignified ornament which is accorded to a person’s name viz. Dr. John E. Hall, Ph.D., MARSC or William Walldroff, M.S., MARSC.

MARSC accrediting is an honor. It authenticates your research activities. After becoming MARSC, you can add 'MARSC' title with your name as you use this recognition as additional suffix to your status. This will definitely enhance and add more value and repute to your name. You may use it on your professional Counseling Materials such as CV, Resume, Visiting Card and Name Plate etc.

The following benefitscan be availed by you only for next three years from the date of certification.

MARSC designated members are entitled to avail a 25% discount while publishing their research papers (of a single author) in Global Journals Inc., if the same is accepted by our Editorial Board and Peer Reviewers. If you are a main author or co-author of a group of authors, you will get discount of 10%.

As MARSC, you will be given a renowned, secure and free professional email address with 30 GB of space e.g. johnhall@globaljournals.org. This will include Webmail, Spam Assassin, Email Forwarders, Auto-Responders, Email Delivery Route tracing, etc.

We shall provide you intimation regarding launching of e-version of journal of your stream time to time. This may be utilized in your library for the enrichment of knowledge of your students as well as it can also be helpful for the concerned faculty members.

The MARSC member can apply for approval, grading and certification of standards of their educational and Institutional Degrees to Open Association of Research, Society U.S.A.

Once you are designated as MARSC, you may send us a scanned copy of all of your credentials. OARS will verify, grade and certify them. This will be based on your academic records, quality of research papers published by you, and some more criteria.

It is mandatory to read all terms and conditions carefully.

AUXILIARY MEMBERSHIPS

Institutional Fellow of Open Association of Research Society (USA)-OARS (USA)

Global Journals Incorporation (USA) is accredited by Open Association of Research Society, U.S.A (OARS) and in turn, affiliates research institutions as "Institutional Fellow of Open Association of Research Society" (IFOARS).

The "FARSC" is a dignified title which is accorded to a person's name viz. Dr. John E. Hall, Ph.D., FARSC or William Walldroff, M.S., FARSC.

The IFOARS institution is entitled to form a Board comprised of one Chairperson and three to five board members preferably from different streams. The Board will be recognized as "Institutional Board of Open Association of Research Society"-(IBOARS).

The Institute will be entitled to following benefits:

The IBOARS can initially review research papers of their institute and recommend them to publish with respective journal of Global Journals. It can also review the papers of other institutions after obtaining our consent. The second review will be done by peer reviewer of Global Journals Incorporation (USA) The Board is at liberty to appoint a peer reviewer with the approval of chairperson after consulting us.

The author fees of such paper may be waived off up to 40%.

The Global Journals Incorporation (USA) at its discretion can also refer double blind peer reviewed paper at their end to the board for the verification and to get recommendation for final stage of acceptance of publication.

The IBOARS can organize symposium/seminar/conference in their country on behalf of Global Journals Incorporation (USA)-OARS (USA). The terms and conditions can be discussed separately.

The Board can also play vital role by exploring and giving valuable suggestions regarding the Standards of "Open Association of Research Society, U.S.A (OARS)" so that proper amendment can take place for the benefit of entire research community. We shall provide details of particular standard only on receipt of request from the Board.

The board members can also join us as Individual Fellow with 40% discount on total fees applicable to Individual Fellow. They will be entitled to avail all the benefits as declared. Please visit Individual Fellow-sub menu of GlobalJournals.org to have more relevant details.

We shall provide you intimation regarding launching of e-version of journal of your stream time to time. This may be utilized in your library for the enrichment of knowledge of your students as well as it can also be helpful for the concerned faculty members.

After nomination of your institution as "Institutional Fellow" and constantly functioning successfully for one year, we can consider giving recognition to your institute to function as Regional/Zonal office on our behalf.
The board can also take up the additional allied activities for betterment after our consultation.

The following entitlements are applicable to individual Fellows:

Open Association of Research Society, U.S.A (OARS) By-laws states that an individual Fellow may use the designations as applicable, or the corresponding initials. The Credentials of individual Fellow and Associate designations signify that the individual has gained knowledge of the fundamental concepts. One is magnanimous and proficient in an expertise course covering the professional code of conduct, and follows recognized standards of practice.

Open Association of Research Society (US)/ Global Journals Incorporation (USA), as described in Corporate Statements, are educational, research publishing and professional membership organizations. Achieving our individual Fellow or Associate status is based mainly on meeting stated educational research requirements.

Disbursement of 40% Royalty earned through Global Journals : Researcher = 50%, Peer Reviewer = 37.50%, Institution = 12.50% E.g. Out of 40%, the 20% benefit should be passed on to researcher, 15 % benefit towards remuneration should be given to a reviewer and remaining 5% is to be retained by the institution.

We shall provide print version of 12 issues of any three journals [as per your requirement] out of our 38 journals worth $ 2376 USD.

Other:

The individual Fellow and Associate designations accredited by Open Association of Research Society (US) credentials signify guarantees following achievements:

- The professional accredited with Fellow honor, is entitled to various benefits viz. name, fame, honor, regular flow of income, secured bright future, social status etc.

- In addition to above, if one is single author, then entitled to 40% discount on publishing research paper and can get 10%discount if one is co-author or main author among group of authors.
- The Fellow can organize symposium/seminar/conference on behalf of Global Journals Incorporation (USA) and he/she can also attend the same organized by other institutes on behalf of Global Journals.
- The Fellow can become member of Editorial Board Member after completing 3yrs.
- The Fellow can earn 60% of sales proceeds from the sale of reference/review books/literature/publishing of research paper.
- Fellow can also join as paid peer reviewer and earn 15% remuneration of author charges and can also get an opportunity to join as member of the Editorial Board of Global Journals Incorporation (USA)
- • This individual has learned the basic methods of applying those concepts and techniques to common challenging situations. This individual has further demonstrated an in–depth understanding of the application of suitable techniques to a particular area of research practice.

Note :

"

- In future, if the board feels the necessity to change any board member, the same can be done with the consent of the chairperson along with anyone board member without our approval.
- In case, the chairperson needs to be replaced then consent of 2/3rd board members are required and they are also required to jointly pass the resolution copy of which should be sent to us. In such case, it will be compulsory to obtain our approval before replacement.
- In case of "Difference of Opinion [if any]" among the Board members, our decision will be final and binding to everyone.

"

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 .

You must strictly follow above Author Guidelines before submitting your paper or else we will not at all be responsible for any corrections in future in any of the way.

Before start writing a good quality Computer Science Research Paper, let us first understand what is Computer Science Research Paper? So, Computer Science Research Paper is the paper which is written by professionals or scientists who are associated to Computer Science and Information Technology, or doing research study in these areas. If you are novel to this field then you can consult about this field from your supervisor or guide.

TECHNIQUES FOR WRITING A GOOD QUALITY RESEARCH PAPER:

1. Choosing the topic: In most cases, the topic is searched by the interest of author but it can be also suggested by the guides. You can have several topics and then you can judge that in which topic or subject you are finding yourself most comfortable. This can be done by asking several questions to yourself, like Will I be able to carry our search in this area? Will I find all necessary recourses to accomplish the search? Will I be able to find all information in this field area? If the answer of these types of questions will be "Yes" then you can choose that topic. In most of the cases, you may have to conduct the surveys and have to visit several places because this field is related to Computer Science and Information Technology. Also, you may have to do a lot of work to find all rise and falls regarding the various data of that subject. Sometimes, detailed information plays a vital role, instead of short information.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

31. Adding unnecessary information: Do not add unnecessary information, like, I have used MS Excel to draw graph. Do not add irrelevant and inappropriate material. These all will create superfluous. Foreign terminology and phrases are not apropos. One should NEVER take a broad view. Analogy in script is like feathers on a snake. Not at all use a large word when a very small one would be sufficient. Use words properly, regardless of how others use them. Remove quotations. Puns are for kids, not grunt readers. Amplification is a billion times of inferior quality than sarcasm.

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

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

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

Informal Guidelines of Research Paper Writing

Key points to remember:

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

Final Points:

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

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

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

General style:

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

To make a paper clear

· Adhere to recommended page limits

Mistakes to evade

- Insertion a title at the foot of a page with the subsequent text on the next page
- Separating a table/chart or figure - impound each figure/table to a single page
- Submitting a manuscript with pages out of sequence

In every sections of your document

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

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

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

· Align the primary line of each section

· Present your points in sound order

· Use present tense to report well accepted

· Use past tense to describe specific results

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

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

Title Page:

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

Abstract:

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

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

Write your summary when your paper is completed because how can you write the summary of anything which is not yet written? Wealth of terminology is very essential in abstract. Yet, use comprehensive sentences and do not let go readability for briefness. You can maintain it succinct by phrasing sentences so that they provide more than lone rationale. The author can at this moment go straight to shortening the outcome. Sum up the study, with the subsequent elements in any summary. Try to maintain the initial two items to no more than one ruling each.

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

Approach:

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

Introduction:

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

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

Approach:

- Use past tense except for when referring to recognized facts. After all, the manuscript will be submitted after the entire job is done.
- Sort out your thoughts; manufacture one key point with every section. If you make the four points listed above, you will need a least of four paragraphs.

- Present surroundings information only as desirable in order hold up a situation. The reviewer does not desire to read the whole thing you know about a topic.
- Shape the theory/purpose specifically - do not take a broad view.
- As always, give awareness to spelling, simplicity and correctness of sentences and phrases.

Procedures (Methods and Materials):

This part is supposed to be the easiest to carve if you have good skills. A sound written Procedures segment allows a capable scientist to replacement your results. Present precise information about your supplies. The suppliers and clarity of reagents can be helpful bits of information. Present methods in sequential order but linked methodologies can be grouped as a segment. Be concise when relating the protocols. Attempt for the least amount of information that would permit another capable scientist to spare your outcome but be cautious that vital information is integrated. The use of subheadings is suggested and ought to be synchronized with the results section. When a technique is used that has been well described in another object, mention the specific item describing a way but draw the basic principle while stating the situation. The purpose is to text all particular resources and broad procedures, so that another person may use some or all of the methods in one more study or referee the scientific value of your work. It is not to be a step by step report of the whole thing you did, nor is a methods section a set of orders.

Materials:

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

Methods:

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

Approach:

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

What to keep away from

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

Results:

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

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

Content

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

What to stay away from

- Do not discuss or infer your outcome, report surroundings information, or try to explain anything.
- Not at all, take in raw data or intermediate calculations in a research manuscript.
- Do not present the similar data more than once.
- Manuscript should complement any figures or tables, not duplicate the identical information.
- Never confuse figures with tables - there is a difference.

Approach

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

Figures and tables

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

Discussion:

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

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

Approach:

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

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