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

Global Journal

of Computer Science and Technology: E

Network, Web & Security

Highlights

- Hospital Management
- IP TRACEBACK Scenarios
- Multi Attacker Collision
- Energy Metering System

Discovering Thoughts, Inventing Future

VOLUME 13 ISSUE 3 VERSION 1.0

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

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

Volume 13 Issue 3 (Ver. 1.0)

Open Association of Research Society

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

Global Journals Inc.

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

Sponsors:Global Association of Research

Open Scientific Standards

Publisher's Headquarters office

Global Journals Inc., Headquarters Corporate Office, Cambridge Office Center, II Canal Park, Floor No. 5th, ***Cambridge (Massachusetts)***, Pin: MA 02141 United States

USA Toll Free: +001-888-839-7392

USA Toll Free Fax: +001-888-839-7392

Offset Typesetting

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

Packaging & Continental Dispatching

Global Journals, India

Find a correspondence nodal officer near you

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

eContacts

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

Pricing (Including by Air Parcel Charges):

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

Editorial Board Members (HON.)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Contents of the Volume

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 13 Issue 3 Version 1.0 Year 2013
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

It Security in Hospital Management

By Manoj Chopra
Bonnie Foi College

Abstract - Hospital IT security presents many unique challenges that must be solved by the entire organization. Network and computer threats can cause thousands of dollars in lost time and resources, legal repercussions, and damaged reputation. Despite warnings from a wealth of public breach notifications, many hospitals are inadequately prepared to deal with today's computer-based attacks. This research explores the root causes of hospital network and computer in security, and addresses these problems with methods implemented in actual hospitals. A lack of comprehension of methods to assess and implement security measures by hospital IT security employees can hinder network visibility and prevent their ability to stop threats. In addition, these same people are unable to express security concerns in terms management can understand, harming their credibility within the business as a whole. Without this support, organizational change is impossible. By addressing these concerns with a combination of people, process, and tools, we can solve complex problems, protect patient data, and ensure IT operations so hospitals can serve their community and save lives.

Keywords : *web filtering, e-mail filtering, system patching, antivirus, secure wireless access, firewall configuration.*

GJCST-E Classification : *K.6.5*

Strictly as per the compliance and regulations of:

It Security in Hospital Management

Manoj Chopra

Abstract - Hospital IT security presents many unique challenges that must be solved by the entire organization. Network and computer threats can cause thousands of dollars in lost time and resources, legal repercussions, and damaged reputation. Despite warnings from a wealth of public breach notifications, many hospitals are inadequately prepared to deal with today's computer-based attacks. This research explores the root causes of hospital network and computer in security, and addresses these problems with methods implemented in actual hospitals. A lack of comprehension of methods to assess and implement security measures by hospital IT security employees can hinder network visibility and prevent their ability to stop threats. In addition, these same people are unable to express security concerns in terms management can understand, harming their credibility within the business as a whole. Without this sup- port, organizational change is impossible. By addressing these concerns with a combination of people, process, and tools, we can solve complex problems, protect patient data, and ensure IT operations so hospitals can serve their community and save lives.

Keywords : web filtering, e-mail filtering, system patching, antivirus, secure wireless access, firewall configuration.

I. Introduction

Securing a hospital network is challenging. Doctors and physicians often require special needs, and external vendor systems require agreements that pose restrictions on possible security controls. In addition, hospitals have many of the same challenges other organizations struggle with. Improper management of systems and network defenses can expose private information and credit card numbers to attackers. This can violate laws and regulations, cause negative publicity, impact the financial stability of the business, and hinder the ability to provide care to patients.

Effective security requires many working parts in an organization, not all of which are technical solutions. Defined process, skilled and well-managed personnel, and management support are vital aspects of security. Many hospitals fail to address one or more of these aspects, leaving their network open from multiple attack vectors.

Security breaches may also hinder a hospital's ability to adequately care for its patients, or admit new patients. Viruses and other attacks can cause medical record systems to be disabled, forcing hospitals to revert to a paper system and decreasing efficiency. In some cases, incidents can prevent hospitals from providing adequate care. In these cases, ambulances may have to be rerouted to other medical facilities in the area, losing business and endangering those who need immediate care.

Author : Computer Science Department.
E-mail : Manoj_19143@ rediffmail.com

II. Defining 'Security'

First, when we refer to 'security' throughout this research paper, we are referencing IT security, not physical or some other type. Security is often defined as protecting the confidentiality, integrity, and availability of data, but the interpretation and context of these aspects will change from organization to organization.

Rather than creating an overall definition of 'security', we will define it in terms of several goals. When we refer to 'security' throughout this paper, we will mean technology, processes, procedures, and organizational structures that:

- Ensure the confidentiality, availability and integrity of electronic/digitized assets and data, especially PHI.
- Ensure the ability to provide quality care to hospital patients through the use of technology.
- Minimize the impact of security threats against the needs of the business.

We hope to represent the flexible and intangible nature of security, especially in a hospital environment, by defining 'security' as a collection of goals, rather than an absolute state. As we will show later, security events can be quantified in terms of risk, which must either be accepted or not for each hospital dependent on individual tolerance. Some hospitals may accept more risk while defining themselves as 'secure', while others will accept less risk. It is not a term that can be absolutely defined, and we make no attempt to represent it as such. We simply present one useful definition for our purposes here.

III. Proposal

Many approaches to network and computer security focus purely on better technology. By increasing the effectiveness of anti-virus, web proxies, intrusion detection, and other technologies, attacks can theoretically be prevented over the network. In reality, this is not the case. The true problem of network and computer security in hospitals is not with the current technology solutions available on the market. The problem is with the way security is understood, accepted, and implemented by the people within the hospital. Communication between security teams and

upper-level management is a driving factor for this problem. As we will show, management support is required for any major change in an organization, because many security changes affect the entire organization. If this support is missing, many changes are ineffective or incomplete. Our approach seeks to address both the technical issues as well as communication issues. It meets the needs of the organization while defending its most important assets. It provides the flexibility and resiliency to cope with the changing world of computer and network security, and addresses the complex factors involved in security for a large organization. Our method contains multiple stages. First, hospitals must understand the specific challenges they face. Next, specific methods will be used for assessing a hospital's security and risk posture. Once these are complete, other methods can be used to consistently improve IT security in these organizations. In the final section, case studies will illustrate the success of the method. It was implemented in several hospitals who have all reached various levels of maturity.

IV. Hospital Security

a) *Implementation*

As discussed previously, security within an organization is a combination of people, process, and tools. Technical controls - tools - provide a means to restrict and regulate the network. Process defines standards by which the organization implements and enforces security controls. Finally, the people, including politics between departments, the culture of the organization, and simply their communication, are ultimately responsible for security. All three are necessary to protect the hospital network. The assessment phase helps the hospital understand its current security posture. Using the data obtained, security exposures can be identified, and then corrected. The methods described in this chapter include many specific technical controls that must be implemented to provide a reasonable degree of security. Beyond these controls, most hospitals struggle with communication and internal politics. Lower level security employees cannot communicate appropriately with upper level management, which will allow them to obtain the support they need for security initiatives.

V. Specific Technical Controls

Every hospital must have a set of technical controls to protect their network. They must also have the proper personnel and management support to drive the change necessary to implement and enforce the controls. A list of controls have been defined below that will drastically improve security for most hospitals. Each of these controls can be implemented in many ways. No particular vendor or implementation is recommended, although several are mentioned as examples. These are details that must be worked out for each individual hospital to solve their specific needs.

a) *Web Filtering*

The majority of successful attacks today expose vulnerabilities in web browsers. These can be attacks against the browser itself (such as Internet Explorer or Mozilla Firefox), but they can also exploit other services utilized by the browser such as Java or Adobe Flash. As such, normal web browsing creates a large security risk for any hospital. To help protect against these specific attacks, web filtering appliances can be purchased from many vendors. It is also possible to use an open source tool, such as Snort, to create a custom web filter, but most organizations opt to purchase a pre-built solution.

Control 1: All web browser traffic must be filtered through a web gateway or proxy appliance.

Web filters generally work using blacklists. This approach blocks specific web traffic based on content signatures, DNS name, IP address, or other static rules. Any traffic that does not specifically match is allowed by default. Some web filters act as an enterprise-wide anti-virus solution. For example, McAfee's Web Gateway[19] searches for content matching known viruses. Due to the prominence of attacks originating from web browsing, a web filter is absolutely necessary for any hospital.

b) *Email Filtering*

The primary responsibility of an email filter is often to reduce or eliminate spam for an organization, and minimize viruses and other threats. Email attacks can trick a user into opening a malicious web link or attachment, but they can also attempt to get a user to divulge sensitive information. To prevent most spam and malicious emails, we can use a dedicated email filter, such as Cisco IronPort[9].

Control 2: All email must be filtered through a dedicated email server to remove spam and malicious attachments.

Like the web filter, this approach may not prevent all attacks, but we can use it to help reduce the attack surface of the organization.

c) *System Patching*

Most virus-related incidents in hospitals can be prevented with effective patch management. Most hospitals have thousands of computing devices on their network, a large percentage of which are running some version of Microsoft Windows. Many security vulnerabilities are discovered each month for Windows that can allow an attacker to successfully exploit and compromise a system. Because new vulnerabilities are discovered at a high rate, it becomes equally important

that we are able to apply patches that correct these vulnerabilities. Figure 4.1.3 shows the number of vulnerabilities released per month for Microsoft products that were rated `Consistent Exploit Code Likely' by their Exploitability Index [20]. This rating means\analysis has shown that exploit code could be created in such a way that an attacker could consistently exploit that vulnerability."[20] Also included is a tally of those vulnerabilities that were being actively exploited on the Internet at the time Microsoft released the monthly bulletin announcing the vulnerabilities. [21] This measurement shows that sometimes a vulnerability is being exploited before a patch is even available. This increases the urgency for applying a patch to vulnerable systems.

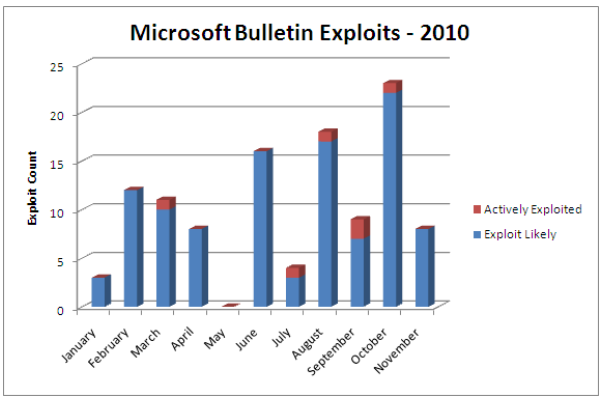


Figure 1 : Microsoft Bulletin - Count of likely exploitable vulnerabilities per month in 2010

Control 3: Automatic patching must be implemented and enforced for all computer systems on the network. Sensitive systems or systems that cannot utilize an automatic system must have a patching procedure in place.

Microsoft Windows is not the only attack surface that requires regular patching. Adobe products (Flash, Acrobat Reader, Shockwave, etc.), Java, Apple Quicktime, and any other popular software are often discovered to have severe security vulnerabilities as well. Other operating systems, such as many Linux variants or Mac OS X release patches for newly discovered security vulnerabilities, although these are exploited less often due to a smaller user base. Finally, many medical system vendors prohibit hospitals from installing patches on their computer systems, even if the hospital owns the system. They instead require the hospital wait for the vendor to patch the system for new vulnerabilities. Unfortunately, many of these systems never get patched once they are installed in the hospital environment. To combat this, other controls must protect these systems, such as network segregation and strict policy surrounding their usage.

d) Anti-Virus

Anti-virus is primarily the last defense against an attack. When all other con- trols have failed, a local anti-virus installation can detect and block malicious code before it is able to compromise and infect a system. When referring to `anti-virus' in this paper, it should be considered a program which tries to detect and prevent any type of malicious attack on an end-point system. This can include Trojan Horses, viruses, worms, adware, spyware, and any type of attack normal enterprise anti-virus can detect and prevent. Anti-virus is most useful on Microsoft Windows computers. Solutions do exist for Linux and OS X, such as ClamAV[10] for Linux and Sophos[33] for OS X, but they typically provide less value to hospitals, who have a high number of Windows systems in the network environment.

Control 4: Anti-virus must be installed and up-to-date on end systems.

Anti-virus should be installed on any Microsoft Windows system with adequate resources. Administrators often forgo installing it on high load servers for fear it will adversely impact performance. This is a risk that can be accepted provided other controls protect the system. Like system patching, many medical system vendors prohibit hospitals from installing anti-virus solutions on their systems. Their reasons include performance concerns and unintended side effects. When this occurs, other controls must adequately protect these systems. The hospital should ensure that anti-virus is updated regularly to the latest software versions. This includes the anti-virus installation itself, but it also includes virus signatures released regularly from the vendor. This ensures the system can be protected from the latest known threats. Despite providing a valuable control, anti-virus is still limited by its signature definitions. It can only detect and protect a system from known threats. Polymorphic viruses and new attacks will bypass anti-virus and are still capable of compromising a system.

e) External Device Control

Any device capable of easily and physically carrying data inside or outside the hospital network can be classified as an \external device". This includes both hospital provided and personal laptops, and removable media such as USB ash drives or external hard drives. These devices can be connected to insecure networks outside of hospital control, which can cause them to become infected with a virus or other malicious software. Upon returning to the internal hospital network, the malicious code can then attack the internal network and company resources. Hospitals should also be concerned with data ex- filtration. A laptop is capable of carrying PHI outside the network, which can lead to a security incident if not adequately controlled.

Control 5 : Only hospital provided and controlled PCs should be allowed to connect to the internal network. USBs and other forms of removable media should be tightly controlled, and ideally completely restricted.

While company policy can provide some mitigation of this threat, it may not be a strong deterrent for many employees or other outside personnel (consultants, guests, etc.). Effective technical solutions tend to be expensive and difficult to implement. One example is Cisco's Network Access Control (NAC), which is certainly expensive, but when configured properly can protect against external devices.

Ideally, in the case of an external laptop or other computer, a technical solution will detect an attempt to connect to the network. It will then run through a series of checks before allowing the device to communicate with the rest of the network. These checks can include system patch levels, anti-virus installation and version, and other software checks. If the system passes, it is allowed to connect. If not, it must correct the problems before it can access the internal network. To correct the problems, a separate VLAN is often utilized to allow the user to download patches or other requirements. Software controls can be used to prevent users from using unauthorized external media. Super glue can also physically seal the USB drives of a computer, although we do not recommend this.

Laptops and other hospital resources (hard drives, USB sticks, etc.) carrying sensitive data must be fully encrypted if they can be taken outside hospital property. This is especially important for laptops or any device that may be a target for thieves. Many HITECH breach incidents[14] were related to stolen hard drives, USB sticks, or laptops containing personal data. In such cases, companies must disclose the data loss to the public, and then pay for remediation. With encryption, the only loss is the physical hardware.

Control 6: External devices storing sensitive data must be encrypted.

f) Secure Wireless Access

Wireless access points provide convenience for hospital employees and outside guests. The signal for access points is broadcast over the air, which can allow anyone within range to view and attempt to connect to the network. Without proper controls, an intruder could gain access to sensitive resources or disrupt network operations. Primarily, employee wireless access should be encrypted with enterprise WPA2 using a central RADIUS (Remote Authentication Dial In User Ser- vice) or AAA (Authentication, Authorization, Accounting) server. This provides a strong level of encryption and allows employee access to be controlled with a central server. Guest wireless access is typically unencrypted and open in most hospitals. This allows anyone, even attackers, to connect to the network. To prevent a malicious user from compromising the internal hospital network, the guest network should be on a completely separate network. Without restrictions on the guest wireless network, employees can also connect to this open network and bypass normal internal network filters (such as web filters or tight firewall rules). This can lead to employees accessing Internet resources that should be restricted. It is also possible external users can detect and attack an employee system connected in this way. To prevent this, WPA/WPA2 encryption should be enabled on the guest network, even if it uses a simple and publicly available encryption key. Employee systems should also be denied access to this network by using a network access control tool like Cisco NAC.

g) Firewall Configuration

Numerous resources exist explaining how to properly configure an enterprise firewall for security. This is only mentioned for posterity. Firewalls should be configured as restrictively as possible. Internal systems should not have unrestricted access to the external Internet. Direct access from the external Internet should be prohibited to the internal hospital network. A demilitarized zone (DMZ) should be designated for allowing external Internet access to resources hosted on the hospital network. The DMZ must be restricted from accessing the internal network.

Control 7: Firewalls should be properly configured to be as restrictive as possible.

VI. Other Controls

Most hospitals struggle to implement and maintain even basic controls, and the broad range of controls we listed above attempt to solve the most common areas of exposure. They should be implemented on any hospital network. However, many other controls should be used to provide more granular protections. As an example, passwords should be complex and changed regularly (as defined and accepted by company policy). This is a minor control that can be implemented with Microsoft Active Directory, and its definition can change per individual hospital. There are different ways to provide authorization to resources, such as Active Directory for network shares, or specific configurations for individual systems. Generally, users should be given minimal access to the resources they need to do their jobs. External Internet access should be restricted, internal server resources should be restricted, and individual workstation access should be restricted. By providing minimal access, we limit the exposure surface of the hospital computer and network resources. Technical controls help protect the hospital network. However, they are only one aspect of securing a network. The next section will discuss the

human aspect of security, which must be successful in order to meet the constantly changing security world.

VII. Security Personnel

The technical controls in the previous section provide strong protection against many forms of attack, but it is equally important to address the people side of security. Politics between differing groups and individuals, as well as the culture of the organization, play a role in security. Individual knowledge and skill are important as well. Hospitals are no different than any other organization in this manner. Low level security personnel are essential for implementing and maintaining security controls and providing creative solutions to problems. In addition, management must actively support and enforce security initiatives. The interaction between these groups has an effect on how security is implemented within the hospital. In this section, guidelines will be provided for structuring the security of a hospital. Also, when groups within an organization communicate effectively, they can solve security problems.

VIII. Security Team

The security team is tasked with administering and reviewing the security systems at the hospital. Not only do members of the security team configure and maintain appliances, systems, and security software throughout the organization, but they must also review logs and other reports for security incidents. They think and make decisions about security for the hospital, although final approval may defer to a manager or director. Members of the security team generally administer major security systems at the hospital such as firewalls, web filtering appliances, email and spam filters, IDS/IPS appliances, vulnerability scanning, central logging systems, anti-virus, and patch management systems. In many cases they will have other responsibilities that may or may not directly impact the security of the organization. Hospitals often do not have the resources to have dedicated security personnel without other responsibilities. In many cases, the members of the security team will not be directly responsible for administering a system that has an impact on security. This could be a weakness discovered from a vulnerability scan, a new web server that will be placed on the DMZ, or any number of IT operational items. When this occurs, members of the security team must work with other members of the organization to implement or maintain a system. They can provide advice on the security of the system, as well as test it to ensure it functions as intended. Good inter-departmental relationships are vital for this to be a success. When dealing with another department the security team will often rely on their manager or director. In some cases, a formal security team has not been established for the hospital. If this is the case, a security team should be created. When selecting team members, choosing personnel who already administer many of the devices and systems mentioned above can be a good idea. However, this selection is often decided by an already existing IT manager. The members must be trustworthy and reasonably knowledgeable about security. The team must also include a manager with the authority to make decisions acting the network infrastructure of the organization, and he or she must also be able to raise concerns with higher level management when necessary. When a team is established, they can begin to discuss and handle many of the responsibilities required of this team. Weekly meetings are often worth- while to ensure that everyone and the manager is on the same page. Formal policies must also be defined around this team and they must work with the organization to get these policies and responsibilities accepted. The security team is also responsible for thinking about and solving IT security problems for the hospital. Some problems may be directly solvable by members of the security team, while others must be delegated to outside groups through management. For example, a security team member may be directly responsible for the management of the hospital firewall, and can make any adjustments as necessary. This depends on the expertise of the individual team members. In some cases, the security team may only need to provide recommendations to other groups within the hospital. The security team should meet regularly, usually once per week. In each meeting the security team should assess the current state of computer and network security for the hospital, then address any new or ongoing initiatives. The team should always explore ways to improve the hospital's security, even if improvements are not forthcoming. It is then the manager's responsibility to best utilize the resources at his disposal and drive the initiatives of the security team.

IX. Management Support

Strong and efficacious network security begins with management support. The security manager oversees the security team and is responsible for ensuring resources are focused where necessary. This can be a balancing act between security responsibilities and normal IT responsibilities. The manager must also ensure that team members are consistently reviewing security data and reports so incidents are noticed and duly investigated. The security team must be supported further by an executive at the director or higher position (like Chief Information Security Oficer). The director must handle funding for the security program. They must also understand IT security risk and be able to present this effectively to the rest of the organization. Most importantly, they must help the security team navigate

the politics and culture of the entire hospital. Without support from the rest of the organization at a high level, the security team will be hindered during investigations and response, they will not be able to enforce policy, and they will not get proper funding. Management support is required to get the resources necessary, both in personnel and monetary, to efficiently and effectively deal with security problems. Their support is also needed for policy change and enforcement. "Those with the power to allocate resources, both financial and the time of employees, can control any change expressed from lower in the power structure.

Figure 2 : An example hospital organizational structure

X. Conclusion

Hospitals have many of the same IT security problems experienced by other organizations, but with added complications from doctors, external vendor systems, patient records, and specific legislation. They also struggle with insufficient resources and often lack comprehensive expertise to cover all areas of security. Ineffective communication between low level security personnel and management can cause misplaced priorities and misguided initiatives. Securing a hospital network requires a combination of technical controls, policies and processes, and responsibility among the people of the organization. By first understanding the hospital network and its resources, then by quantitatively measuring the IT security risk and understanding areas of exposure, a strong security strategy can be created and supported by management, the security team, and the rest of the organization. Finally, security must be continually assessed and reassessed. With new and innovative threats, effective security cannot remain stationary. It must constantly evolve to meet new challenges. IT security for hospitals cannot be solved with a simple approach and a single piece of technology. It is an entire process among many people within the organization. By addressing these problems as they are - complex and multi-tiered - the confidentiality, integrity, and availability of computing resources will be ensured. This will allow the hospital to function normally as a business and serve patients effectively and with privacy.

XI. Acknowledgements

A special thanks for Dr. G. K. IYER, He has provided valuable input and direction, and has supported me throughout this entire process. He has shown great patience while waiting for me to write, change direction, rewrite, slightly change direction, continue to write, and finish this research. Thanks to my parents for their unwavering love and support.

References Références Referencias

1. Affinity Press Release. url: https : / / www . affinityplan . org /uploadedFiles / Affinity _ Home / Who _ We _ Are / PressRelease _040510.pdf.
2. Carol Ag_ocs. \Institutionalized Resistance to Organizational Change: Denial, Inaction and Repression". In: Journal of Business Ethics 16 (1997), pp. 917-931.
3. Nessus Website. url: http://www.nessus.org.
4. ntop. url: http://www.ntop.org/.
5. OSSEC. url: http://www.ossec.net/.
6. Jeffrey Wheatman, Rob McMillan, and Andrew Walls. \How to Build a Computer Security Incident Response Team". In: Gartner Research Group (June 2010).
7. Microsoft Exploitability Index. url: http://technet. microsoft.com/en-us/security /cc998259.aspx.

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 13 Issue 3 Version 1.0 Year 2013
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Economical Way of GPRS Based Fully Automated Energy Metering System

By Md. Abul Bashar, Maruf Ahmad, Sobuj Kumar Ray, Fahad Bin Sayed & Asif Ahmed

IUBAT-International University, Bangladesh

Abstract - This paper presents a design of secure and economical (low cost) way of GPRS based fully automated energy metering system that measures and transmits the total electrical energy consumption to main server using general packet radio service (GPRS) technology provided by GSM networks and also present how the meter reading, disconnection and reconnection can be controlled from server end. The proposed EGFAEM system consist of four main parts: Energy Meters, Communication part over GPRS, Server and Management part and consumer end for billing and payment. A single phase energy meter prototype has been implemented to provide measurement up to 40A load current and 230V line to neutral voltage. Communication part is implemented by GPRS module and microcontroller, sever and consumer end are implemented in web server.

Keywords : *energy meter, pre-paid energy meter, automatic meter reading, GPRS communication, UART, i^2c, web server.*

GJCST-E Classification : *J.1*

Strictly as per the compliance and regulations of:

Economical Way of GPRS Based Fully Automated Energy Metering System

Md. Abul Bashar [α], Maruf Ahmad [σ], Sobuj Kumar Ray [ρ], Fahad Bin Sayed [ω] & Asif Ahmed [¥]

Abstract - This paper presents a design of secure and economical (low cost) way of GPRS based fully automated energy metering system that measures and transmits the total electrical energy consumption to main server using general packet radio service (GPRS) technology provided by GSM networks and also present how the meter reading, disconnection and reconnection can be controlled from server end. The proposed EGFAEM system consist of four main parts: Energy Meters, Communication part over GPRS, Server and Management part and consumer end for billing and payment. A single phase energy meter prototype has been implemented to provide measurement up to 40A load current and 230V line to neutral voltage. Communication part is implemented by GPRS module and microcontroller, sever and consumer end are implemented in web server.

Keywords : energy meter, pre-paid energy meter, automatic meter reading, GPRS communication, UART, i^2c, web server.

I. Introduction

Designing and implementing of automatic system has been becoming a prominent feature in our modern life in commercial as well as industrial systems. Due to enhancing automated networking system and modern information technology, automatic meter reading systems [1] and industrial sensor networks are getting acquainting with multifarious communication media [2].

For conventional systems, meter reader has to go to meter to get reading then we have to put the reading from their reading books. Sometimes, the meter keeps in lock then the meter reader can't get the reading.

Again, the operators put the wrong reading from their record book of reading. Moreover for reconciliation, we have to entry the collection amount from payment information of the consumer. This approach requires human involvement and it is tiresome and time consuming.

By using PSTN network, we can get meter reading [3]. Again, automatic meter reading networks introduced in [4], [5].

For high speed data control we have to use fiber optic communication but in rural area distribution system with more dispersed Distributed Energy Resources (DERs), it is not economical to deploy fiber-optic communication. Hence, wireless communication technologies are more feasible. The protection, control, monitoring, and metering between Distribution Automation Systems (DAS), and DERs have been studied in reference [6].

GPRS play an important role for transmitting data at a favorable price from residential buildings to central billing centers and providing extra services for the user. Due to high–speed, unlimited transmission range, GPRS is very appropriate for the power applications. This cellular network consists of cells, which are formed by many low power wireless transmitters. With the moment of mobile devices having cellular modem, transmission of data is also exchanged between cells to cell, which facilitates non interrupted data flow. This way it forms a point to point architecture. This technology offers extensive data coverage, no maintains costs and network fully maintained by carrier [7].

The user can obtain the status of the energy consumption and the billed amount by sending the corresponding commands from the mobile phone to the GSM modem. Then it sends the commands to the microcontroller section and the required information is sent to the user mobile through the GSM modem. Also they can obtain their consumption and billing status from specific website which is provided by Power Distributor Company. This increases the efficiency of the distribution system.

II. The System Architecture

The system architecture of economical way of GPRS based fully automated energy metering system is shown in figure 1.

Author α σ ω : Dept. of Electrical and Electronic Engineering, IUBAT-International University of Business Agriculture and Technology Dhaka, Bangladesh. E-mails : mabashar@iubat.edu, maruf@eee-lab.com, fahad@eee-lab.com

Author ρ : Assistant Manager, DESCO-Dhaka Electric Supply Company Limited. E-mail : sobuj_kumar_ray@yahoo.com

Author ¥ : Dept. of Electrical and Electronic Engineering, IUB-Independent University of Bangladesh. E-mail : sfshkl8@gmail.com

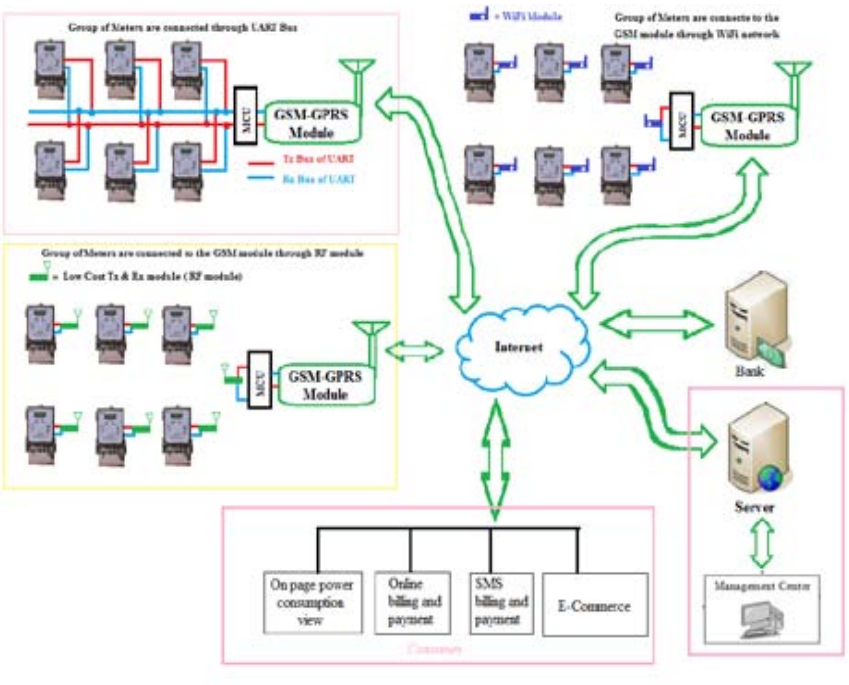


Figure 1 : System Architecture of EGFAEM System

The proposed EGFAEM system design consist of four main parts: Energy meters part, Communication part over GPRS, Server and Management part and consumer end for billing and payment.

In this system a group of meters are connected into a GSM-GPRS module by three different techniques which are shown in the figure 1. In the first system, group of meters are connected into a same bus through UART of meter MCU which connection process is done by I^2C (Intrigued Inter Connection) system and then connected to GSM-GPRS controller MCU. In second system, group of meters are connected into GSM-GPRS controller MCU through TX-RX (Transmitter and Receiver) module. And the third one, group of meters is connected into GSM-GPRS module via Zigbee or low-cost Wi-Fi module. In this paper we will present only first method of those systems.

a) Metering Part

Although a group of meters is used in the system but for example, a single phase energy meter is implemented for this purpose.

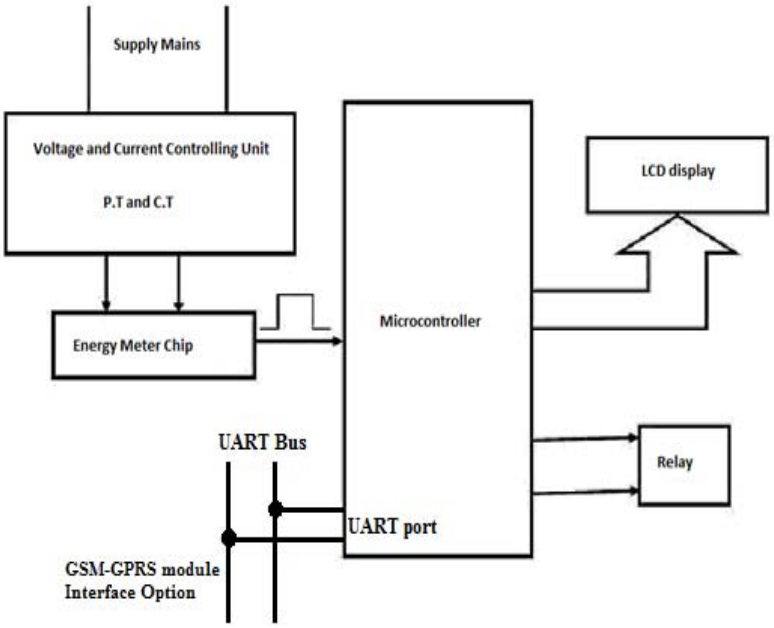


Figure 2 : Block diagram of Energy Meter

The energy meter part consist of Energy Meter IC, Voltage and Current controlling unit, Microcontroller, relays, UART bus and Liquid Crystal Display (LCD).[8]

- At first, supply mains are connected to the Voltage and Current regulating unit.
- This Voltage and Current regulating units feeds the actual voltage and current of the consumer load to the Energy meter IC with a specific ratio.
- Energy meter IC produces electrical pulses proportional to the power consumed by the consumer supply and the power supply of this metering system.
- The pulses of the energy meter chip are counted by the Microcontroller internal counter and then Microcontroller calculates the energy consumed of the consumer. It also maintains the all communication, control and display process.
- Microcontroller UART port (TXD and RXD pin) be connected to the GSM-GPRS module through UART bus for transmit the energy reading (KWh) data and receive the command from the server end.
- Relay mainly performs the opening and closing of a connection between energy meter and load through supply mains depending upon the command given from the server end.
- Liquid Crystal Display shows the energy consumption, date, time, etc. or any necessary message if the service center wants to give.

b) Communication Part

The Communication part block diagram is shown in figure 3.

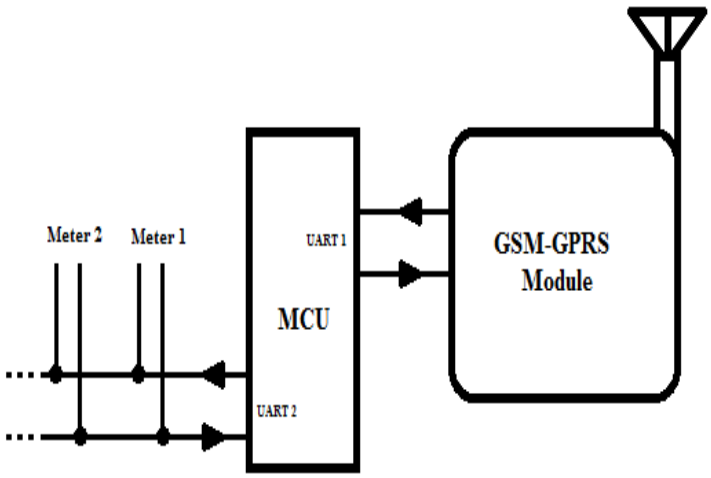


Figure 3 : Block Diagram of Communication Part

The communication part consists of UART bus, Microcontroller and GSM-GPRS module.

- GSM-GPRS module has been used to maintain the communication between meters and server thought its GSM and GPRS functions.
- Microcontroller drives the GSM-GRPS module via AT command and it also keeps communication to the Meters MCU though UART bus.

c) Server and Management Part

The Collected power consumption reading is sent to the computer server database where it is stored. As it is fully automated so, controlling or managing the consumer power supply like disconnection-reconnection, reading collection is done by the server managerial system.

d) Consumer Part

In this system, all consumer service like billing information, power consumption (KWh) reading and payment option is provided by specific website, SMS or by any other e-commerce system. So, that consumer can read and check unit consumption and pay their bill from home.

III. Hardware Development of Egfaem System

The hardware development of EGFAEM system can be divided into three parts. This are circuit diagram of energy meter unit, circuit diagram of communication unit and hardware development of management center. The description of these three parts is introduced as follows.

a) Circuit Diagram of Energy Meter Unit

The circuit diagram of energy meter unit is shown in fig. 4. The energy consumption is measured and calculated by energy meter IC and Microcontroller.

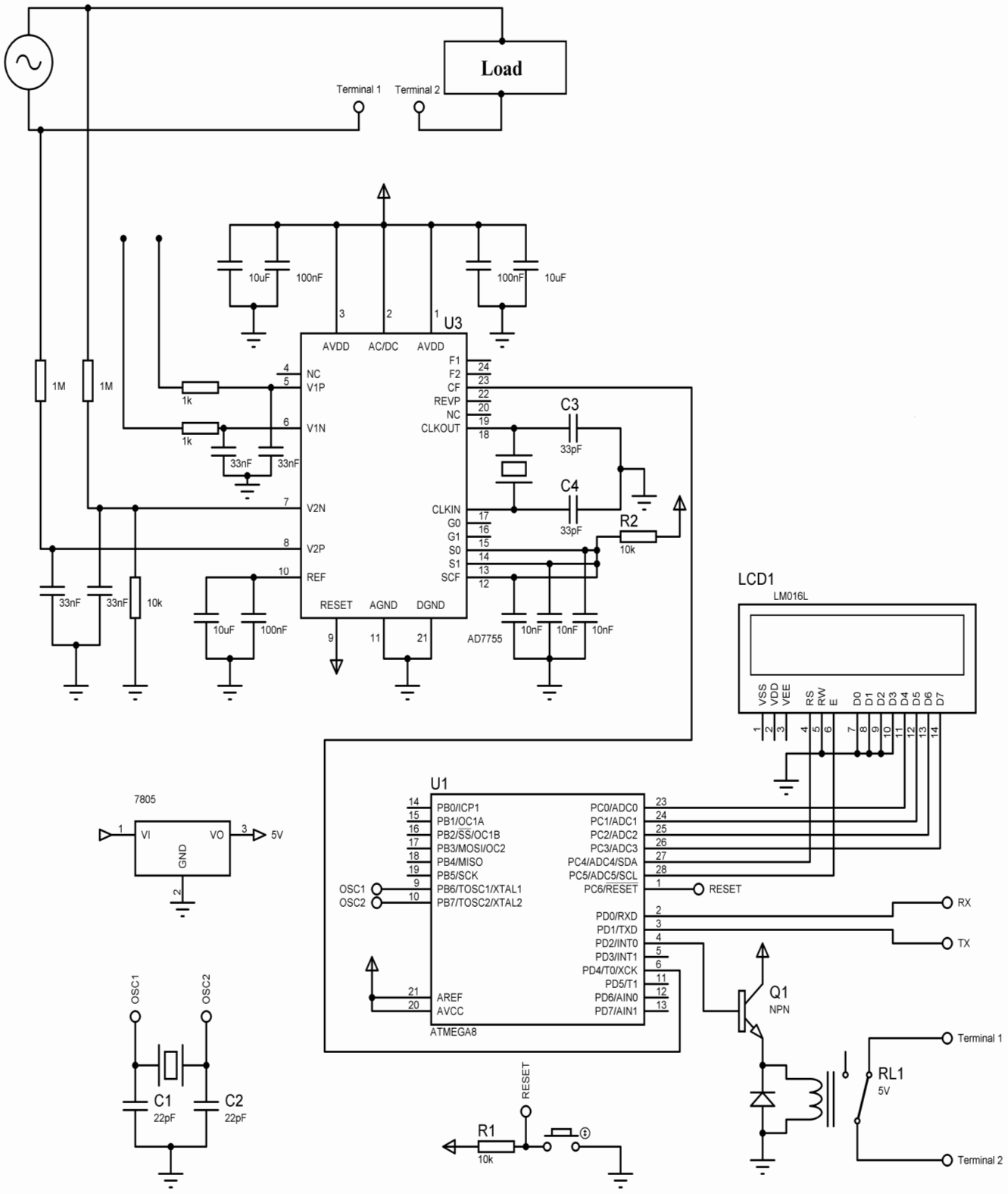


Figure 4 : Circuit Diagram of Energy Meter

In the following circuit diagram VDD represent the positive supply and GND represent the Ground. The circuit description is separately introduced as follows:

i. *Voltage and Current Transducer*

In this scheme,

ii. *Energy Metering IC*

At this project we use AD7755 as an Energy Metering IC. It is a high accuracy electrical energy measurement IC. The part specifications surpass the accuracy requirements as quoted in the IEC1036 standard. The only analog circuitry used in the AD7755 is in the ADCs and reference circuit. All other signal processing (e.g., multiplication and filtering) is carried out in the digital domain. This approach provides superior stability and accuracy over extremes in environmental conditions and over time [9]. It has two ADCs that digitalize the voltage signals from voltage and current transducer. These ADCs are second order sigma-delta converters and it's over sample rate is 900 KHz. The real power calculation is derived from the instantaneous power signal which is generated by a direct multiplication of the current and voltage signals. In order to extract the real power component (i.e., the dc component), the instantaneous power signal is low-pass filtered. The low frequency output of this AD7755 is generated by accumulating this real power information. This low frequency inherently means a long accumulation time between output pulses. The output frequency is therefore proportional to the average real power. This average real power information can, in turn, be counted by a microcontroller counter to generate real energy information.

iii. *Microcontroller*

It is a small computer on a single integrated circuit containing a processor core, memory, and programmable input-output peripherals. As its small size and low cost it is popularly used in automatic control system. In this scheme, ATmega8 Microcontroller is used. The number of pulses per second present at pin CF (pin 22) of Energy Meter IC is directly proportional to the instantaneous real power information for a particular load and microcontroller counts this pulses that appear at counter pin (pin 1) of Microcontroller within every 20 seconds [10]. The information such as power, energy and maximum demand are stored in the EEPROM of the Microcontroller. Also Microcontroller's UART port (TXD and RXD pin) be connected to the UART bus for communicating between Energy Meter and GSM-GPRS module controller MCU.

iv. *Display Unit*

In this scheme, a 16x2 LCD display module is used for this project. It is mainly used to display energy consumption of the load and maximum demand of the consumer.

v. *Relay Control Unit*

This is a very important part of the Energy Meter. It provides the useful functionality of remotely disconnect and reconnect the consumer power supply which is operated by Microcontroller. It consists of a protective relay, breaker control circuit & line breaker.

vi. *Power Supply Unit*

As Energy Meter IC, Microcontroller, relay and LCD operate on 5 volts supply. Therefore, we used a constant 5 volt DC power supply. This small energy is taken from consumer supply.

b) Circuit Diagram of Communication Unit

The circuit diagram of communication unit is shown in fig. 5. It is mainly two part GSM-GPRS module part and microcontroller part. These are separately discussed as follows.

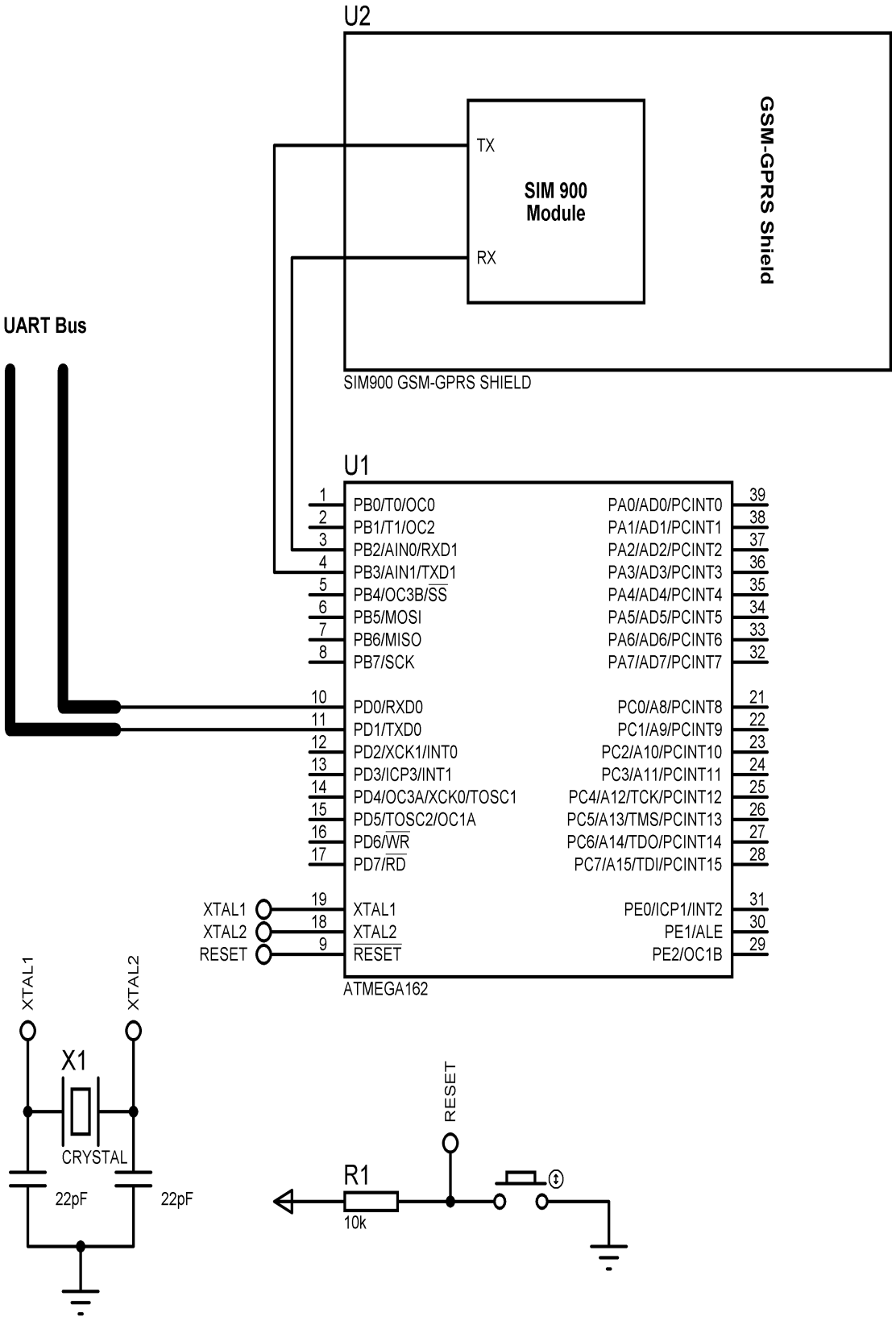


Figure 5 : Circuit Diagram of Communication Unit

i. *GSM-GPRS Module*

GSM stands for Global System for Mobile and GPRS stands for General Packet Radio Service is widely used in mobile communication architecture in most of the countries. In this scheme, we use SIM900 GSM module which is manufactured by SIMCON Limited. SIM900 is a Tri-band GSM/GPRS engine that works on frequencies EGSM 900 MHz, DCS 1800 MHz and PCS1900 MHz It is designed with power saving technique, the current consumption to as low as 2.5mA in SLEEP mode. The SIM900 is integrated with the TCP/IP, HTTP, FTP and SMTP protocols; extended AT commands are also developed for using these protocol easily. We use a GSM-GPRS Arduino shield module in the prototype implementation which has an on board SIM holder to place the SIM card and also it has GSM antenna. The transmit pin (TXD1) of the microcontroller's UART1 serial communication port is connected with the receive pin (RX) of the GSM module [11]. The transmit pin (TX) of the GSM module is connected to receive pin (RXD1) of microcontroller's UART1 serial transmission pin. Therefore the commands and their results are transmitted and received in a triangular fashion [12]. The serial communication protocol operate at the baud rate of 9600bps, one start bit, eight data bit, one parity bit and one stop bit. The AT (ATtension) commands are used to communicate with this module.

ii. *Microcontroller*

In this scheme, we use ATmega162 as a GSM-GPRS Module operator microcontroller. It has two USART ports for this reason we have chosen this IC. One is used for operating the GSM-GPRS Module and other one (TXD0 and RXD0 pin) is used for communicating the Energy Meter through UART bus.

c) Hardware Development of Management Center

In this prototype implementation, we use an internet connected Server Computer with necessary computer application and software. Meter reading collection, process and stored to the server database and reconnect and disconnect the consumer power supply (if needed), billing information publish to the web portal and automatic bill collection by web portal is done by this Server Computer of the Management Center.

IV. The Software Development of Egfaem System

In the meter and communication unit, the system software is implemented by C language and the developed code is compiled and debugged by mikroC PRO for AVR compiler.

a) Algorithm for Meter Part of EGFAEM System

1. Start.
2. Initialize the device and display.
3. Check whether the UART data ready or not. If the receive data available of the UART port then go to next or go to step 6.
4. Check the instruction command which is received by the meter and sent by the communication unit. Is the Meter ID of the instruction is matched to ID of the Meter then go to next or go to step 6.
5. Check the op-code (operation code), whether it is "Active", "Deactive" or sending the meter status command. If the command is "Active" then connect the load with the supply mains and set "active" in specific memory location for further determination or the command is sending the meter status then send meter ID and reading status to the communication unit Microcontroller via UART. After complete both process then go to step 7. If the command is "Deactive" then disconnect the load from supply mains by triggering the relay then go to step 3.
6. At this stage meter will check its specific memory location, is it previously set by "Active" means continuing supply to the load or "Deactive" means disconnecting the load from the supply. If yes then go to step 7 otherwise go to step 3.
7. Microcontroller internal counter count the pulses which are provided by AD7755 Energy Meter IC and Calculate power consumption, Energy and unit uses.
8. Store the energy, power reading and units' uses into the EEPROM of ATmega8 Microcontroller for future use.
9. Display the reading status on LCD.
10. Repeat the step 3.

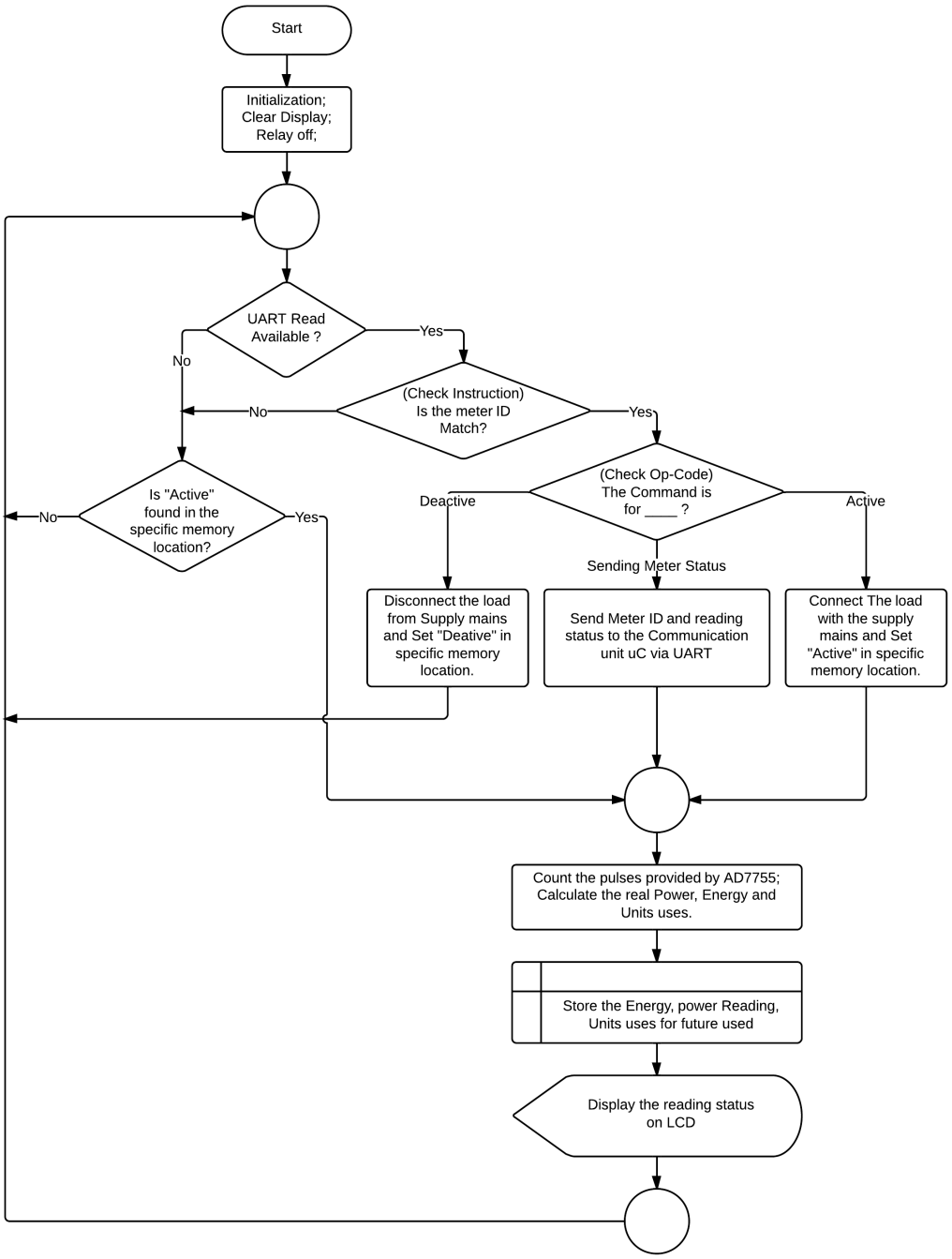


Figure 6 : Flowchart of Meter Part

b) Algorithm for Communication Unit

1. Start.
2. Initialize the device and switch on the GSM-GPRS Module.
3. Set content type as GPRS parameters, set APN, set GPRS profile to use with HTTP, set the URL direction from where it will take the instruction command. All this setting is done by specific AT command of the SIM900 module.
4. Connect with the HTTP server and check and read the instruction command. If the module ID of the read instruction command is matched with the ID of the Module then go to next or go to step 6.
5. At this stage, communication unit send the meter ID and op-code of the read instruction command which is declared by the server. This instruction byte is send by the UART0 port of the microcontroller.
6. Check the UART0, whether any data is available? If yes, the read the data like Meter ID and Meter Reading and write or upload this data to the server database through GPRS. If not then skip the read and write process.
7. Repeat step 4.

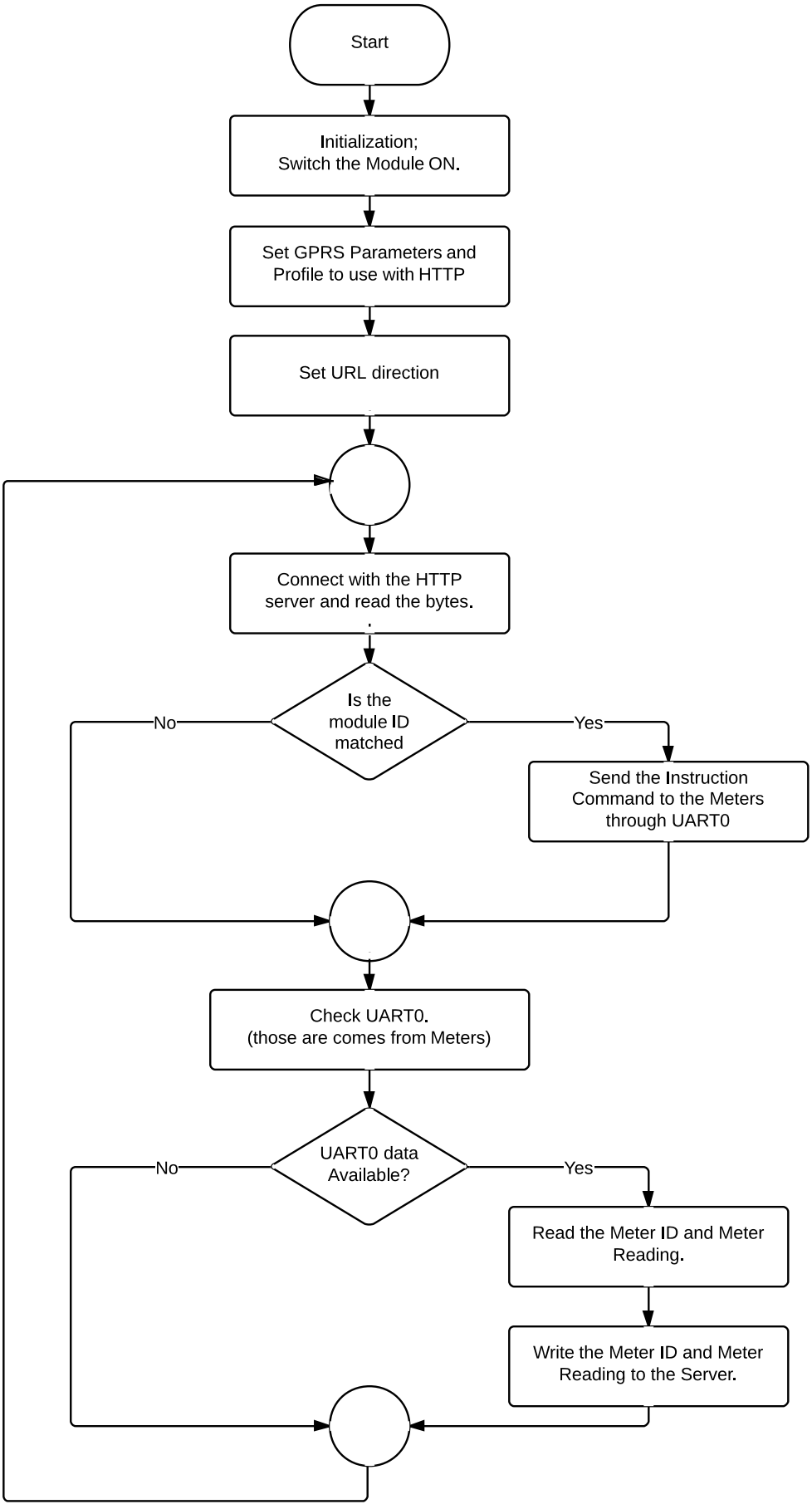


Figure 7 : Flowchart of the Communication Unit

V. Experimental Views

This experiment four energy meters with GPRS Communication box are installed in Electrical Lab at IUBAT. Each meter contains 0.5KW load by 20 one hundred bulb each of 5. Then the meter reading and terminal on-off control are successfully tested. Below Fig.8 shows the control and management web portal where consumers unit (KWh) uses, bill info, control option, current load etc can be shown.

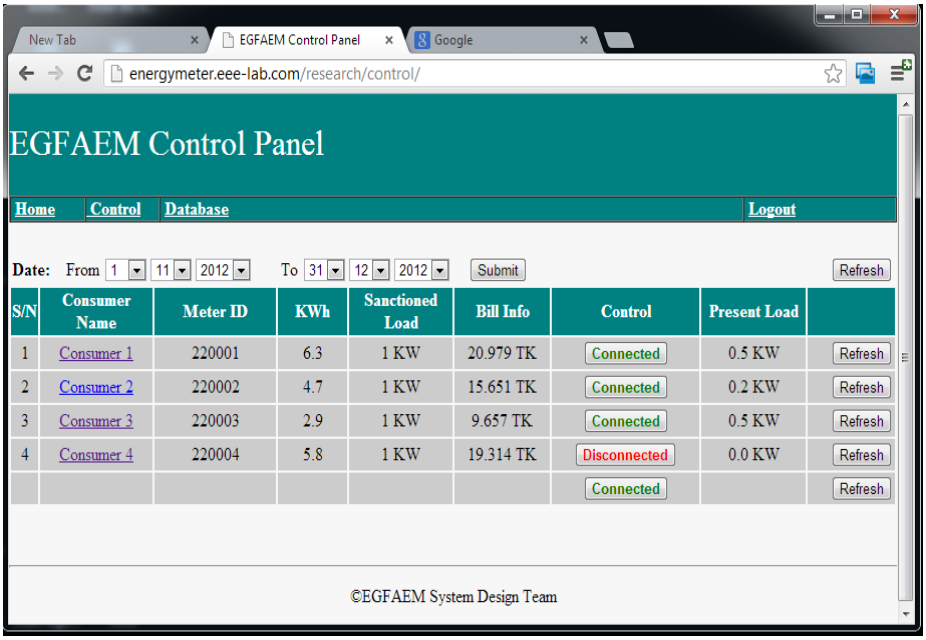


Figure 8 : Server Control Panel

Fig. 9 shows the consumer panel where consumer can check and read their billing information, unit (KWh) uses, billing history and also online payment option are added so that consumer can pay their bill from home.

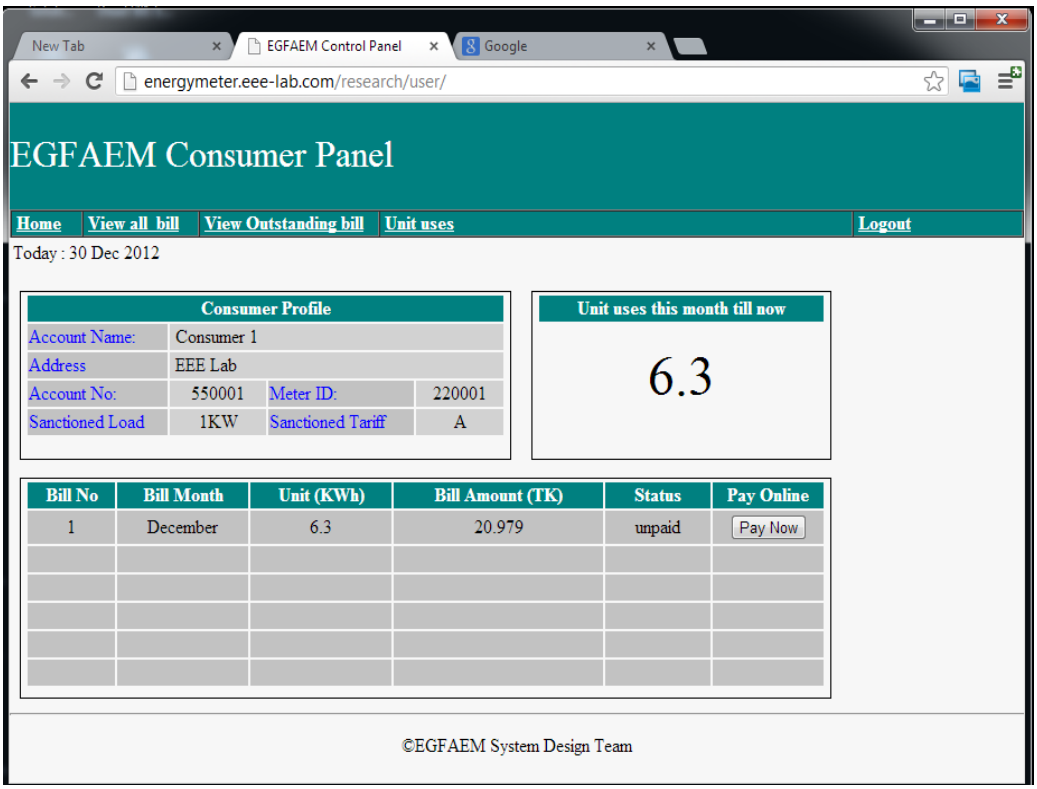


Figure 9 : Consumer Panel

VI. Conclusion

The economical way of GSM-GPRS based fully automated energy metering (EGFAEM) system has developed for efficient, secure and low cost automatic meter reading, billing and control from management center. As GSM network has covered all the housing and billing area which leads low infrastructure installation cost. This EGFAEM system can be use as both the post-paid and pre-paid metering purpose. So, that distributor can customize their package for different types of consumers which will ensure efficient business planning for the company. The management center gives automatic billing and payment system so, no man power require for meter reading and billing collection purpose which reduce human operator meter reading operation cost that's very efficient and economical for any power distribution company. Instant control (disconnection and reconnection of power supply) of individual consumer from management center gives secure and reliable power distribution because if any inconvenience situation occurred at any individual consumer then distributor can quickly disconnect that specific individual consumer supply. Consider all this things, it can be stated that EGFAEM system can bring a great change in power distribution companies of Bangladesh if the distribution companies apply this system on their field.

References Références Referencias

1. Mahmood, M. Aamir, M. I. Anis, "Design and Implementation of AMR Smart Grid Sytem," Electric Power Conference, IEEE EPEC 2008, pp. 1-6, 2008.
2. V.C. Gungor, G.P. Hancke, "Industrial Wireless Sensor Networks: Challenges, Design Principles, and Technical Approaches," IEEE Trans. on Industrial Electronics, vol. 56, no. 10, pp. 4258-4265, 2009.
3. S.W. Lee, C.S. Wu, W. M.S. Chiou and K.T. Wu. "Design of an Automatic Meter Reading System", proc. of IEEE International Conference on Industrial Electronics, Control, and Instrumentation, vol. 1.
4. L. Hong and L. Ning. "Design and Implementation of Remote Intelligent Management System for City Energy Resources based on Wireless Network", Study of Computer Application, no.12, pp. 237-239, 2004. pp. 631–636, 1996.
5. C. Yin-kang, L. Xiang-yang and X. Jing. "The Hardware Design of Concentrator for Wireless Intelligent Meter Reading System", Element and IC, no. 1, pp. 37-39, 2005.
6. P.M. Kanabar, M.G. Kanabar, W. El-Khattam, T.S. Sidhu, and A. Shami, "Evaluation of Communication Technologies for IEC 61850 Based Distribution Automation System with Distributed Energy Resources", Proc. of the IEEE PES General Meeting, Calgary, July 26-30, 2009.
7. P.K. Lee, L. L. Lai, "A Practical Approach to Wireless GPRS On-Line Power Quality Monitoring System," *Proc. of the IEEE PES General Meeting,* June 2007.
8. Haque, Md. Mejbaul, et al., "Microcontroller Based Single Phase Digital Prepaid Energy Meter for Improved Metering and Billing System", International Journal of Power Electronics and Drive System (IJPEDS), Vol.1, No.2, December 2011, pp. 139-147.
9. Analog Devices, "AD7755, Energy Meter IC with Phase output", http://www.datasheetcatalog.org/datasheet/analogdevices/AD7755.pdf
10. Microchip, "PIC16F72Datasheet",http://www.microchip.com
11. GSM Module, "SIM900 GSM-GPRS Module", http://wm.sim.com/producten.aspx?id=1019
12. Quazi, Irfan, et al., "Pre-paid Energy Meter based on AVR Microcontrolle", International Journal of Engineering Research and Applications (IJERA), Vol. 1, Issue 4, pp. 1879-1884.

This page is intentionally left blank

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 13 Issue 3 Version 1.0 Year 2013
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

IP TRACEBACK Scenarios

By Tenali. Naga Mani & Jyosyula. Bala Savitha
CSE Gudlavalleru Engineering College

Abstract - Internet Protocol (IP) trace back is the enabling technology to control Internet crime. In this paper, we present novel and practical IP traceback systems which provide a defense system with the ability to find out the real sources of attacking packets that traverse through the network. IP traceback is to find the origin of an IP packet on the Internet without relying on the source IP address field. Due to the trusting nature of the IP protocol, the source IP address of a packet is not authenticated. As a result, the source address in an IP packet can be falsified (IP address spoofing). Spoof IP packets can be used for different attacks. The problem of finding the source of a packet is called the IP traceback problem. IP Traceback is a critical ability for identifying sources of attacks and instituting protection measures for the Internet. Most existing approaches to this problem have been tailored toward DDoS attack detection.

GJCST-E Classification : C.2.0

Strictly as per the compliance and regulations of:

IP TRACEBACK Scenarios

Tenali. Naga Mani [α] & Jyosyula. Bala Savitha[σ]

Abstract - Internet Protocol (IP) trace back is the enabling technology to control Internet crime. In this paper, we present novel and practical IP traceback systems which provide a defense system with the ability to find out the real sources of attacking packets that traverse through the network. IP traceback is to find the origin of an IP packet on the Internet without relying on the source IP address field. Due to the trusting nature of the IP protocol, the source IP address of a packet is not authenticated. As a result, the source address in an IP packet can be falsified (IP address spoofing). Spoof IP packets can be used for different attacks. The problem of finding the source of a packet is called the IP traceback problem. IP Traceback is a critical ability for identifying sources of attacks and instituting protection measures for the Internet. Most existing approaches to this problem have been tailored toward DDoS attack detection.

I. Introduction

A great amount of effort in recent years has been directed to the network security issues. In this paper, we address the problem of identifying the source of the attack. We define the source of the attack to be a device from which the flow of packets, constituting the attack, was initiated. This device can be a zombie, reflector, or a final link in a stepping stone chain. While identifying the device, from which the attack was initiated, as well as the person(s), behind the attack is an ultimate challenge, we limit the problem of identifying the source of the offending packets, whose addresses can be spoofed. This problem is called the IP traceback problem [1]. IP spoofing occurs when a hacker inside or outside a network impersonates the conversations of a trusted computer [2]. A hacker changes the routing table to point to the spoofed ip address, then the hacker can receive all the network packets that are addressed to the spoofed address and reply just as trusted users.

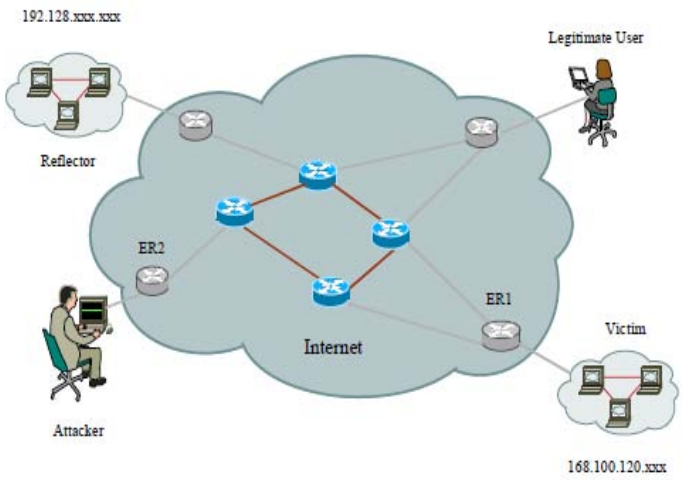


Figure 1 : A Scenario of DOS Attack

Several solutions to this problem have been proposed. They can be divided in two groups. One group of the solutions relies on Fig 1 A Scenario of DOS Attack.

The routers in the network to send their identities to the destinations of certain packets, either encoding this information directly in rarely used bits of the IP header, or by generating a new packet to the same destination. The biggest limitation of this type of solutions is that they are focused only on flood-based (Distributed) Denial of Service [DoS] attacks [3], and cannot handle attacks comprised of a small number of packets. The second type of solutions involves centralized management, and logging of packet information on the network. Solutions of this type introduce a large overhead, and are complex and not scalable.

Author α : Asst. Professor, CSE Gudlavalleru Engineering College Gudlavalleru, Krishna (D.t), A.P. E-mail : tenalinagamani@gmail.com
Author σ : B.Tech (3/4), IT Vijaya Institute of Technology Krishna (D.t), A.P.

IP traceback is a name given to any method for reliably determining the origin of a packet on the Internet. Due to the trusting nature of the ip protocol, the source IP address of a packet is not authenticated. As a result, the source address in an IP packet can be falsified (IP address spoofing) allowing for [7] Denial of Service attacks (DoS) or one-way attacks (where the response from the victim host is so well known that return packets need not be received to continue the attack). The problem of finding the source of a packet is called the IP traceback problem. IP Traceback [9] is a critical ability for identifying sources of attacks and instituting protection measures for the Internet. Most existing approaches to this problem have been tailored toward DoS attack detection. Such solutions require high numbers of packets to converge on the attack path(s).

II. Overview

This section provides overview of IP header [2] and the current state of the art approaches to IP traceback and evaluates. While sending data over the internet the IP header contains above details (Fig: 2). Such as type of service, its length, from which source and destination address. Header checksum for error correction and protocol-specifies the type of protocol and set of rules in data exchange.

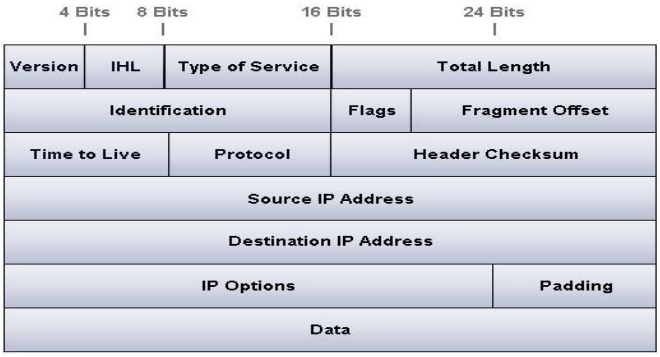


Figure 2 : IP Header

Overview of an ideal traceback system is given below.

- Able to trace the attacker with a single packet.
- Minimal processing overhead during traceback.
- Classification based evaluation.
- No packet transformed through that techniques.
- Limited amount of additional memory requirement at the dedicated server and no additional memory requirement on network
- High level of protection is preferred in a trace back.
- Network overhead based evaluation.
- Router overhead based evaluation.
- Correctly trace back attacks consisting of packets that undergo any number of transformations of any type.
- Producing meaningful traces are limited to the range of deployment of the traceback system.

We are having different traceback schemes exist. Among those FDPM provides innovative features to trace the source of IP packets and can obtain better tracing capability than others. In particular, FDPM adopts a flexible mark length strategy to make it compatible to different network environments; it also adaptively changes its marking rate according to the load of the participating router by a flexible flow-based marking scheme. Evaluations on both simulation and real system implementation demonstrate that FDPM requires a moderately small number of packets to complete the traceback process; add little additional load to routers and can trace a large number of sources in one traceback process with low false positive rates. The built-in overload prevention mechanism makes this system capable of achieving a satisfactory traceback result even when the router is heavily loaded. The motivation of this traceback system is from DDoS defense. It has been used to not only trace DDoS attacking packets but also enhance filtering attacking traffic. It has a wide array of applications for other security systems.

III. Classification of Traceback Methods

Traceback methods can be broadly categorized [2] as preventive and reactive. Preventive methods take precautionary steps in preventing DoS attacks. A wide range of solutions has been proposed, however, this problem still remains as open one. The reactive methods solutions aim at identifying the source of the attacks. This is very important because attackers spoof their addresses, thus techniques are needed to trace back to the source to the source of the attack. The evaluation is based the above two categorized methods.

a) Preventive Methods

i. *Ingress Filtering*

One way to address the problem of anonymous attacks is to eliminate the ability to forge source addresses. One such approach, frequently called ingress filtering, is to configure routers to block packets that arrive with illegitimate source addresses. This requires a router with sufficient power to examine the source address of every packet and sufficient knowledge to distinguish between legitimate and illegitimate addresses. Consequently ingress filtering is most feasible in customer networks or at the border of Internet Service Providers (ISPs) where address ownership is relatively unambiguous and traffic load is low. As traffic is aggregated from multiple ISPs into transit networks, there is no longer enough information to unambiguously determine if a packet arriving on a

particular interface has a "legal" source address. Moreover, on many deployed router architectures the overhead of ingress filter becomes prohibitive on high-speed links. The principal problem with ingress filtering is that its effectiveness depends on widespread, if not universal, deployment. A secondary problem is that even if ingress filtering were universally deployed at the customer to ISP level, attackers could still forge addresses from the hundreds or thousands of hosts within a valid customer network.

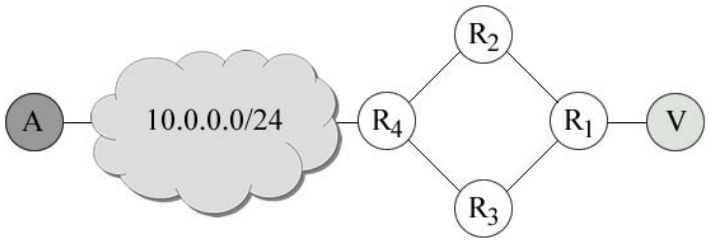


Figure 3 : Ingress Filtering is used at router R4 to prohibit the attacker from using a source IP address residing outside the 10.0.0.0/24 prefix

Ingress filtering restricts the routing of traffic that originates from a downstream network to only well-known and advertised prefixes. Equivalently, a router must drop any packet whose source address does not belong to one of such advertised networks.

Figure 2 depicts a simple network where ingress filtering is used against source address spoofing. For convenience, only IP addresses are used. With ingress filtering, router R4 drops any packet coming from subnet work spoofed source addresses to the victim V.[8] The spoofed source address, however, must reside inside the 10.0.0.0/24 prefix. For instance, the IP address of a neighbor machine could be used as the source address of attack packets. In addition, there is an undesirable dependency between security of end hosts and universal deployment of this technique. Since the filtering directly affects the routing process, inspecting the source address of every packet may also require additional resources from routers. Further, some technologies, such as Mobile IP (Perkins, 2002), legitimately employ spoofed source addresses and could also be affected.

A protection scheme has also been proposed to protect a server from SYN flooding attacks (Belenky and Ansari, 2003). Basically, [7] the scheme keeps track of half-opened TCP connections at a particular server. The tracking is not necessarily implemented on end servers; it can also be implemented on routers and firewalls, for instance. When the number of these connections exceeds a threshold, either new connection requests are blocked, or old half-opened connections are closed in order to make room for new connections. This scheme, however, is specifically designed for this kind of attack and does not provide any information about real perpetrators.

b) Reactive Methods

i. *Link Testing*

Most existing traceback techniques [2] start from the router closest to the victim and interactively test its upstream links until they determine which one is used to carry the attacker's traffic. Ideally, this procedure is repeated recursively on the upstream router until the source is reached. Below describe two varieties of link testing schemes, input debugging and controlled flooding.

a. *Disadvantage*

It consumes huge amount of resources, introduces additional traffic, and possibly causes denial of service when the number of sources needed to be traced increases.

b. *Input Debugging*

Many routers include a feature called input debugging[2],which allows an operator to filter particular packets on some egress port and determine which ingress port they arrived on. This capability is used to implement a trace as follows. First, the victim must recognize that it is being attacked and develop an attack *signature* that describes a common feature contained in all the attack packets. The most obvious problem with the input debugging approach, even with automated tools, is its considerable management overhead. Communicating and coordinating with network operators at multiple ISPs requires the time, attention and commitment of both the victim and the remote personnel many of whom have no direct economic incentive to provide aid.

c. *Controlled Flooding*

Burch and Cheswick have developed a link-testing traceback technique that does not require any support from network operators. We call this technique *controlled flooding [2]* because it tests links by flooding them with large bursts of traffic and observing how this perturbs traffic from the attacker. Using a regenerated

"map" of internet topology, the victim coerces selected hosts along the upstream route into iteratively flooding each incoming link on the router closest to the victim. Since router buffers are shared, packets traveling across the loaded link including any sent by the attacker have an increased probability of being dropped.

c) Drawbacks of Input Debugging

1. A high management overhead.
2. It needs communication and coordination between different ISPs, when the attacking packets traverse different ISPs networks.
3. This scheme works only for ongoing attacks. The last but not the least, it requires network administrators to have the appropriate technical skills and capabilities.

i. *Logging*

An approach suggested is to log packets at key routers and then use data mining techniques[9] to determine the path that the packets traversed. This scheme has the useful property that it can trace an attack long after the attack has completed. However, it also has obvious drawbacks, including potentially enormous resource requirements and a large scale interprovider database integration problem. We are unaware of any commercial organizations using a fully operational traceback approach based on logging.

ii. *ICMP Traceback*

Internet Control Message Protocol (ICMP) in need of trace out full path of the attacks. This approach was originally introduced by Bellovin. The principle idea in these schemes is for every router to generate an ICMP traceback message or iTrace directed to the same destination as the selected packet. The iTrace message itself consists of the next and previous hop information and a time stamp As packets travel through the network, they gather and store information about the routers they traverse.

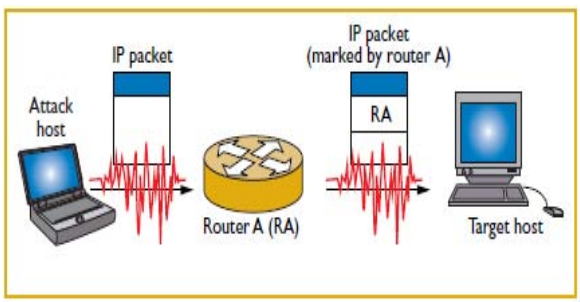


Figure 4 : Packet Marking

A router creates an ICMP traceback message, which contains part of a traversing IP packet, and sends the message to the packet's destination. We can identify the traversed router by looking for the corresponding ICMP traceback message and checking its source IP address. Because creating an ICMP traceback message for every packet increases network traffic, however, each router creates ICMP traceback messages for the packets it forwards .If an attacker sends many packets the target network can collect enough ICMP traceback messages to identify its attack path.

iii. *Packet Marking Algorithm*

In Packet Marking Algorithm [5] schemes, each router in addition to forwarding a packet also inserts a mark in the packet. This mark is a unique identifier corresponding to this particular router.

As a result the victim can determine all the intermediate hops for each packet by observing the inserted marks. There are two variants to this marking scheme. First is the Deterministic Packet Marking [5] (DPM) scheme in which each router marks all the packets passing through it with its unique identifier? This scheme is thus similar to the IP record-route option. This makes the reconstruction of the attack path at the victim trivial. But the downside to this scheme is that routers are slowed down as they have to perform additional functionality. An attacker who controls a trusted router can forge any path up to that router unless some further authentication scheme is used. A router that trusts data from an attacker effectively allows that attacker to act like a compromised router. Authentication methods could be used, but these add significant cost in the form of processing time and space in the marked packets. A downside of this scheme is that some packets will not be overwritten by any of the routers. The attacker can therefore write bogus information in all the packets knowing that some of these packets will get through and confuse the victim. This method also does not work well for DoS attacks that can work without a lot of packets as it requires a large number of packets to converge. The second instances is probabilistic packet marking[10] (PPM), DoS attacks can be prevented if the spoofed source IP address is traced back to its origin which allows assigning penalties to the offending party or isolating the compromised hosts and domains from the rest of the network.

Recently IP traceback mechanisms based on probabilistic packet marking have been proposed for achieving traceback of DoS attacks. In this paper, we show that probabilistic packet marking of interest due to its efficiency and implement ability vis-à-vis deterministic packet marking and logging or messaging based schemes suffers under spoofing of the marking field in the IP header by the attacker which can impede traceback by the victim. Attacks on PPM: Attacks involving spoofed traceback data are described in. In general the two major problems in PPM reliability are the probabilistic nature of the algorithm causes some packets not to be marked by cooperating routers and these retain whatever marks are given them by the senders. Attackers can simply mark their original packets to intentionally mislead the traceback mechanism. In DPM routers mark all forwarded packets

with link identifying data. With PPM, multiple routers on the paths overwrite the same data, and each packet identifies at most one link. With DPM, each co-operating router adds link identifying data to the packet and each packet ends up with data that identifies all of the links (under universal co-operation) that it traversed.

a. *Disadvantages of Packet Marking*

1. Mark Length: It cannot adjust the length of marking field according to the network protocols deployed.
2. Marking Rate is not flexible according to the load of the participating router.
3. Number of Packets required is comparatively more.
4. False Positive rate is large.
5. Tracing Capability is less.
6. The path reconstruction process requires high computational work, especially when there are many sources. For example, a 25-source path reconstruction will take days, and thousands of false positives could happen.
7. When there are a large number of attack sources, the possible rebuilt path branches are actually useless to the victim because of the high false positives.

iv. *FDPM Traceback*

Flexible Deterministic Packet Marking [6] (FDPM) is the optimized version of DPM. This scheme provide more flexible features to trace the IP packets and can obtain better tracing capabilities over other previous IP traceback mechanisms, such as Link testing, logging, ICMP traceback, probability packet marking (PPM) and Deterministic packet marking (DPM).In FDPM schemes, the Types of Services (ToS) fields will be used to store the mark under some circumferences. The two fields in the IP header are exploited, one is fragment ID and other is Reversed flag. An identifying value is assigned to the ID field by the sender to aid in assembling the fragments of a datagram. Given that less than0.25%of all internet traffic is fragments, this field can be safely overloaded without causing serious compatibility problems. FDPM reconstruction process includes two steps: mark recognition and address recovery. Compared to DPM [5], the reconstruction process is simpler and more flexible. When each packet that is used to reconstruct the source IP address arrives at the victim, it is put into a cache, because in some cases the processing speed is lower than the arrival speed of the incoming packets.

The FDPM [6] scheme utilizes various bits (called marks) in the IP header. The mark has flexible lengths depending on the network protocols used, which is called flexible mark length strategy. When an IP packet enters the protected network, it is marked by the interface close to the source of the packet on an edge ingress router.

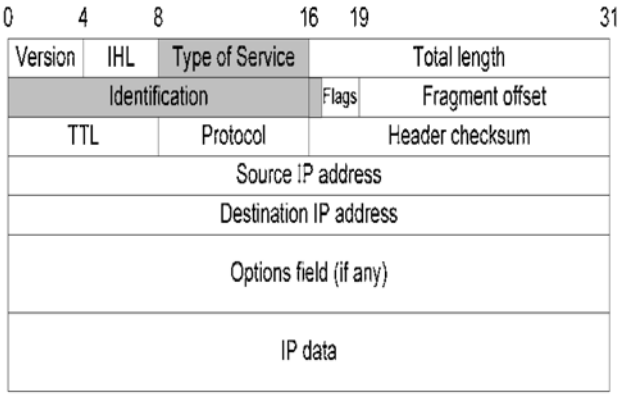


Figure 5 : IP (darkened) headers utilized in FDPM

The source IP addresses are stored in the marking fields. The mark will not be overwritten by intermediate routers when the packet traverses the network. At any point within the network, e.g., the victim host, the source IP addresses can be reconstructed when required. Processing packets consume resources such as memory and CPU time of a participating router. Therefore, it is possible for a router to be overloaded when there are a large number of arrival packets waiting for FDPM to mark them.

The flow-based marking scheme is proposed to solve the overload problem. When the load of a router exceeds a threshold, the router will discern the most possible attacking packets from other packets then selectively mark these packets. The aim is to alleviate the load of the router while still maintaining the marking function.

a. *Advantages*

1. Easy to find out packet loss and Duplicate packets.
2. Reduces the network traffic.
3. Bandwidth consumption is less.
4. Flexible mark length: The length of marking field can be adjusted according to the network protocols deployed.
5. Flexible mark rate: The marking rate can be changed adaptively according to the load of the participating router.
6. Low false Positive rate.
7. Number of packets required is comparatively less.
8. Better Tracing Capability.
9. It has Different probabilities that a router marks the attack packets.

v. *TBPM Method*

Topology [9] aware single packet IP traceback system is namely TOPO. It is based on the bloom filter which utilizes router's local topology information, i.e., its immediate predecessor information, to traceback. TOPO can significantly reduce the number and scope of unnecessary queries and thus, significantly decrease the false attributions to innocent nodes. The main goals of TOPO as follows:

1. To design a single packet IP traceback system, this has fewer unnecessary query messages and fewer false attributions to innocent nodes.
2. To design a single packet IP traceback system this needs not to be fully deployed in the entire network.
3. To design a mechanism which helps achieve the best performance of Bloom filters by adaptively adjust using parameter.

Topology Based Packet Marking (TBPM) has been a new approach in Anti-IP spoofing techniques.

TBPM builds on the strengths of the packet marking principal; however it focuses not merely on the source, but also the path traversed by a datagram. We have pointed out how a route discovery method can be more effective, especially during DoS attacks where edge routers that mark packets may themselves be unavailable as a result of the attack. Embedded topological information may enable DoS attacks to be prevented even by intermediate routers. TBPM also enables the source to be identified using a single marked packet; unlike previous techniques that require multiple packets. TBPM techniques are compatible with both IPv4 and IPv6; unlike present packet marking techniques that cannot be effectively implemented in IPv6 networks.

IV. Technologies for Preventing Network Attacks

Current technologies for protecting networks against attacks focus on access control and attack detection [2]. Although some methods can find the attacker's identity, they are unsuccessful when the attacker's true IP address is hidden or unknown.

a) Firewalls

Firewalls are widely used to protect networks against attacks, especially those coming from the Internet. Usually, firewalls control access based on source IP address, destination IP address, protocol type, source port number, and destination port number. For example, we can configure a firewall to deny any access to a WWW server except for WWW access using HTTP (destination port number 80). If an attacker attempts to exploit the WWW server using HTTP, however, the firewall cannot prevent it.

b) Intrusion Detection

An intrusion detection system (IDS) detects network attacks to a computer system. One major method currently implemented in IDS products is misuse detection. In this method, the IDS compare the attack signatures, which are features of known attacks, with the contents of packets on the network or log data on the host computer. When the packet content or log data matches an attack signature, the system recognizes that an attack has occurred. IDSs still pose accuracy problems for site managers, however. In practice, IDSs detect possible attacks, which site managers must examine to determine whether it is a real attack.

c) Intrusion Source Identification

Using IDSs, we can detect certain attacks and find the attack packets' source IP addresses. Because the IP address is not enough to identify the attack source, however, we typically run a DNS inverse query to check the fully qualified domain name (FQDN),or look up the database in a WHOIS server to find the source identity (for example, organization name and e-mail address). If the attack's purpose is penetration or reconnaissance, most attackers will hardly disguise the source IP address because they must receive a response from the target.

An attacker who aims for denial of service (DoS), however, does not need to receive packets from the target and can therefore forge its source IP address. Ingress filtering deals with forged addresses.1 in this method, a router compares an incoming packet's source IP address with a router's routing table and discards packets with inconsistent source addresses as having been forged. This method is effective for many spoofed DoS attacks, but it fails if an attacker changes its source IP address to one that belongs to the same network as the attacker's host.

V. Limitation and Open Issues

IP traceback has several limitations [1], such as the problem with tracing beyond corporate firewalls. To accomplish IP traceback, we need to reach the host where the attack originated. It is difficult, however, to trace packets through firewalls into corporate intranets the last- traced IP address might be the firewall's address. Knowing the IP address of the organization's network entry point, however, allows us to obtain information about the organization where the attacker's host is located, such as the organization's name and the network administrator's e-mail address. If we can identify the organization from which the attack originated, the organization can often identify the user who launched the attack.

Another limitation relates to the deployment of traceback systems. Most traceback techniques require altering the network, including adding router functions and changing packets. To promote traceback approaches, we need to remove any drawbacks to implementing them.

Moreover, even if IP traceback reveals an attack's source, the source itself might have been used as a stepping-stone in the attack. IP traceback methods cannot identify the ultimate source behind the stepping-stone; however, techniques to trace attacks exploiting stepping-stones are under study. Some operational issues must also be solved before IP traceback can be widely deployed. To trace an attack packet through

different networks, for example, there must be a common policy for traceback. We also need guidelines for dealing with traceback results to avoid infringing on privacy. Furthermore, we need to consider how to use information about an attack source identified by IP traceback.

VI. Conclusion

One conclusion we can draw from this is that unless IP trace back measures are deployed all over the Internet, they are only effective for controlled networks than for the Internet. Today we can find many tools for doing DoS attacks. DoS attacks have become very popular. Hence we need to design proper mechanisms to protect systems from such attacks. Mechanisms has been developed and deployed to prevent such attacks. But DDoS is still a problem as it is difficult to trace DDoS attackers and its effect is too bad. We need to start development towards defending DDoS. Some schemes are present which very well defends such attacks, but without the cooperation of ISPs it will be difficult to deploy any scheme. Though RFC asks to deploy ingress filtering, still very less number of ISPs have deployed that. Mechanisms like hash based traceback leads to many management issues, which in current scenario doesn't seem to be working. Mechanisms are there which talks about single packet traceback, but there are lots of overheads for such methods.

References Références Referencias

1. http://en.wikipedia.org/wiki/IP_traceback
2. IP Traceback: A New Denial-of-Service And different IP hacking approaches from google search engine.
3. http://cseweb.ucsd.edu/~savage/papers/Ton01.pdf: "Different :IPtraceback approaches"
4. G. Jin and J. Yang, "Deterministic Packet Marking Based on Redundant Decomposition for IP Traceback," IEEE Comm. Letters,vol. 10, no. 3, pp. 204-206, 2006.
5. Belenky and N. Ansari, "IP Traceback with Deterministic Packet Marking," IEEE Comm. Letters, vol. 7, no. 4, pp. 162-164, 2003.
6. Y. Xiang, W. Zhou, and J. Rough, "Trace IP Packets by Flexible Deterministic Packet Marking (FDPM)," Proc. IEEE Int'l Workshop IP Operations and Management (IPOM '04), pp. 246-252, 2004.
7. H. Farhat, "Protecting TCP Services from Denial of ServiceAttacks," Proc. ACM SIGCOMM Workshop Large-Scale AttackDefense (LSAD '06).
8. H. Aljifri, "IP Traceback : A New Denial-of-Service Deterrent,"IEEE Security and Privacy, vol. 1, no. 3, pp. 24-31, 2003.
9. Study on Flexible Deterministic Packet Marking An IP Traceback System - 1.IJAEST-Vol-No-9-Issue-No-1-A-Study-on-Flexible-Deterministic-Packet-Marketing-An-IP-Traceback-System-001-007.pdf.
10. M. Adler, "Trade-Offs in Probabilistic Packet Marking for IP Traceback," J. ACM, vol. 52, no. 2, pp. 217-244, 2005.

This page is intentionally left blank

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 13 Issue 3 Version 1.0 Year 2013
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Multi Attacker Collision Analysis in MANETs using Conditional likilihood

By Nitta Rajkiran

Abstract - Mobile ad hoc networks will aim to provide services to the wireless network without depending on any fixed infrastructure There are basically two approaches to motivate players: 1) by denying service to misbehaving players by means of a reputation mechanism or 2) by remunerating honest players, using for example a micropayment scheme. In these works, malicious players are modelled as never cooperative, without any further sophistication, since their main focus was discouraging selfish players. There is no degree of selfishness that can approximate the behaviour of malicious players. This work will focus on multi-attacker collusion in the regular/malicious player game. The Proposed System also model the regular/malicious player game as a multistage dynamic Bayesian signalling game to find the optimal strategy of regular and malicious players. Apart from that utility function, degree of selfishness of a player and degree of uncertainty are also considered.

Keywords : *bayesian signaling game, game theory, mobile ad hoc networks (MOBILE AD HOC NETWORKS), mobility, reputation systems, sequential rationality, uncertainty.*

GJCST-E Classification : *C.2.m*

Strictly as per the compliance and regulations of:

Multi Attacker Collision Analysis in MANETs using Conditional Likilihood

Nitta Rajkiran

Abstract - Mobile ad hoc networks will aim to provide services to the wireless network without depending on any fixed infrastructure There are basically two approaches to motivate players: 1) by denying service to misbehaving players by means of a reputation mechanism or 2) by remunerating honest players, using for example a micropayment scheme. In these works, malicious players are modelled as never cooperative, without any further sophistication, since their main focus was discouraging selfish players. There is no degree of selfishness that can approximate the behaviour of malicious players. This work will focus on multi-attacker collusion in the regular/malicious player game. The Proposed System also model the regular/malicious player game as a multistage dynamic Bayesian signalling game to find the optimal strategy of regular and malicious players. Apart from that utility function, degree of selfishness of a player and degree of uncertainty are also considered.

Keywords : *bayesian signaling game, game theory, mobile ad hoc networks (MOBILE AD HOC NETWORKS), mobility, reputation systems, sequential rationality, uncertainty.*

I. Introduction

Manets is the self organizing nature without relaying on any fixed infrastructure. The beautiful nature of the mantes is their topology is dynamic. They do not fallow any fixed topology in nature. As we know that in the network their two kinds of nodes. Malicious nodes other are regular. The malicious nodes always tend to attack other nodes and alter the data or waste the resources. We can consider this as a wrestling scenario between the two. There are so many approaches to find the malicious nodes. But we have taken the game theory to find the malicious nodes because game theory is the study of wrestling between the nodes. In the game theory everything is probality based. We shall be considering the scenario between the two players as a game. At the time of playing the game we usually intend to know strategy of other player. But we always land up in half knowledge about the other player i.e. the strategy of the opposite player is not completely known, that concept is called as baysion signalling game. At the time of playing we keep mentoring other players, that concept is know is neighbouring monitoring. As we malicious nodes always tend to attack and keep fleeing to avoid punishment. So what it does is it goes to the other network and attack or cooperate with the other nodes at some point i.e. is the threshold point the malicious nodes get caught. Normal players will aim to focus with their resources on cooperating with regular nodes and do not accept the requests of from suspicious neighbouring and keep reporting when the neighbouring is considered to be malicious. Both regular and malicious nodes' best responses are guided by threats about certain reactions from other players. [1] Such threats are dependent on their current beliefs. [1] The regular node sets a reputation threshold and judges other nodes' types based on the evaluated belief and this threshold. [1] The malicious node continuously evaluates the risk, which is decided by the possibility that a regular node would choose to report under current conditions. [1] On the basis of the risk and expected fleeing cost, the malicious node makes a decision on fleeing. [1] The contributions of this paper are as follows: 1) We had theorized a Bayesian game framework to understand and study the strategy of regular and malicious nodes in MANETs; 2) we will be simulating it for multiple and single attacker for regular nodes to report and malicious nodes to flee [1].

Author : Computer Science/M.Tech Bangalore, 560097, India.
E-mail : rajkiran8630@rediffmail.com

II. Related Work

In the existing work most of the game theory is based on single attacker and multiple individual attacker. So in general those attackers will not co-operate with each other so the strategy of every attacker is independent of other. In the existing work most of the game theory is based on single attacker and multiple attacker. So in general those attackers will not co-operate with each other so the strategy of every attacker is independent of other. The payoff for players to cooperate are analyzed and presented in [1]–[3]. Well, in this works, malicious players are structured as never cooperative, since there main motive is to discouraging players which are stingy. As we know that the good players' behaviour in [5] is simple, and it fails to consider the possibility that an attacker can choose different attack frequencies toward different opponents depending upon the requirement [26]. There can be no degree of stingy that can approximate the attitude of malicious players. In this, we have modelled the malicious players with their own functions of utility, which will be different from regular players. In other sense, we will assume that malicious players are also rational concerning their goals.

In recent works we studied the payoff for malicious players and simulated their behaviour more rationally. In [4], Liu *et al.* present a general incentive-based method to model the attackers' intents, objectives, and strategies. In [5], Theodorakopoulos and Baras further study the payoff of the malicious players and identify the influence of the network topology.

We consider malicious players, making the malicious and regular players' game in this paper more and more interesting. Game theory [6] is a powerful tool in modelling interactions among self-interested players and predicting their choice of strategies [7]–[10]. Therefore, wireless ad hoc networks [11]–[13] are more often studied using game theory [26]. The equilibrium of the contention window game is studied in [13] [26]. In the previous work they have simulated for single attacker using the PBE strategy with other strategy and found that PBE works much better compared to other. But in the current work we have taken same PBE strategy for multiple attackers and found that belief, disbelief and uncertainty is much efficient to find the malicious nodes by comparing with single attacker [26].

III. Proposed Model

Some how this type of attacker model may not create to serious theats in the data transmission so this will give flexi able sometimes equal probality to attack or flee. Because of probality it is not possible to predict the strategy of the attacker. If the attacker drops problity is equal to overcome these limitations there is a need to introduce cryptographic technique as well as considerations of multiple collisions attackers model.

To specify the collision attacker we need to consider conditional probity as well as lo likili hood of the player's strategy. According the the conditional probility we can verify the strategy of a player for given class where class indicates the evidence already we having so there reprentation is given by P(x|c). In the above representation x specifies strategy of current player and c represents the total strategic the game. Likili hood specifies for given behaviour to a given class. In this paper we are also applying condition probility and likilihood between players also by applying the condition probility between the two players specifies what the level of support coming from other player is. Based on this assumption we can divide the player into two groups 1) specifies high transmission error rate and other group specifies high packet delivery ratio. Based on the probility in the error transmission group we can also say that those players are playing the game with co-operation. This will be treated as collision attacker with respect to the high transmission error group. To achieve this there is need to monitor and record the activates of each players throughout the game. If the player is a new comer in the game than is a need to find the likilihood of the player. Likili hood calculate involves behaviour of the player so that there is a need to verify the behaviour against the available strategy.

Apart from the pure probility theory there is a need to provide cryptographic solution for path security. We need to incorporate digital signature for the strategy of a every player as well as digital signature for the control packets. Every time we are reading route request and route reply we need to verify the signature of those packets. This very much useful when the attackers are try to introduce wormhole attack in the given path.

a) Neighbour Observing

By exploring the nature of broadcast intercommunication in wireless network, players will track the outgoing of packets from one-hop neighbours through passive observation. But, a player will able to differentiate whether a failure in communication is caused by its opposite player A or D[26]. Therefore, an detail observation will be classified as either a detected *C* or a detected *A/D*. The correspond discrete variable namely α for detected *C* and β for detected *A/D*, will be incremented as shown in Fig. 1(b). This mechanism is called neighbour monitoring [24] [26]. In practical MOBILE AD HOC NETWORKs, the detection process has challenges. First, the malicious player can disguise itself. Second, the unreliability and the wireless channelizes bring more uncertain to the observing to the process [26]. The schemes which ignore the noise in the observation may not be practical in the actual wireless intercommunication. We assume that the bugs in the observation will occur with low probability. Else it would be impossible to distinguish a malicious player by Neighbour observing.

b) Decision Reckon

We analyze the MOBILE AD HOC NETWORK to find the best decision rules and action by using the dynamic Bayesian game framework Fig. 1(b) shows the process of regular and malicious players to take decision. The regular player obtains feedback from its neighbor observing and calculates the belief and sufficiency of evidence toward the opposite player based on the α and β values. It follow threshold rules to decide whether to report or not. If not the regular player will choose *C* with a probability *p*, which is calculated based on its belief [26]. The malicious player calculates the risk of being caught. It follows rule to decide whether to flee or not depending on the threshold. If else, the malicious player chooses *A* with a probability φ.

c) Bayesian Signalling Game

A signaling game is a dynamic, Bayesian game with two players, the sender (S) and the receiver (R). The sender has a certain type, t, which is given by nature.[1] (The sender observes his own type while the receiver does not know the type of the sender.[1] Based on his knowledge of his own type, the sender chooses to send a message from a set of possible messages M = {m_1,

m_2, m_3,..., m_j} [1]. The receiver observes the message but not the type of the sender. Then the receiver chooses an action from a set of feasible actions A = {a_1, a_2, a_3,...., a_k}. The two players receive payoffs dependent on the sender's type, the message chosen by the sender and the action chosen by the receiver. A related game is a screening game where rather than choosing an action based on a signal, the receiver gives the sender proposals based on the type of the sender, which the sender has some control over [1] [26].

The equilibrium concept that is relevant for signaling games is Perfect Bayesian equilibrium. Perfect Bayesian equilibrium is a refinement of Bayesian Nash equilibrium, which is an extension of Nash equilibrium to games of incomplete information. Perfect Bayesian equilibrium is the equilibrium concept relevant for dynamic games of incomplete information) [1] [26].

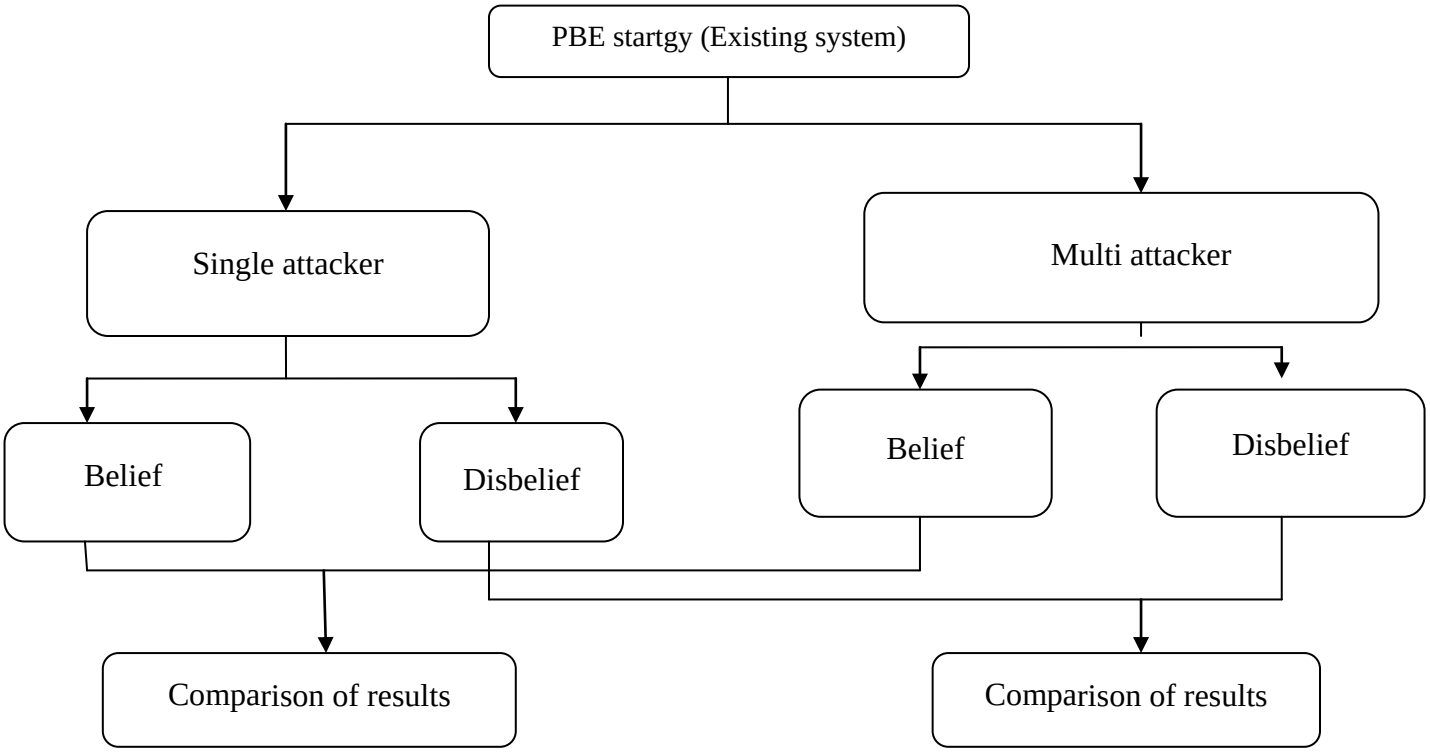


Figure 1(b)

By seeing the above block diagram we can find the flow of the game. In the above diagram first the regular node decides to cooperate or not if it fails to do so Beta value will be incremented else alpha value will be incremented if it alpha it will calculate the trust if the threshold is reached it will be reporting else the process keeps continuing else if it is a malicious nodes it will tracks the regular node trust and evaluate the risk of being caught and it estimates the risk i.e. if the risk is greater than flee cost than it will flee else it will attack. at last end of the game.

IV. PBE

The PBE of this game describes the optimal decision rules for both regular and malicious players and reveals the connection between the best strategy profile and the cost and gain of individual strategies [26]. From the discussion, we can summarize player *j*'s PBE strategy σ^*j as strategy profile 1. The regular type player *i* has the same PBE strategy profile as *j*, and the PBE strategy σ^*i of malicious-type player *i* is listed as strategy profile [26].

V. Experimental Results and Analysis

All proposed have been implemented and compared on a discrete event simulator. All simulations are conducted in randomly generated MOBILE AD HOC NETWORKs. The regular player can track its neighbor's outgoing packets by neighbour monitoring. We have taken 10 players to 50 players and made 10 iterations for each player are randomly placed in a 900 m ×900 m region which is evenly divided into clusters. The transmission range is 50 m. Any two players within the same cluster are considered as neighbours. Players follow the cluster based mobility model [25]. It shows this mobility model for players in Fig. 1(a). It is the probability that regular players in cluster *Cx* will move to cluster *Cy*. The minimum number of malicious players is 1.

VI. Comparison with Previous Schemes

In this section, we compare the performance of the proposed scheme with those for the previous schemes, namely Yinying Yang [25], Jie Wu [25]. The comprations are made with single attacker vs multiple attackers and found the results were much better with multiple attackers than single attacker as shown in the table 2 the proposed approach of multiple attackers is compared with previous approaches.

No of nodes	Belief wrt multi-attacker	Belief wrt single attacker
10	0.222	0.634
20	0.852	0.919
30	0.222	0.222
40	0.852	0.936
50	0.412	0.412
60	0.833	0.852
70	0.412	0.412
80	0.833	0.852
90	0.222	0.412
100	0.833	0.747

Table 1

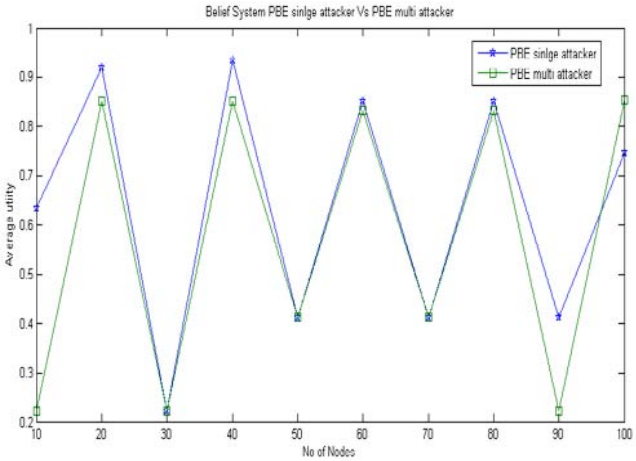


Figure 2 : Shows the comparations with single attacker with multi-attacker

The values in the above table taken by considering the belief system of multi attacker and single attacker and found that graph 3 for belief system for multi attacker increases but the graph for the single attacker slowly decreasing with respect of nodes and the graph is plotted which is show in the fig 2.

No of nodes	Disbelief Belief wrt multi-attacker	Disbelief Belief wrt single-attacker
10	0.111	0.111
20	0.137	0.137
30	0.111	0.111
40	0.137	0.126
50	0.137	0.111
60	0.312	0.137
70	0.126	0.111
80	0.412	0.137
90	0.111	0.111
100	0.137	0.216

Table 2

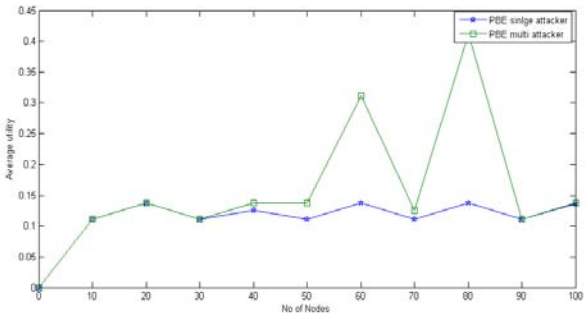
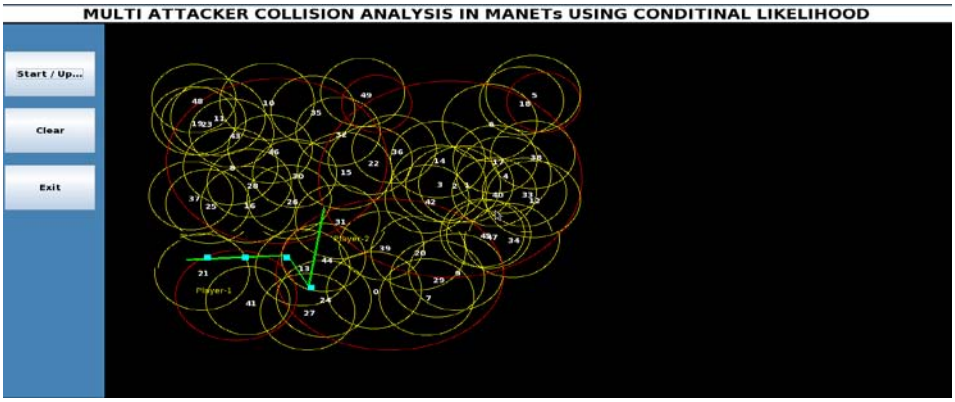


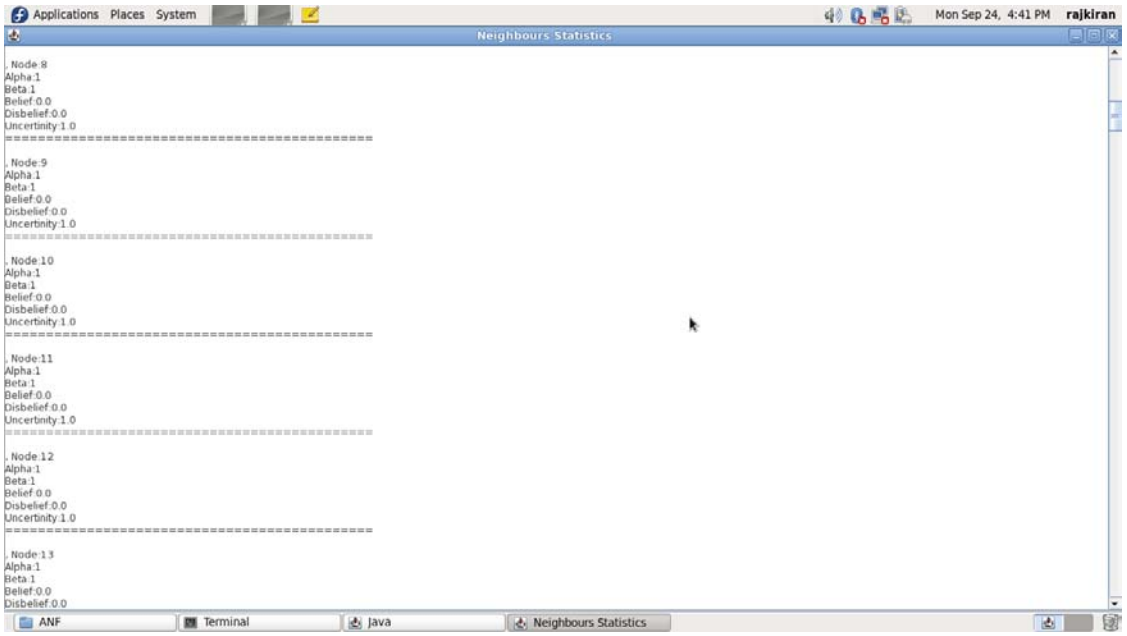
Figure 3 : Shows the comparations of disbelief of single attacker with respect multiattacker

In the figure 3 it shows the comparations of disbelief of single attacker with multi attacker and found that disbelief keeps increasing and decreasing.

Screen Shots



The above pic its shows the screen shots for 100 nodes simulated on the JNS



In the above screen shots it shows the values taken at the time of iteration

VII. Conclusion

The proposed system is simulated in java network animator and found that the results were good and efficient compared to the previous approach. In this paper, there is need to enhance the by introducing probality decision tree classification of data mining to predict behaviour of the players to increase the accuracy.

References Références Referencias

1. Blanc, Y. Liu, and A. Vahdat, "Designing incentives for peer-to-peer routing," in *Proc. IEEE INFOCOM,* 2005, pp. 374–385.
2. L. Buttyan and J. Hubaux, "Stimulating cooperation in self-organizing mobile ad hoc networks," *ACM Mobile Netw. Appl.,* vol. 8, no. 5, pp. 579–592, Oct. 2003.
3. M. Felegyhazi, J. Hubaux, and L. Buttyan, "Nash equilibria of packet forwarding strategies in wireless ad hoc networks," *IEEE Trans. Mobile Comput.,* vol. 5, no. 5, pp. 463–476, May 2006.
4. P. Liu, W. Zang, and M. Yu, "Incentive-based modeling and inference of attacker intent, objectives and strategies," *ACM Trans. Inf. Syst. Secur.,* vol. 8, no. 1, pp. 78–118, Feb. 2005.
5. G. Theodorakopoulos and J. Baras, "Malicious users in unstructured networks," in *Proc. IEEE INFOCOM,* 2007, pp. 884–891.
6. D. Fudenberg and J. Tirole, *Game Theory*. Cambridge, MA: MIT Press, 1991.
7. R. Axelrod and W. Hamilton, "The evolution of cooperation," *Science,* vol. 211, no. 4489, pp. 1390–1396, Mar. 1981.
8. P. Nuggehalli, M. Sarkar, K. Kulkarni, and R. Rao, "A game-theoretic analysis of QoS in wireless MAC," in *Proc. IEEE INFOCOM,* 2008, pp. 1903–1911.

9. S. Ng and W. Seah, "Game-theoretic model for collaborative protocols in selfish, tariff-free, multihop wireless networks," in *Proc. IEEE INFOCOM,* 2008, pp. 216–220.
10. S. Sarkar, E. Altman, R. El-Azouzi, and Y. Hayel, "Information concealing games," in *Proc. IEEE INFOCOM,* 2008, pp. 2119–2127.
11. X. Liu, G. Noubir, R. Sundaram, and S. Tan, "SPREAD: Foiling smart jammers using multi-layer agility," in *Proc. IEEE INFOCOM,* 2007, pp. 2536–2540.
12. Y. Liu, C. Comaniciu, and H. Man, "A Bayesian game approach for intrusion detection in wireless ad hoc networks," in *Proc. ACM Game Nets,* p. 4.
13. L. Chen and J. Leneutre, "Selfishness, not always a nightmare: Modeling selfish MAC behaviors in wireless mobile ad hoc networks," in *Proc. IEEE ICDCS,* 2007, p. 16.
14. S. Buchegger and J. Boudec, "A robust reputation system for P2P and mobile ad-hoc networks," in *Proc. 2nd Workshop Econ. Peer-to-Peer Syst.*, 2004, pp. 403–410.
15. P. Michiardi and R. Molva, "CORE: A collaborative reputation mechanism to enforce player cooperation in mobile ad hoc networks," in *Proc. Commun. Multimedia Secur.,* 2002, pp. 107–121.
16. S. Buchegger and J. Boudec, "Performance analysis of the confidant protocol," in *Proc. ACM MobiHoc,* 2002, pp. 226–236.
17. S. Bansal and M. Baker, "Observation-based cooperation enforcement in ad hoc networks," Stanford Univ. Press, Stanford, CA, Tech. Rep. (CoRRcs.NI/0307012), 2003.
18. F. Li and J. Wu, "Mobility reduces uncertainty in MOBILE AD HOC NETWORKs," in *Proc. IEEE INFOCOM,* 2007, pp. 1946–1954.
19. Josang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *Decis. Support Syst.,* vol. 43, no. 2, pp. 618–644, Mar. 2007.
20. F. Li, A. Srinivasan, M. Lu, and J. Wu, "Uncertainty mitigation for utility-oriented routing in MOBILE AD HOC NETWORKs," in *Proc. IEEE GLOBECOM,* 2007, pp. 427–431.
21. F. Li and J. Wu, "Hit and run: A Bayesian game between malicious and regular players in mobile networks," in *Proc. IEEE SECON,* 2008, pp. 432–440.
22. V. Srinivasan, P. Nuggehalli, C. Chiasserini, and R. Rao, "Cooperation in wireless ad hoc networks," in *Proc. IEEE INFOCOM,* 2003, pp. 808–817.
23. E. Altman, A. Kherani, P. Michiardi, and R. Molva, "Non-cooperative forwarding in ad hoc networks," INRIA, Sophia-Antipolis, France, Tech. Rep. RR-5116, 2004.
24. S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehaviour in mobile ad hoc networks," in *Proc. ACM MobiCom,* 2000, pp. 255–265.
25. W. Hsu, T. Spyropoulos, K. Psounis, and A. Helmy, "Modeling timevariant user mobility in wireless mobile networks," in *Proc. IEEE INFOCOM,* 2007, pp. 758–766.
26. Feng Li, Yinying Yang, Jie Wu," Attack and Flee: Game-Theory-Based Analysis on Interactions among Nodes in MANETs', in Proc. IEEE.

Global Journals Inc. (US) Guidelines Handbook 2013

www.GlobalJournals.org

FELLOW OF ASSOCIATION OF RESEARCH SOCIETY IN COMPUTING (FARSC)

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

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

MEMBER OF ASSOCIATION OF RESEARCH SOCIETY IN COMPUTING (MARSC)

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

AUXILIARY MEMBERSHIPS

ANNUAL MEMBER

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

PAPER PUBLICATION

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

Process of submission of Research Paper

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

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

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

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

(II) Choose corresponding Journal.

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

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

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

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

Preferred Author Guidelines

MANUSCRIPT STYLE INSTRUCTION (Must be strictly followed)

Page Size: 8.27" X 11'"

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

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

1. General,

2. Ethical Guidelines,

3. Submission of Manuscripts,

4. Manuscript's Category,

5. Structure and Format of Manuscript,

6. After Acceptance.

1. GENERAL

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

Scope

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

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

2. ETHICAL GUIDELINES

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

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

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

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

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

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

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

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

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

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

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

Please mention proper reference and appropriate acknowledgements wherever expected.

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

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

3. SUBMISSION OF MANUSCRIPTS

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

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

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

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

4. MANUSCRIPT'S CATEGORY

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

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

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

Research articles: These are handled with small investigation and applications.

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

5. STRUCTURE AND FORMAT OF MANUSCRIPT

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

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

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

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

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

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

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

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

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

(h) Brief Acknowledgements.

(i) References in the proper form.

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

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

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

Format

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

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

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

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

Structure

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

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

Abstract, used in Original Papers and Reviews:

Optimizing Abstract for Search Engines

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

Key Words

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

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

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

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

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

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

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

Acknowledgements: Please make these as concise as possible.

References

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

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

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

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

Tables, Figures and Figure Legends

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

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

Preparation of Electronic Figures for Publication

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

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

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

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

6. AFTER ACCEPTANCE

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

6.1 Proof Corrections

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

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

(Free of charge) from the following website:

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

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

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

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

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

6.3 Author Services

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

6.4 Author Material Archive Policy

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

6.5 Offprint and Extra Copies

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

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.

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

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

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

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

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

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

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

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

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

INDEX

R

S

T

U

V

W

save our planet

Global Journal of Computer Science and Technology

Visit us on the Web at www.GlobalJournals.org | www.ComputerResearch.org
or email us at helpdesk@globaljournals.org

ISSN 9754350