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

Global Journal

of Computer Science and Technology: E

Network, Web & Security

Highlights

Sensor Information

Replication in Mobile Ad-hoc

RSA for Security

Security & Management

Discovering Thoughts, Inventing Future

VOLUME 13 ISSUE 15 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 15 (Ver. 1.0)

Open Association of Research Society

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

Global Journals Inc.

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

Sponsors: *Open Association of Research Society*
Open Scientific Standards

Publisher's Headquarters office

Global Journals Headquarters
301st Edgewater Place Suite, 100 Edgewater Dr.-Pl,
Wakefield MASSACHUSETTS, Pin: 01880,
United States of America
USA Toll Free: +001-888-839-7392
USA Toll Free Fax: +001-888-839-7392

Offset Typesetting

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

Packaging & Continental Dispatching

Global Journals
E-3130 Sudama Nagar, Near Gopur Square,
Indore, M.P., Pin:452009, India

Find a correspondence nodal officer near you

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

eContacts

Press Inquiries: *press@globaljournals.org*
Investor Inquiries: *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)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Contents of the Volume

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 13 Issue 15 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

Replication in Mobile Ad-hoc Network using Hopfield Network

By Tanu Chawla & Dr. Mukesh Kumar
The Technological Institute of Textile & Sciences, India

Abstract- Mobile Ad hoc Network (MANET) is a network comprises of mobile nodes connected without any centralized administration. Each node in the network has the ability to share a large number of objects with other nodes. The nodes are connected with other nodes to forward a message to other nodes until the search for node that desire meets. This paper represents a new replication method to recover the performance in distributed system. Objects are replicated on different nodes in the network to minimize the search for an object. It is observed that mobility of nodes predicted using SOM (Self Organizing Maps) technique provides less accuracy. This paper represents an algorithm that uses the network parameters as input condition to replicate objects into the nodes. The decision for each node will be taken by gathering the input conditions and feed to the Hopfield Neural Network. It is view that it will provide more accuracy and improve the performance.

Keywords: hop field network, mobile ad hoc networks, neural networks, replication, routing, routing protocols.

GJCST-E Classification : C.2.0

Strictly as per the compliance and regulations of:

Replication in Mobile Ad-hoc Network Using Hopfield Network

Tanu Chawla [α] & Dr. Mukesh Kumar [σ]

Abstract- Mobile Ad hoc Network (MANET) is a network comprises of mobile nodes connected without any centralized administration. Each node in the network has the ability to share a large number of objects with other nodes. The nodes are connected with other nodes to forward a message to other nodes until the search for node that desire meets. This paper represents a new replication method to recover the performance in distributed system. Objects are replicated on different nodes in the network to minimize the search for an object. It is observed that mobility of nodes predicted using SOM (Self Organizing Maps) technique provides less accuracy. This paper represents an algorithm that uses the network parameters as input condition to replicate objects into the nodes. The decision for each node will be taken by gathering the input conditions and feed to the Hopfield Neural Network. It is view that it will provide more accuracy and improve the performance.

Keywords: hop field network, mobile ad hoc networks, neural networks, replication, routing, routing protocols.

I. Introduction

Due to increase in the demand of the computers in our daily life, it increases the demand of connectivity. Through connectivity of various nodes in the network, these nodes in the network can easily share their data or objects. Wired network have been used for a long time. Due to some restrictions of wired network, requirement for the wireless network has been increased for sending messages, emails and communicate with other. So Mobile Ad-hoc Network (MANET) have been developed which comprises of a large number of nodes. In mobile ad-hoc network, nodes can communicates with the other nodes without any need of central administration or base station [2]. MANET is commonly used for all purpose like offices for doing work and colleges for maintain details.

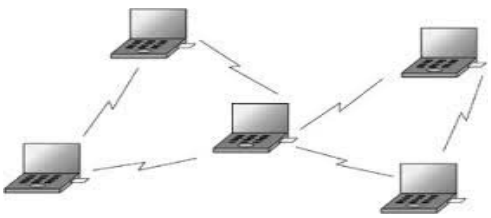


Figure 1 : Example of Mobile Ad hoc Network with having five nodes.

Authors α σ: Computer Science & Engineering Department, The Technological Institute of Textile & Sciences, Bhiwani- 127021, India. e-mails: tanuchawla15@rediffmail.com, drmukeshji@gmail.com

So today demand for the ad-hoc network enhances. Mobile Ad-hoc Network is an autonomous system of mobile routers which are connected with the wireless links and easily communicate with each other. Each node has the ability to move freely in the network at any place. In Mobile ad-hoc network, each node communicates with its neighbours by forward a query message and establishes the communication between them [3].

This shows that every node acts as a host as well as a router [4]. Such a network may be used for the large number of nodes. So this network is a multi-hoped communication network. In this network, the routing protocols are used to transmit the data between the nodes in the network. MANET is used in many applications such as military services, healthcare [1]. Inside the wired network, when one node goes outside from the network, then it disturbs the whole network and the problem will not easily solved. So these days, people prefers to wireless network

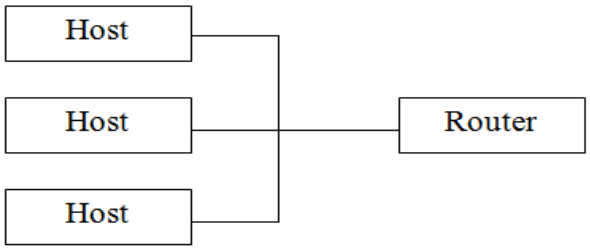


Figure 2 : Block Diagram of Mobile nodes that are act as a host as well as router.

Mobile ad-hoc network is a wireless network topology which is commonly used now-a-days. It consists of a large number of nodes that are linked with each other and share the objects between them. There are a large number of characteristics of MANET [2]. Some of these are summarized as below:

i. Nodes can perform the role of host as well as router.
ii. There is no need of centralized controller and infrastructure.
iii. MANET provides limited security.
iv. This network can be set up anywhere.
v. MANET is a dynamic network topology.
vi. Communication is done without the need of wires.

II. Overview On Data Replication

Data replication is a most useful technique is commonly used today. It is used for improving reliability,

scalability, fault-tolerance and accessibility of data services [6]. It is a technique stored on the multiple locations which reduce the search size. To be most useful, data replication should be invisible to the user. The main improvement of using replication is that if you change only single copy of the data that presents in one node then data available on other nodes changes automatically. This solves a large number of problems. So replication is commonly used.

Maintaining various copies of data is one of the most successful ways to stay away from database availability problems. After failure produced in one database, then you have the ability to use another local copy of the database or you can also competent of use the copy of the database that are present on other site. In networking, replication is well thought-out as a most important method to extend reliability [7].

III. Overview on Artificial Neural Network

Artificial Neural Network (ANN) is a computing system consists of a large number of processing elements which are used to take inputs and then processing takes place and then gives response to the inputs [8]. A large Neural Network consists of a large number of processing elements [9].

Neural network is made up of a number of layers. Layers are prepared by a number of interconnected nodes which include an activation function. Patterns are represented in the network as the input layer, which has links to one or more 'hidden layers' and input layer communicates with middle layer known as hidden layer. In the hidden layer, processing is done through a number of weighted connections. The hidden layer directly linked to an output layer which has the capability to gives response to all the inputs [10].

IV. Role of Replication in Manet

Replication is one of the most important techniques is most commonly used in MANET which allow the nodes to come apart the objects between them. The objective of this technique is to care for a number of object replicas in excess of the time before a node exits in decentralized and amorphous environment [11]. That is the reason that shows the need to replicate objects on the number of nodes that are linked to one another in the network, which is necessary [13].

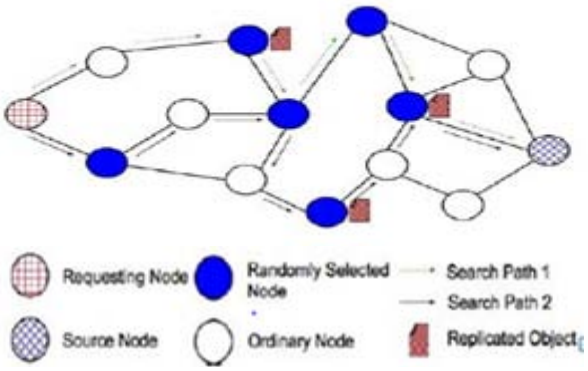


Figure 3 : Shows the replication of nodes in the network.

V. Related Work

We observe a large number of replication techniques that are most commonly used. Some of them are: reactive and proactive replication. Reactive replication is the generally used algorithm. **In reactive replication**, the requesting node has the copy of the object from the source node. After completion of the search, a copy of object is produced into the node where the query was generated. In this type of replication overhead is higher. But the main advantage of using this technique is that it minimizes the storage for replicas, so it provides better results. The only problem with this replication method is more overhead.

In proactive replication, the object is replicated from the node that is requested to the node that is provided only in the selected nodes. Sometimes it is copied along the complete path of the successful query from source node to requested node. It is called as the path replication. After the completion of the query, replication of object is takes place in the complete path from source node to node that are requested [13]. Beyond that a new third type of replication algorithm is developed known as "**random replication**". In random replication, beyond the enquiry is completed, the objects are copied randomly in selective nodes along the path from the requester to the requested node.

VI. Problem Overview

A network consists of a large number of nodes. Each node in the network has the ability to share their objects with other nodes [1]. By using one of the different kinds of search techniques, the location of the data is retrieved. A query for the certain object is initiated to perform the search among nodes. These nodes are linked with one another forward a request message from one node to another node until a search for a certain object is completed. The queries were processed on each node from source node to requested node. The message passes to the various nodes through connection between them until the node that is requested is determined. The nodes which are

used to forward a message from source node to request node is known as the path. The shorter path length has more performance than a longer path.

Replication method is the one of the method to get a good performance in a search on a distributed system [13]. This paper also calculates the predictability of the nodes. The main benefit of mobility prediction is to assign next access point before the mobile terminal leaves its current one which reduces the intrusion time in communication between terminal mobiles. Prediction is implemented using SOM (Self Organizing Maps) technique [13]. But that offers less accuracy. This paper implements new prediction technique which is Hopfield Neural Network technique used in MANET that will offer high accuracy and provide high performance.

VII. Proposed Algorithm

This algorithm is used to replicate the objects randomly on the nodes after the successful search to reduce our search and time and improve the performance of the system. This algorithm depends upon the theory of finding the conditions of the nodes that are moves out of network. According to this scheme, when a request for a certain object is created, and previously it is to be found then this algorithm is used to randomly replicate the objects along the path from source node to the node that is requested. The proposed algorithm uses the hops as an input condition to make the decision for replicate objects into the nodes. The decision made by gathering the input parameters of each node and feed this input parameters into the Hopfield Network technique.

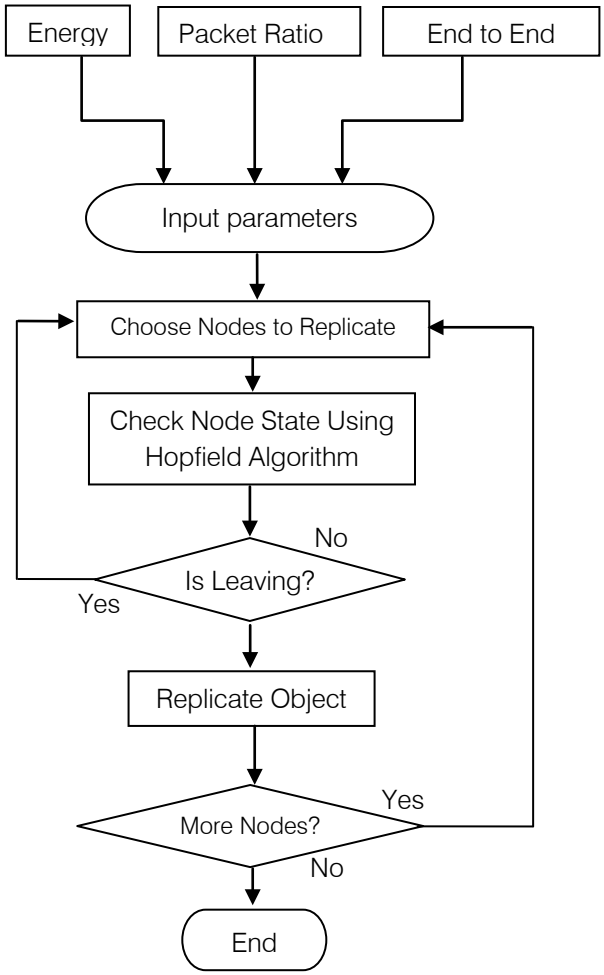
The various steps of the proposed algorithm are as follows:

1. Firstly, a set of input parameters such as packet ratio, energy and E2E delay are gathered as inputs.
2. Then the algorithm has to choose the nodes that are needed to replicate.
3. Then it checks the state of the node using Hopfield Network algorithm.
4. The output "0" is for nodes about to leave the network and "1" for those who have enough time to stay in the network.
5. Once a nodes category is specified, the copy of the requested object is placed for those nodes whose category is set to "1".
6. On the other hand, those nodes which contains the "0" category, the replication scheme ignores the replication of object on that node.
7. Then the category for the next node to be evaluated.
8. The method keeps on going until the requesting node in the random replication is reached.

VIII. Hopfield Network

Hopfield Network is a neural recurrent network which is used to classify input data into groups. The data is trained using the supervised learning. So it gives better performance than using SOM Algorithm.

Flow Chart of the proposed algorithm is



A set of input parameters are fed into Hopfield algorithm as input for each node to classify the input data into the groups. Only two categories of output are produced by Hopfield network for making decisions for the nodes. These are either "0" or "1". The number "0" indicates the nodes about to leave the network and "1" for those who are not going out from the network. When the search for all the data completed, then the random replication is used to replicate the objects randomly from the source node to requested node. It firstly checks the category of each node along the path by using the Hopfield algorithm. After the category for each node is explained, then replication scheme randomly copy the requested object for those nodes whose category is set to "1". On the other hand, the nodes which contain the "0" category, the replication scheme will not produce the replication of object for that node and check the category for the next node. The method keeps on going until the requesting node in the random replication is produced.

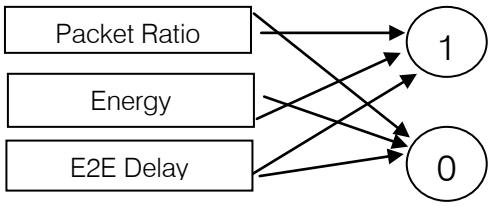


Figure 4 : Example of input parameters are given to the algorithm and produces only two outputs 0 and 1.

The inputs parameters for the nodes are distance energy and round trip time (RTT) and output contains only two values 0 or 1. This process is used for each node until the node that is requested is reached.

a) Distance

In the Mobile Ad-hoc Network, each node must be able to send a message to another node and able to establish the communication between them. Each node in the network sends the message to a node that it is linked is called initial node. The distance between two nodes is intended by using the simple equation which is expressed as:

$$D = \sqrt{[(x(i) - x(i+1))^2 + (y(i) - y(i+1))^2]}$$

Here D shows the distance between two nodes and i shows the initial node from which we want to calculate the distance and sqrt is a square root function which is used to calculate the square root of given value.

b) Round Trip Time (RTT)

The Round Trip Time is the return time measured by sending a packet from the local node to the isolated node. In this paper, this time is used to calculate the performance of the algorithm which is proposed. The Round Trip Time is evaluated by solving the simple equation which is expressed as:

$$RTT = (2*D)/C$$

Here RTT shows the Round Trip Time and D shows the distance between two nodes and C indicates the velocity of light and the velocity of light has the value $3*10^8$ m/s.

c) Energy

Each node in the network wants to communicate with the neighbouring nodes. Each node contains some energy. When the nodes communicate with neighbouring nodes, they consume some energy. Here energy factor is used to calculate the energy which is consumed when the nodes communicates with another nodes.

IX. Results

The performance evaluation of SOM and Hopfield Network was carried out using NS-2.34. For the experiments performed, a variable-size network of size 300 sq m was randomly generated with number of nodes typically in the range of 10-100. The power of the sensor radio transmitter was set so that any node within a 20 meter radius is within communication range and is called a neighbour of the sensor. Hopfield network provides better result than SOM Network.

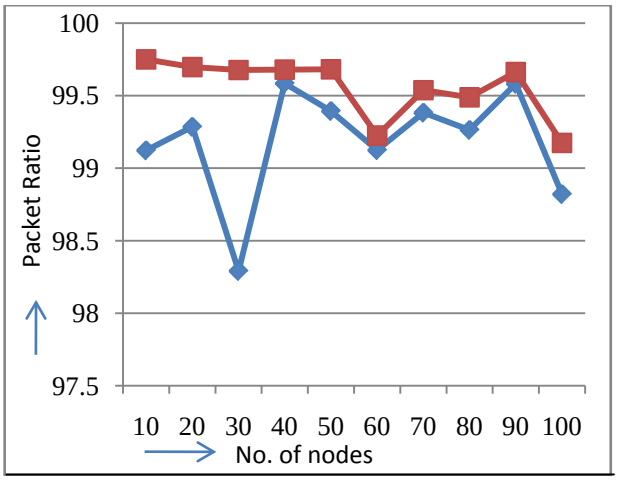


Figure 5 : Indicates the packet delivery ratio produced by SOM and Compare it with the packet ratio of new proposed Hopfield Algorithm.

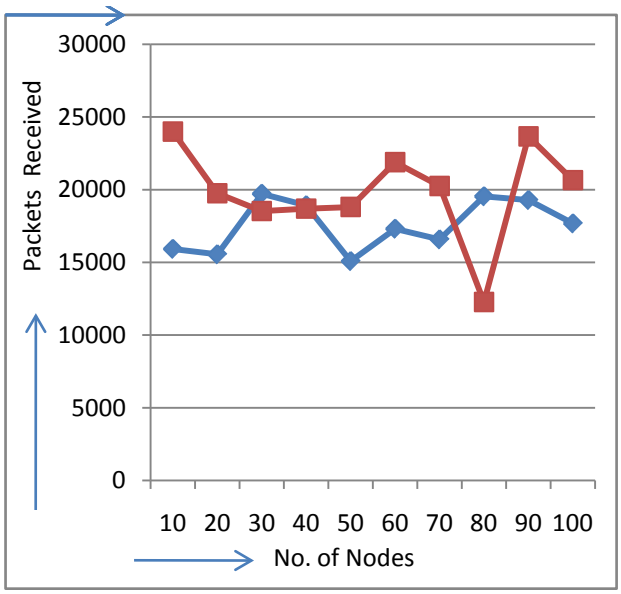


Figure 6 : Indicates the packets received by SOM and Compare it with the packets received by new proposed Hopfield Algorithm.

Table 1

For 100 Nodes in a Network	Packet Delivery Ratio	End to End Delay
Existing Algorithm	98.8202	474.827
Proposed Algorithm	99.1743	362.867

It shows the packet delivery ratio and E2E Delay generated by SOM Algorithm using 100 nodes and compares it with the packet delivery ratio and E2E Delay generated by Hopfield Algorithm.

Table 2

For 100 Nodes in a Network	Generated Packets	Received Packets
Existing Algorithm	17885	17674
Proposed Algorithm	20830	20658

It shows the Generated and Received Packets by SOM Algorithm using 100 nodes and compares it with the Generated and Received Packets by Hopfield Algorithm.

X. Conclusion and Future Work

This paper has proposed a scheme that is used for replicating objects on various nodes in a shapeless, self-configuring and self-motivated network, which randomly replicate the objects by determining the states of the node. If the status of the node is 1, which means that object is replicated for that node and status 0 indicates that object is not replicated for that node. For this, we proposed a new algorithm. The proposed algorithm tries to increase the accuracy and enhance the performance in MANET. As a result, data will be available at more nodes and it will be accessible vastly. Due to this, it will improve the performance of the network and provides more accuracy.

References Références Referencias

1. Che-Yu Liu, Isaac Woungang, Han-Chief Chao, Sanjay K. Dhurandher, Ting-Yun Chi, Mohammad S. Obaidat, "Security of Message in Multi-Path Ad Hoc Networks Using a Neural Network-Based Cipher", 2011, Fellow of IEEE and Fellow of SCS.
2. (2008) Rashmi: Mobile Ad-hoc Network [Online]. Available: http://MobileAdhocNetwork.htm.
3. P. Mukilan, A. Wahi, "CDRA: Consistency based Data Replication Algorithm of MANET",August 2012, International Journal of Computer Applications (0975 – 8887) Volume 51– No.14.
4. Heni Kaaniche and Farouk Kamoun, "Mobility Prediction in Wireless Ad Hoc Networks using Neural Networks", April 2010, Journal of Telecommunications Volume 2.
5. (1989) Dr. Robert Hecht-Nielsen: A Basic Introduction to Neural Network [Online]. Available: http://networkintroduction.com.
6. Marius Christian MAZILU, "Database Replication", Feb 2010, Database Systems Journal vol. I.
7. Matthias Wiesmann, Fernando Pedone and Andre Schiper and Bettina Kemme and Gustav Alonso, "Database Replication Techniques: a Three Parameter Classification", 2010, Research supported by EPFL-ETHZ DRAGON project.
8. Ani1 K. Jain, Jianchang Mao and K.M. Mohiuddinn, "Artificial Neural Network", March 1996, published in IEEE.
9. Hugo Larochelle, Yoshua Bengio and Jerome Louradour and Pascal Lamblin, "Exploring Strategies for Training Deep Neural Networks", published in Jan 2009, Journal of Machine Learning Research.
10. Carlos Baladron, Javier M. Aguiar, Lorena Calavia, Belén Carro, Antonio Sanchez- Esguevillas and Luis Hernandez, "Performance Study of the Application of Artificial Neural Networks to the Completion and Prediction of Data Retrieved by Underwater Sensors", Jan 2012, Published in ISSN 1424-8220.
11. Frank-Florian Steege and Horst-Michael Groß, "Comparison of Long-Term Adaptively for Neural Networks", 2012, Published in International Conference on Artificial Neural Networks.
12. Vorgelegt von, Jorg Hahner and Aus Dusseldorf, "Consistent Data Replication in Mobile Ad Hoc Networks", 2007, Published in IPVS.
13. Geofrey Cantara Soriano, Yoshiyori Urano, "Replication with State Using the Self-Organizing Map Neural Network", 2011, published in ICACT.
14. M. Pushpalatha, Revathi Venkatraman and T. Ramarao, "An Approach to Design an Efficient Data Replication Algorithm in Mobile Ad hoc Networks", May 2009, International Journal of Recent Trends in Engineering, Vol. 1, No. 2.
15. S.R. Das, R. Castaneda, and J. Yan, "Simulation-based performance evaluation of routing protocols for mobile ad hoc networks", Mobile Networks and Applications, 2000, 5, pp. 179-189.
16. R. Patil, A. Damodaram and R. Das, Cross layer AODV with position based forwarding routing for mobile ad-hoc network, Proc. of the 5th IEEE Conference on Wireless Communication and Sensor Networks, 2009.
17. S.-J. Lee and M. Gerla, "Dynamic load-aware routing in ad hoc networks", Proc. of IEEE International Conference on Communications, pp .3206-3210, 2001.
18. VINT Project, The NS Manual Formerly NS Document,http://www.isi.edu/nsnam/ns/ns-documentation.html, 2005.
19. Mueen Uddin, Azizah Abdul Rahman, Abdulrahman Alarifi, Muhammad Talha, Asadullah Shah, Mohsin Iftikhar and Albert Zomaya, "Improving Performance of Mobile Ad Hoc Networks Using Efficient Tactical on Demand Distance Vector (TAODV) Routing Algorithm", June 2012, International Journal of Innovative Computing, Information and Control Volume 8, Number 6.
20. Pravin Ghosekar, Girish Katkar, Dr. Pradip Ghorpade, "Mobile Ad Hoc Networking: Imperatives and Challenges", 2010, IJCA Special Issue on Mobile Ad-hoc Network.
21. C. Bisdikian, An overview of the Bluetooth wireless technology, IEEE Communication Magazine, December 2001.
22. J. Broch, D. A. Maltz, D. B. Johnson, Y. Hu, J. Jetcheva, A Performance Comparison of Multi-Hop

Wireless Ad Hoc network Routing Protocols, Proc. of MobiCom'98, Oct. 1998.
23. P. Sinha, R. Sivakumar, V. Bharghavan, CEDAR: a Core- Extraction Distributed Ad hoc Routing algorithm, IEEE INFOCOM'99.
24. E. R. Royer, C.-K. Toh, A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks, , IEEE Personal Communications, Apr. 1999.
25. V. D. Park and M. S. Corson, A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks, IEEE INFOCOM'97, 1997.

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 13 Issue 15 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

Efficient use of Mobile Agents for Network Security & Management

By S. V. Patil, Dr. S. D. Khamitkar & S. N. Lokhande
SRTM University, India

Abstract- Mobile agents have special characteristics which can help intrusion detection in several ways. The use of mobile codes and mobile agent based computing paradigms has been proposed in several researches till date. In this paper we try to present a scope for the possible association of Mobile Agents in the field of network security and management.

Keywords: *mobile agent, network security, intrusion detection.*

GJCST-E Classification : *C.2.0*

Strictly as per the compliance and regulations of:

Efficient use of Mobile Agents for Network Security & Management

S. V. Patil [α], Dr. S. D. Khamitkar [σ] & S. N. Lokhande [ρ]

Abstract- **Mobile agents have special characteristics which can help intrusion detection in several ways. The use of mobile codes and mobile agent based computing paradigms has been proposed in several researches till date. In this paper we try to present a scope for the possible association of Mobile Agents in the field of network security and management.**

Keywords: mobile agent, network security, intrusion detection.

I. Introduction

Mobile Agents are composition of computer software and data which migrates from one computer to another. While doing this, they continue their itinerary up to the home computer. Autonomy and mobility are main features of mobile agents, specifically mobile agent is a process where mobile agent moves from one environment to another environment, with remains data intact. Mobile agent it self decides when and where to move. When a mobile agent decides to move then they save their own state and this state transport to another host. Mobile agents are specific about mobile code and they are choose the host and also active in respect of execution [1,4].

Mobile agents have special characteristics which can help intrusion detection in several ways. The use of mobile code and mobile agents computing paradigms have been proposed in several researches. The advantages include: overcoming network latency, reducing network load, executing asynchronously and autonomously, adapting dynamically, operating in heterogeneous environments, and having robust and fault-tolerant behavior. Moreover implementation of mobile agents in languages such as JAVA, provides mobile agents with system and platform independence and considerable security features [1,7].

As computer network is a collection of autonomous connected computers and other communication devices used for sharing resources or computers uses wired or wireless links as transmission media. Network security is an important task that must be seriously considered when designing a network. Network security is defined as the policies and procedures followed by a network administrator to protect the network devices from threats and simultaneously the unauthorized users must be prevented from accessing the network[2]. Maintaining Network security is a broad subject means securing our network from unauthorized entity or Mal ware. The unauthorized entity may modify the information or accessing the network through remote computer may harm the network. Following are some network security measures,

1. ***Availability :*** The term Availability means that a node should maintain its ability to provide all the designed services regardless of the security state of it.
2. ***Integrity :*** Integrity guarantees the identity of the messages when they are transmitted.
3. ***Confidentiality :*** Confidentiality means that certain information is only accessible to those who have been authorized to access it.
4. ***Authenticity :*** Authenticity is essentially assurance that participants in communication are genuine and not impersonators.
5. ***Non repudiation :*** Non repudiation ensures that the sender and the receiver of a message cannot disavow that they have ever sent or received such a message.
6. ***Authorization :*** Authorization is a process in which an entity is issued a credential, which specifies the privileges and permissions it has and cannot be falsified, by the certificate authority.

II. Literature Review and Findings

In this section we are reviewing some literature related with Mobile agent and Network management and security. Once the mobile agent has migrated, the connection between the client and server is disconnected, later when mobile agent finishes its job at the server, then it will reconnect to the client or host. This clearly saves the network bandwidth especially in the wireless environment where disconnection is frequent and bandwidth play a major role[3]. A Mobile agent (MA) is a composition of computer software and data which is able to migrate (move) from one computer to another autonomously and continue its execution on the destination computer. Taking the recent development i.e. going to this field, mobile agent based intrusion detection system is an efficient way to the intrusion detection in the distributed environment. [4] . Mobile agents perform a task by migrating and executing on several hosts connected to the network. For the sniffer

Author α: Assistance Professor, Department of Computer Science, Rajshree Shahu College, Latur(MS). e-mail: svp11110@rediffmail.com
Author σ: Associate professor, School of Computational Sciences, SRTM University, Nanded (MS). e-mail: s_khamitkar@yahoo.com
Author ρ: Assistance Professor, School of Computational Sciences, SRTM University, Nanded(MS). e-mail: lokhande_sana@rediffmail.com

detection, the network administrator sends some special types of mobile agents in the network and collects information from different nodes. After analyzing this information the network administrator can identify the computer system running in promiscuous mode. [5] In [1] evaluate the implications of applying mobile agent technology to the field of intrusion detection and present a distributed intrusion detection system (IDS) based on mobile agents that considers large-scale network environment in order to monitor multiple hosts connected via a network as well as the network itself. Once system will be operational it will be the first comprehensive real–life application using mobile agents that will not only provide security to network resources but also provide security and protection to the mobile agents system itself. The system efficiently solves several problems with the existing IDS/IPS solutions: it can detect new vulnerabilities, it can process and filter large volumes of logs, it reacts to intrusions in real–time, provides protection against unknown attacks, supports and improves IDS/IPS commercial products by different vendors, and handles software patches. The system not only improves the existing IDS/IPS solutions, but it also eliminates several of their core problems. In addition, it is self protected by full encryption, both mobile agents and their platforms, and therefore not vulnerable to attacks against its own components and resources. [6]

III. Discussions on Network Security & Management using Mobile Agents

There exist many contemporary approaches for network security categorized as Host based and Network based. However, they work for Intrusion detection and not for overall security management. As mentioned earlier, Mobile Agents can be useful in such places where we need network security as well as network management. We can use different mobile agents for securing the network from the threats as well as detect the threats. For example, network sniffing detector mobile agent used to find the network sniffer program in the network. Mobile agents can be used in above context as follows:

a) ***Network load Reducing*** *:* Due to the multiple interactions in network, it creates excess network traffic. A mobile agent through the package conversation they dispatches the packets on the destination host at that time locally interaction happens and it helps to reduce the network load.

b) ***Overcome Network Latency*** *:* In real time systems, with the help of mobile agents overcome the network latency, because mobile agents dispatches from central controller and acts locally.

c) ***Tolerant to Network Faults*** *:* Without active connection between clients and server mobile agents can operate.

d) ***Encapsulate Protocols*** *:* When data is being exchanged in network at that time every host has a code, for this code needs protocols e.g. incoming and outgoing. When these protocols needs security at that time protocol code becomes heavy and creates problems. Mobile agents move on the remote host and using specific channels creates new protocols.

e) ***Execute Asynchronously and Autonomously*** *:* It is possible to embedded different tasks in the mobile agents and may be dispatched on the hosts. When agents are dispatched they becomes independent from the process and due to this mobile agents become asynchronous and autonomous.

f) ***Adapt Dynamically*** *:* Mobile agents have their own sense about execution environment, because they reacts autonomously with the changes. They solve specific problem in the network by their own.

g) ***They are Naturally Heterogeneous*** *:* Network computing is itself heterogeneous in respect of hardware and software; therefore mobile agents are also heterogeneous in nature. [7]

In case of network management, the Mobile agents assist to the network administrator to manage the network security. For security management mobile agent's team launched in the network this team visits to all the computers in the network and different services security software analyzes and install. For this mobile agents uses following techniques

1. Connectivity and states of remote hosts are checked and reported.
2. Configuration of remote hosts are cheeked and recorded.
3. Security configuration management related tasks are applied.
4. Mapping of snort rules and identified vulnerabilities.

For completing the above four function mobile agents team automating launched, these teams interact with the all system and install security tools on the remote hosts and complete the desired network security management tasks.

Similarly we can detect intrusions also. Intrusion detection is implemented by an intrusion detection system and today there are many commercial intrusion detection systems available. In 1987 Dorothy E. Denning proposed intrusion detection as is an approach to counter the computer and networking attacks and misuses. In general, most of these commercial implementations are relative ineffective and insufficient, which gives rise to the need for research on more dynamic intrusion detection systems[8].Mobile agents plays very important role in the network security. Mobile agent searches the malicious activity in the network, for these work mobile agents provides following three groups.

1. Analysis of large volume of data in various logs generation of effective reports.
2. Detection of and reaction to host based intrusion attempts in real time.
3. Detection of and reaction in real time of distributed intrusion attempts.

For completing the above three functions the different mobile agent teams assembled and launched. The capacity of these teams to analyses the logs, these logs created from sensors e.g. Snort, Osiris and MS Windows firewall which are present on the host computers.[6] Mobile agent reaches on the remote hosts, analyses the logs and if any serious problem then reports to the security administrator. At the same time second team of mobile agent reaches on the remote host and continuously snorts, monitor and analyze, if this team finds any suspicious activity calls the new mobile agents and lastly the third team of mobile agents detects intrusion activity.

Above case can be extended for Distributed systems also. Today, computer system has evolved into a distributed computing machine, nothing is static now, not even the security threats and attacks. The security issues are of high concern today. In the world of open environment problem faced widely by the computer system and network is the network intrusion. [4] Intrusion detection system is the security mechanism that gathers and analyses the information to detect unwanted attempts of accessing and manipulating the user and system activities and report it to the management section.

As an example, MAIDS was developed by Lowa State University is a distributed IDS based on mobile agent technology. It build a model for an intrusion activity with software fault tree analysis (SFTA), and transform the SFTA model into intrusion detection by the use of Colored Petri net (CPN). Intrusion detection in MADIS is not only relied on direct linked neighbors of a particular host but also other hosts in the network. In this way the original host can obtain more information to achieve a more accurate decision. Mobile agent may enhance the performance of IDS and even offer IDS some new capabilities, however these benefits is not easy obtained. We could learn from these existing system that there are three main research areas in IDS with mobile agent technologies, MAIDS can gather information not only from neighbors of the compromised hosts but from more other hosts in the network that can lead to more accurate final decision.[9]

IV. Conclusion

Mobile agent provides an interestingly new way of network security & management. However, the security, infrastructure and standardizing issues still represent significant constraints. The main thing from our findings is that mobile agent has the potential in increasing the performance of network management. Due to its nature of being an innovative way from the programming environment, but some work is still required.

References Références Referencias

1. Dr. Bhushan Trivedi , Jayant Rajput , Chintan Dwivedi and Pinky Jobanputra , "Distributed Intrusion Detection System using Mobile Agents" 2009 International Symposium on computing, Communication, and Control (ISCCC 2009) Proc .of CSIT vol.1 (2011).
2. Mr. Sachin Taluja, Mr. Pradeep Kumar Verma, Prof. Rajeshwar Lal Dua, " Network Security Using IP firewalls" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 8, August 2012.
3. Yashpal Singh, Kapil Gulati and S Niranjan, "DIMENSIONS AND ISSUES OF MOBILE AGENT TECHNOLOGY International Journal of Artificial Intelligence & Applications (IJAIA), Vol.3, No.5, September 2012.
4. Shiv Shakti Srivastava, Nitin Gupta, Saugata Ghosh, Saurabh Chaturvedi , "A Survey on Mobile Agent based Intrusion Detection System" International Symposium on Devices MEMS, Intelligent Systems & Communication (ISDMISC) 2011, Proceedings published by International Journal of Computer Applications® (IJCA).
5. Amit Mishra, " Mobile Agents: As a Solution for Sniffer Detection" International Journal of Computer Technology and Electronics Engineering (IJCTEE) Volume 2, Issue 4, August 2012.
6. Muhammad Awais Shibli Sead Muftic "INTRUSION DETECTION AND PREVENTION SYSTEM USING SECURE MOBILE AGENTS" IEEE INTERNATIONAL CONFERENCE ON SECURITY AND CRYPTOGRAPHY, (PP 76-82), PORTO PORTUGAL, JULY 2008.
7. Danny B. lange and Mitsuru Oshima "Seven Good Reason for Mobile Agents", (PP 88-89) Communications of the ACM, Vol 42.No.3, March 1999.
8. Mohammad Sazzadul Hoque, Md. Abdul Mukit and Md. Abu Naser Bikas, "AN IMPLEMENTATION OF INTRUSION DETECTION SYSTEM USING GENETIC ALGORITHM" International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, March 2012.
9. Pranita Jain, Sandeep Raghuwanshi and Pateria R.K, "NEW MOBILE AGENT-BASED INTRUSION DETECTION SYSTEMS FOR DISTRIBUTED NETWORKS" International Journal of Wireless Communication Volume 1, Issue 1, 2011, pp-01-04.

This page is intentionally left blank

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 13 Issue 15 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

PEGASIS-E: Power Efficient Gathering in Sensor Information System Extended

By Vibha Nehra & Ajay K. Sharma
Sharda University, Greater Noida, India

Abstract- In this paper, an improved energy efficient PEGASIS based protocol (PEGASIS-E) has been proposed. PEGASIS-E uses average distance among the sensor nodes as the criteria for chaining, thereby providing better performance in terms of energy dissipation and amount of information sent to BS. The simulation results obtained show that PEGASIS-E gives an increase in the network lifetime as compared to PEGASIS.

GJCST-E Classification : I.2.9

Strictly as per the compliance and regulations of:

PEGASIS-E: Power Efficient Gathering in Sensor Information System Extended

Vibha Nehra [α] & Ajay K. Sharma [σ]

Abstract- In this paper, an improved energy efficient PEGASIS based protocol (PEGASIS-E) has been proposed. PEGASIS-E uses average distance among the sensor nodes as the criteria for chaining, thereby providing better performance in terms of energy dissipation and amount of information sent to BS. The simulation results obtained show that PEGASIS-E gives an increase in the network lifetime as compared to PEGASIS.

I. Introduction

Advances in wireless communication have made possible the development of wireless sensor networks consisting of devices called sensor nodes. Sensor nodes are low power, small size & cheap devices, capable of sensing, wireless communication and computation [1,2]. Applications of wireless sensor network include monitoring of harsh inhospitable, remote geographical locations like toxic urban industrial locations or a surveillance field. Other applications may include office automation, robot control, smart homes, interactive toys, identification and personalization [3].

A sensor network consists of hundreds & thousands of sensor nodes deployed in a geographical region. These nodes collectively form a high level description of event being sensed, which is further forwarded to a distant base station (BS), so that end user can access the available information. Energy awareness and computational feasibility are the key parameters that need to be addressed while designing protocols in resource constrained sensor networks. Variation in distance of nodes from BS and differences in internodal distances are primary antecedents causing unequal energy dissipation among the nodes. Thus, energy difference among the nodes increases with time resulting in deterioration of network performance [4]. PEGASIS (Power Efficient GAthering in Sensor Information System) is a chain based protocol [5] which has certain deficiencies like long chaining time in the process of greedy chain formation, inevitability of long links as well as abrupt death pattern of nodes in the network.

In recent years, researchers have proposed numerous improved algorithms based on PEGASIS such as PEG-ant [6], EEPB [7], IEEPB [8]. Among these EEPB adopts a threshold for chain formation to avoid the formation of long links LL, but this threshold is still uncertain and complex to determine, which induces LL, if not valued appropriately [7]. Likewise, IEEPB compares distance between the nodes twice, finds the shortest path to link two adjacent nodes & avoids the formation of LL between the neighbors [8]. The work in this paper introduces a PEGASIS based routing protocol called PEGASIS-E. PEGASIS-E computes average distance among the nodes and sets it as radio range for the farthest node from the BS. Then, it chains all the nodes in the radio range. Further, it compares the distance of all the chained nodes to find the nearest next end node to continue the chaining process. The simulation results show that PEGASIS-E outperforms PEGASIS.

The rest of the paper is organized as follows: section II explains the radio energy dissipation model, section III gives the network model and assumptions used followed by section IV which describes PEGASIS-E. Section V lists the performance metrics used for the simulation. Section VI describes the results obtained. Section VII concludes the paper.

II. Radio Energy Dissipation Model

In the radio energy model [9, 10], the transmitter dissipates energy to run the radio electronics and the power amplifier, and the receiver dissipates energy to run the radio electronics as shown in Figure 1.

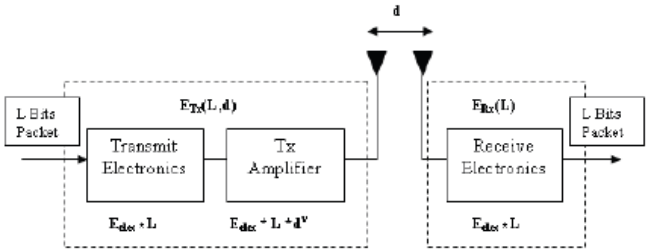


Figure 1 : Radio Energy Dissipation Model

Here both the free space (d^2 power loss) and the multipath fading (d^4 power loss) channel models are used, depending on the distance between the transmitter and receiver [9, 10]. Power control can be used to invert this loss by appropriately setting the power amplifier—if the distance is less than a threshold d_o, the free space model is used; otherwise, the multipath model is used. Thus, to transmit an L-bit message a distance, the radio expends

Author α : Department of Computer Science & Engineering, Sharda University, Greater Noida, India. e-mail: Vibha.nehra@sharda.ac.in
Author σ : Department of Computer Science & Engineering, National Institute of Technology, Jalandhar, India.
e-mail: sharmaajayk@nitj.ac.in

$$E_{Tx}(L, d) = \begin{cases} L.E_{elect} + L.E_{fs}.d^2 & \text{if } d < d_o \\ L.E_{elect} + L.E_{amp}.d^4 & \text{if } d >= d_o \end{cases}$$

The electronics energy, E_{elec}, depends on factors such as the digital coding, modulation, filtering, and spreading of the signal, whereas the amplifier energy, $E_{fs}.d^2$ or $E_{amp}.d^4$, depends on the distance to the receiver and the acceptable bit-error rate [9, 10]. Value of threshold distance d_o is given by

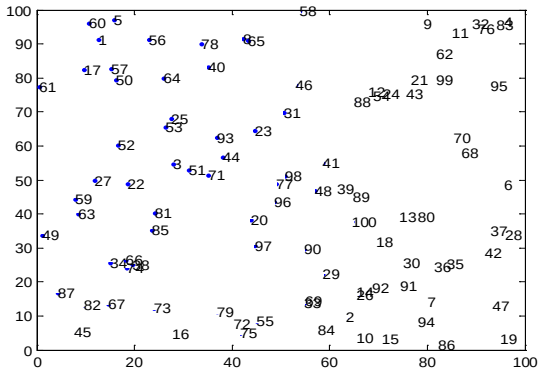
$$d_o = (E_{fs}/E_{mp})$$

And to receive this message, the radio expends energy equivalent to

$$E_{rx}(L) = L \times E_{elec}$$

III. Network Model

Our sensor network consists of 100 nodes in a 100 x 100 sensor field as shown in Figure 2



For Simplicity, we have taken following Assumptions [2, 8]:

- All nodes are static.
- All nodes have power control capabilities, and each node can change the power level and communicate with BS directly.
- BS is located far away from the sensor field and at a fixed location.
- For a given signal to noise ratio, symmetric radio channel, making the energy required to transmit from one point to another and in reverse direction identical.
- Nodes always have data to send.
- Every sensor node generates a fixed size packet and forwards it to next node in the chain.
- BS schedules transmission based on TDMA to avoid collision.

IV. PEGASIS-E

PEGASIS-E is a improved chain based routing algorithm which operates in rounds. It consists of 3 stages: (1) Chain construction phase, (2) leader selection phase, (3) data transmission phase.

a) Chain Construction Phase

The algorithm uses the following steps to form a chain:

a) Initialize the network parameters. Determine the number of nodes, initial energy, BS location information et al. Then, the chain construction starts.
b) BS broadcasts the whole network a *hello* message to obtain basic network information such as ID of nodes alive, distance of each node to BS, and distance among the nodes.
c) Set the node farthest from BS as *end node*, it joins the chain first and is labeled as node 1.
d) Calculate average distance between the alive nodes, D_{avg} and set it as the radio range for *end node*.
e) Join all the nodes to the chain which have not joined the network and lies in the radio range.
f) Compare distance of all nodes joined in the chain to calculate the minimum distance node.
g) Set the selected node as new *end node*.
h) Repeat steps e), f), g) till all the nodes have joined the chain.

The chain building scenario in PEGASIS-E for a network of 100 nodes randomly arranged is shown in figure 3.

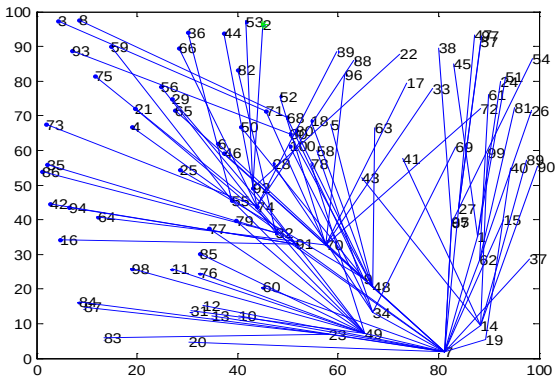


Figure 3 : The chain formed in PEGASIS-E

b) Leader Selection Phase

Leader selection in PEGASIS-E is same as that of PEGASIS [5]. Node which transmits the data from the chain is called a leader. Leader will be in some random position *j* on the chain. Nodes take turns transmitting to the BS, and will use node number *i* mod N (N represents the number of nodes) to transmit to the BS in round *i*. Therefore, the leader in each round of communication will be at a random position on the chain, for node deaths at random locations. This concept of random node deaths on the chain ensures robustness of the network towards failures.

c) Data Transmission Phase

Data transmission starts on successful construction of chain and leader node selection. Leader node initiates a token passing approach to start data

transmission from nodes which have just one link. Each node delivers its own sensed data to its neighbor node in the chain during their time slots assigned by TDMA mechanism. Then, the neighbor nodes fuse the received data with their own data & forwards further towards the leader. One round will end until BS receives data from the leader. In addition, it is assumed that chain is rebuilt when a node of the chain dies during simulation of experiment.

V. Performance Metrics

The number of Nodes Alive, number of Packets received at BS, Energy consumed per round & Total Residual Energy of the sensor network are the performance parameters that have been used to study and evaluate the performance of the proposed protocol.

- *Number of alive nodes :* This instantaneous measure reflects the total number of nodes and that of each type that has not yet expended all of their energy.
- *Data Packets received at base station :* It is total number of data packets or messages that are received by the base station. This is also a measure of amount of information sent to BS from the sensor field. This measure varies linearly for all protocols.
- *Energy consumed :* It measures the instantaneous amount of energy being consumed in the network per round. This is simply the energy difference from the beginning till the end of a round.
- *Network residual energy :* It measures the total remaining energy of the network. It is calculated at each transmission round of the protocol.

The metrics used allow us to conclude about the stability of the network which is the time interval from the start of network operation until the death of the last sensor node. The lifetime of the network defined as the number of rounds until the last node die is simply the operational period of the network that is the period for which the network continues to provide information to the BS.

VI. Results and Discussions

Table 1 : System parameters value

Parameter	Value
Network Size	100 X 100 meter^2
Sink	(50,300)
Number of Nodes	100
Initial Energy of Node	0.50 J
E_{elect}	50 nJ/bit
E_{fs}	10 pJ/bit/m^2
E_{mp}	0.0013 pJ/bit/m^4
E_{fusion}	5 nJ/bit/message
Data Packet	2000 bits

This paper uses MATLAB as simulator to evaluate the performance of PEGASIS-E. The system parameters used in the simulation are shown in the table 1 [1,5,9, 10].

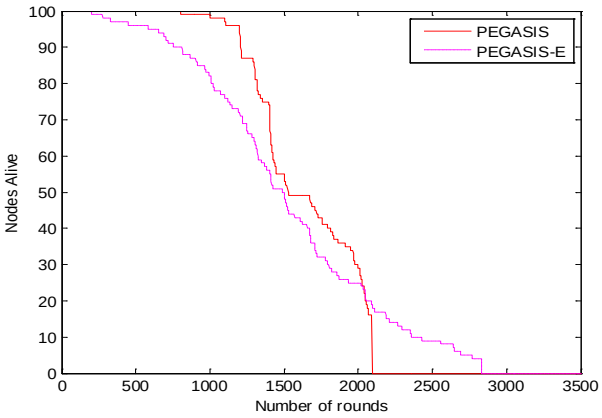


Figure 4 : Number of nodes a live

Figure 4 depicts the number of alive nodes in the network. It is observed that PEGASIS-E has a stable lifetime as compared to PEGASIS. The lifetime period of PEGASIS-E before the death of first node is less, but it continues to provide information about the sensor field for a longer period of time. PEGASIS shows abrupt death of nodes due to almost same energy dissipation in all nodes, as they consume same amount of energy in each round. While in PEGASIS-E, energy dissipation is different in every round. It is higher for end node.

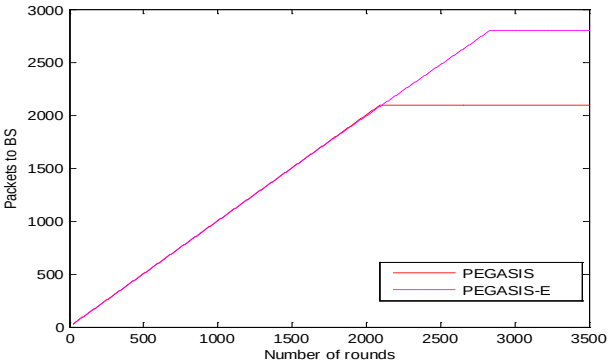


Figure 5 : Number of Packets to BS

Figure 5. indicates a clear gain of 34% in number of Packets sent to BS for PEGASIS-E as compared to PEGASIS. This is because death pattern of nodes in PEGASIS-E is such that a sub section of sensor field is not clearly cut-off after the death of certain nodes, leading to the availability of sensed data for a longer period of time.

Figure 6. shows energy consumption of PEGASIS-E. It is concluded that PEGASIS-E consumes less energy compared to PEGASIS because the number of nodes to be covered becomes less due to death of nodes with simulation time.

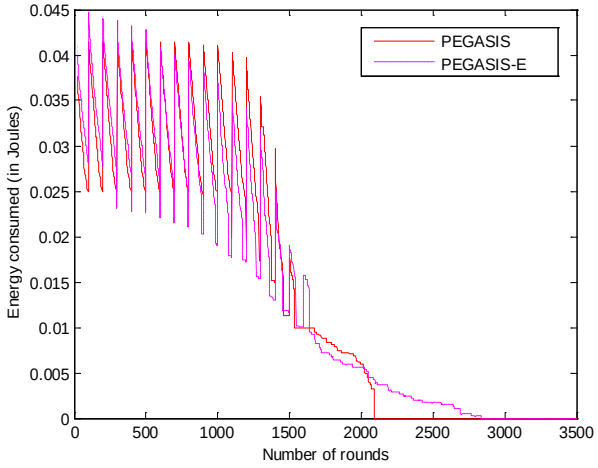


Figure 6 : Energy consumed over time.

Figure 7 depicts that PEGASIS-E has a balanced energy dissipation and more stable lifetime.

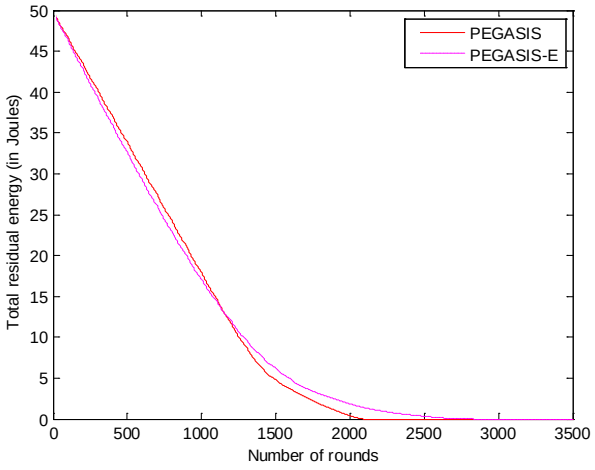


Figure 7 : Total residual energy

VII. Conclusion

This paper proposes an improved energy-efficient PEGASIS based protocol PEGASIS-E, which not only provides a set threshold, D_{avg} for chaining but also simplifies the complexity of chain construction. Moreover, the chaining speed of PEGASIS-E is faster than PEGASIS. The novel algorithm avoids the formation of LL and provides a stable and balanced lifetime to the network. The simulation results prove that PEGASIS-E outperforms PEGASIS by achieving higher energy-efficiency extending lifetime of network.

References Références Referencias

1. I.F. Akyildiz et.al.," Wireless sensor networks: a survey." Computer Networks, 2002, 38 (4) pp:393-422.
2. Jamal N. Al-Karaki, Ahmed E. Kamal, "Routing Techniques in Wireless Sensor Networks: A Survey", IEEE Wireless Communications, Volume: 11, Issue: 6, 26-28, December 2004.
3. Ahmed A. Ahmed, Hongchi Shi & Yi Shang, "A Survey on Network Protocols for Wireless Sensor Networks", IEEE 2003.
4. Yunxia Chen and Qing Zhao, "On the Lifetime of Wireless Sensor Networks", Communications Letters, IEEE, Volume 9, Issue 11, pp:976–978, Digital Object Identifier 10.1109/LCOMM.2005.11010., Nov. 2005.
5. S. Lindsey, C.S. Raghavendra," PEGASIS: Power-efficient gathering in sensor information systems", IEEE Aerospace and Electronic Systems Society, Proc of the IEEE Aerospace Conf, Montana, 2002:1125-1130.
6. GUO Wen-yu, ZHANG Wei, and LU Gang, "PEGASIS protocol in wireless sensor network based on an improved ant colony algorithm," Second International Workshop on Education Technology and Computer Science, 2010, pp.64-67.
7. YU Yong-chang, WEI Gang, "An improved PEGASIS Algorithm in Wireless Sensor Networks", Acta Electronica Sinica, Vol. 36, pp. 1309-1313, July 2008.
8. Feng Sen, Qi Bing, Tang Liangrui, "An Improved Energy Efficient PEGASIS Based Protocol in Wireless Sensor Networks", IEEE 2011 Eighth International Conference on Fuzzy Systems and Knowledge Discovery (FSKD).
9. W. Heinzelman, A. Chandrakasan, and H. Balakrishnan,"Energy-efficient communication protocols for wireless microsensor networks," Proceedings of the 33rd International Conference on System Sciences (HICS '00), January 2000.
10. W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks", IEEE Transactions on Wireless Communications, Vol. 1, No. 4, pp. 660-670, October 2002.

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 13 Issue 15 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

A Study of Encryption Algorithms AES, DES and RSA for Security

By Dr. Prerna Mahajan & Abhishek Sachdeva
IITM, India

Abstract- In recent years network security has become an important issue. Encryption has come up as a solution, and plays an important role in information security system. Many techniques are needed to protect the shared data. The present work focus on cryptography to secure the data while transmitting in the network. Firstly the data which is to be transmitted from sender to receiver in the network must be encrypted using the encryption algorithm in cryptography. Secondly, by using decryption technique the receiver can view the original data. In this paper we implemented three encrypt techniques like AES, DES and RSA algorithms and compared their performance of encrypt techniques based on the analysis of its stimulated time at the time of encryption and decryption. Experiments results are given to analyses the effectiveness of each algorithm.

Keywords: DES, RSA, AES, encryption, decryption, private key encryption, public key encryption, cryptography.

GJCST-E Classification : E.3

Strictly as per the compliance and regulations of:

A Study of Encryption Algorithms AES, DES and RSA for Security

Dr. Prerna Mahajan [α] & Abhishek Sachdeva [σ]

Abstract- In recent years network security has become an important issue. Encryption has come up as a solution, and plays an important role in information security system. Many techniques are needed to protect the shared data. The present work focus on cryptography to secure the data while transmitting in the network. Firstly the data which is to be transmitted from sender to receiver in the network must be encrypted using the encryption algorithm in cryptography. Secondly, by using decryption technique the receiver can view the original data. In this paper we implemented three encrypt techniques like AES, DES and RSA algorithms and compared their performance of encrypt techniques based on the analysis of its stimulated time at the time of encryption and decryption. Experiments results are given to analyses the effectiveness of each algorithm.

Keywords: DES, RSA, AES, encryption, decryption, private key encryption, public key encryption, cryptography.

I. Introduction

Many encryption algorithms are widely available and used in information security. They can be categorized into Symmetric (private) and Asymmetric (public) keys encryption. In Symmetric keys encryption or secret key encryption, only one key is used to encrypt and decrypt data. In Asymmetric keys, two keys are used; private and public keys [1]. Public key is used for encryption and private key is used for decryption (e.g. RSA). Public key encryption is based on mathematical functions, computationally intensive. There are many examples of strong and weak keys of cryptography algorithms like DES, AES. DES uses one 64-bits key while AES uses various 128,192,256 bits keys [2].

Asymmetric key encryption or public key encryption is used to solve the problem of key distribution. In Asymmetric keys, two keys are used; private and public keys. Public key is used for encryption and private key is used for decryption (E.g. RSA and Digital Signatures). Because users tend to use two keys: public key, which is known to the public and private key which is known only to the user[2]. There is no need for distributing them prior to transmission. However, public key encryption is based on mathematical functions, computationally intensive and is not very efficient for small mobile devices [3]. Asymmetric encryption techniques are almost 1000 times slower than Symmetric techniques, because they require more computational processing power [4].

This study evaluates three different encryption algorithms namely; AES, DES and RSA. The performance measure of encryption schemes will be conducted in terms of encryption and decryption time such as text or document[5].

II. Encryption Algorithms

Encryption is a well known technology for protecting sensitive data. Use of the combination of Public and Private Key encryption to hide the sensitive data of users, and cipher text retrieval [6].

a) Data Encryption Standard (DES)

DES (Data Encryption Standard) algorithm purpose is to provide a standard method for protecting sensitive commercial and unclassified data. In this same key used for encryption and decryption process [7].
DES algorithm consists of the following steps

i. *Encryption*

1. DES accepts an input of 64-bit long plaintext and 56-bitkey (8 bits of parity) and produce output of 64 bit block.
2. The plaintext block has to shift the bits around.
3. The 8 parity bits are removed from the key by subjecting the key to its Key Permutation.
4. The plaintext and key will processed by following

i. The key is split into two 28 halves
ii. Each half of the key is shifted (rotated) by one or two bits, depending on the round.
iii. The halves are recombined and subject to a compression permutation to reduce the key from 56 bits to 48 bits. This compressed keys used to encrypt this round's plaintext block.
iv. The rotated key halves from step 2 are used in next round.
v. The data block is split into two 32-bit halves.
vi. One half is subject to an expansion permutation to increase its size to 48 bits.
vii. Output of step 6 is exclusive-OR'ed with the 48-itcompressed key from step 3.
viii. Output of step 7 is fed into an S-box, which substitutes key bits and reduces the 48-bit block back down to 32-bits.
ix. Output of step 8 is subject to a P-box to permute the bits.

Authors α σ : e-mail: aabhi616@yahoo.in

x. The output from the P-box is exclusive-OR'ed with other half of the data block. k. The two data halves are swapped and become the next round's input.

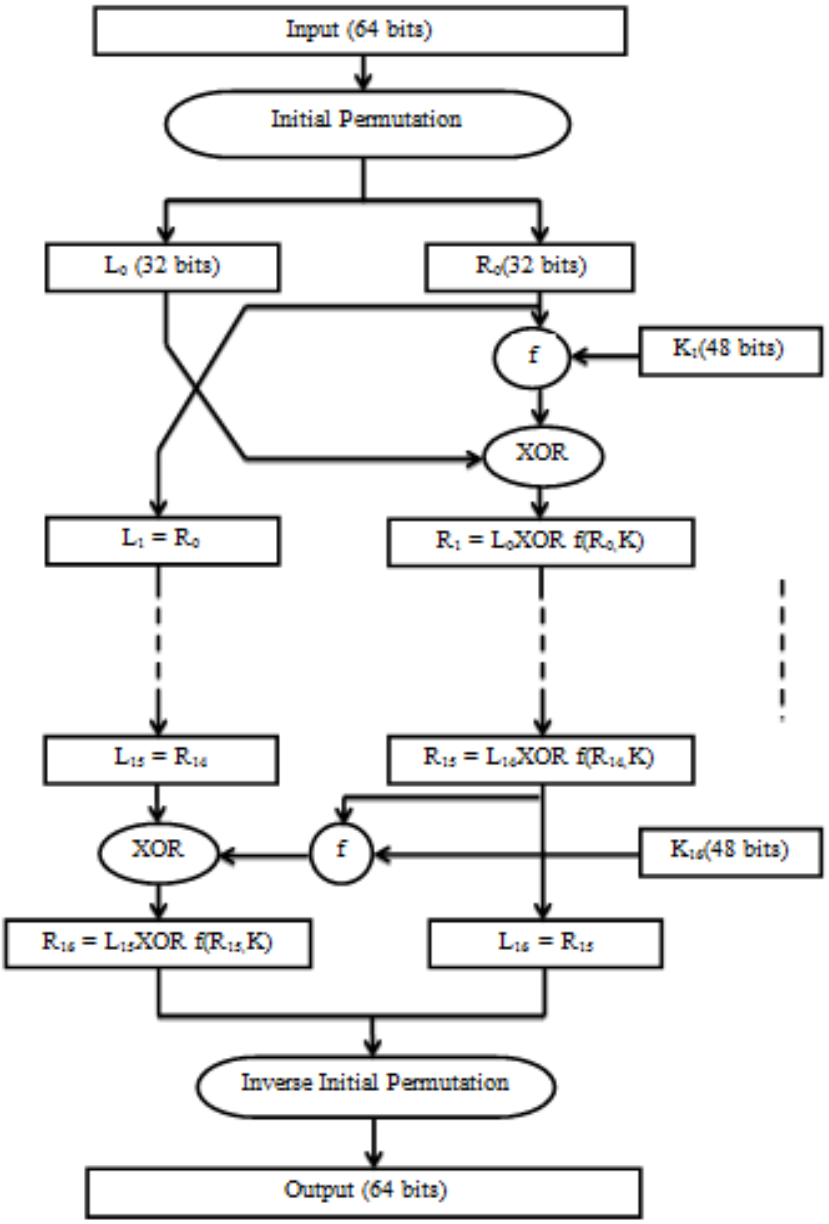


Figure 1 : Diagram of DES Algorithm

b) Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) algorithm not only for security but also for great speed. Both hardware and software implementation are faster still. New encryption standard recommended by NIST to replace DES. Encrypts data blocks of 128 bits in 10, 12 and 14 round depending on key size as shown in Figure - 2. It can be implemented on various platforms specially in small devices. It is carefully tested for many security applications.

i. ***Algorithm Steps :*** These steps used to encrypt 128-bit block

1. The set of round keys from the cipher key.
2. Initialize state array and add the initial round key to the starting state array.
3. Perform round = 1 to 9 : Execute Usual Round.
4. Execute Final Round.
5. Corresponding cipher text chunk output of Final Round Step

ii. *Usual Round :* Execute the following operations which are described above.

1. Sub Bytes
2. Shift Rows
3. Mix Columns
4. Add Round Key , using K(round)

iii. *Final Round:* Execute the following operations which are described above.

1. Sub Bytes
2. Shift Rows
3. Add Round Key, using K(10)

iv. *Encryption :* Each round consists of the following four steps:

i Sub Bytes : The first transformation, Sub Bytes, is used at the encryption site. To substitute a byte, we interpret the byte as two hexadecimal digits.

ii Shift Rows : In the encryption, the transformation is called Shift Rows.

iii Mix Columns : The Mix Columns transformation operates at the column level; it transforms each column of the state to a new column.

iv Add Round Key : Add Round Key proceeds one column at a time. Add Round Key adds a round key word with each state column matrix; the operation in Add Round Key is matrix addition.

The last step consists of XO Ring the output of the previous three steps with four words from the key schedule. And the last round for encryption does not involve the "Mix columns" step. [8]

v. *Decryption:* Decryption involves reversing all the steps taken in encryption using inverse functions like a) Inverse shift rows, b) Inverse substitute bytes, c) Add round key, and d) Inverse mix columns.

The third step consists of XO Ring the output of the previous two steps with four words from the key schedule. And the last round for decryption does not involve the "Inversemix columns" step.

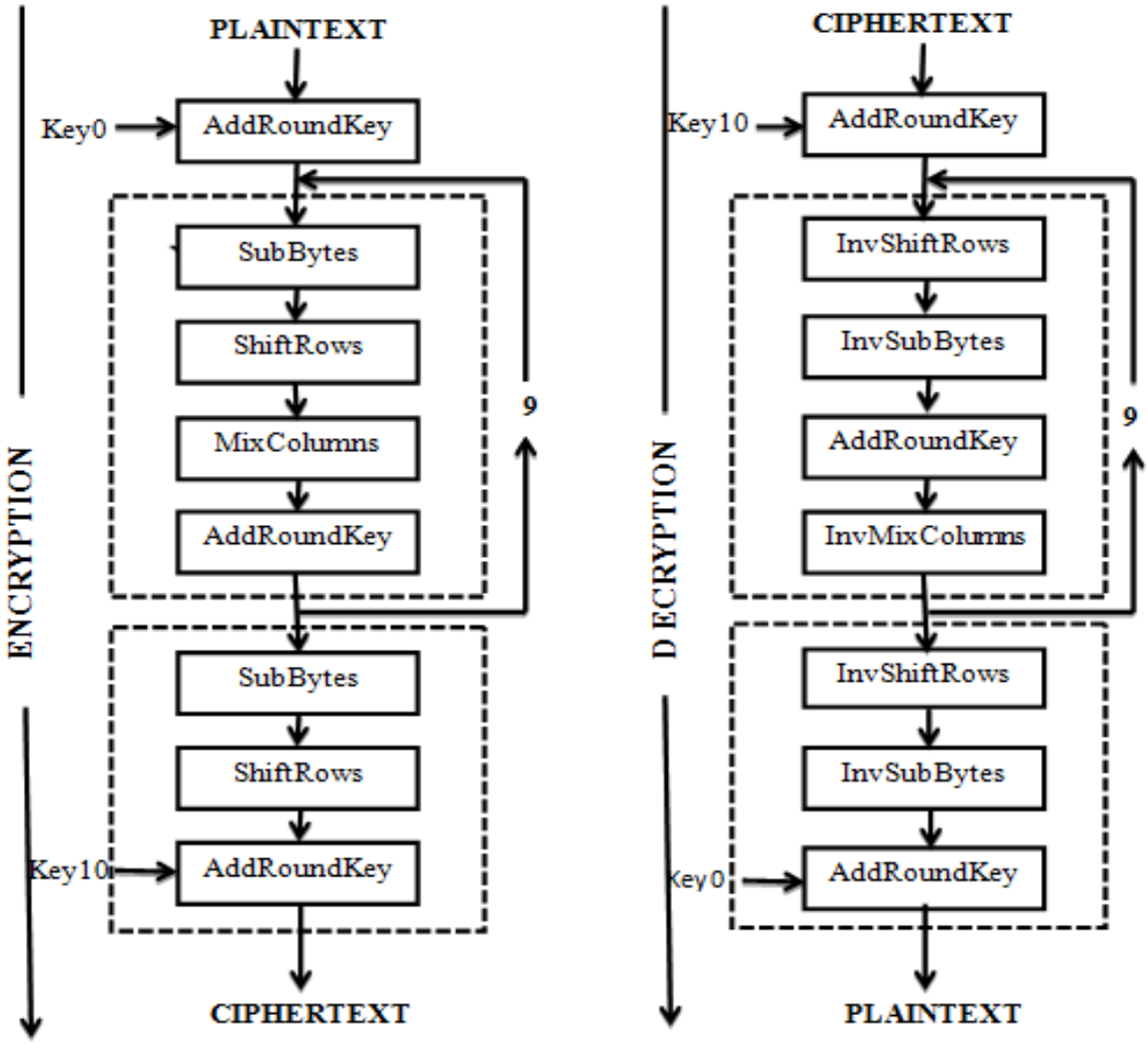


Figure 2 : AES Encryption and Decryption

c) Rivest-Shamir-Adleman (RSA)

RSA is widely used Public-Key algorithm. RSA firstly described in 1977. In our proposed work, we are using RSA algorithm to encrypt the data to provide security so that only the concerned user can access it.

RSA algorithm involves these steps:

1. Key Generation
2. Encryption
3. Decryption

i *Key Generation*

Before the data is encrypted, Key generation should be done. [9]

Steps:

Generate a public/private key pair :

1. Generate two large distinct primes p and q
2. Compute $n = pq$ and $\varphi = (p-1)(q-1)$
3. Select an e, $1 < e < \varphi$, relatively prime to φ.
4. Compute the unique integer d, $1 < d < \varphi$ where $ed \equiv_{\varphi} 1$.
5. Return public key (n, e) and private key d

ii *Encryption*

Encryption is the process of converting original plain text (data) into cipher text (data).

Encryption with key (n , e)

1. Represent the message as an integer $m \in \{0, \ldots, n-1\}$
2. Compute $c = m^e \bmod n$

iii *Decryption*

Decryption is the process of converting the cipher text (data) to the original plain text(data). [10]

Decryption with key d: compute $m = c^d \bmod n$

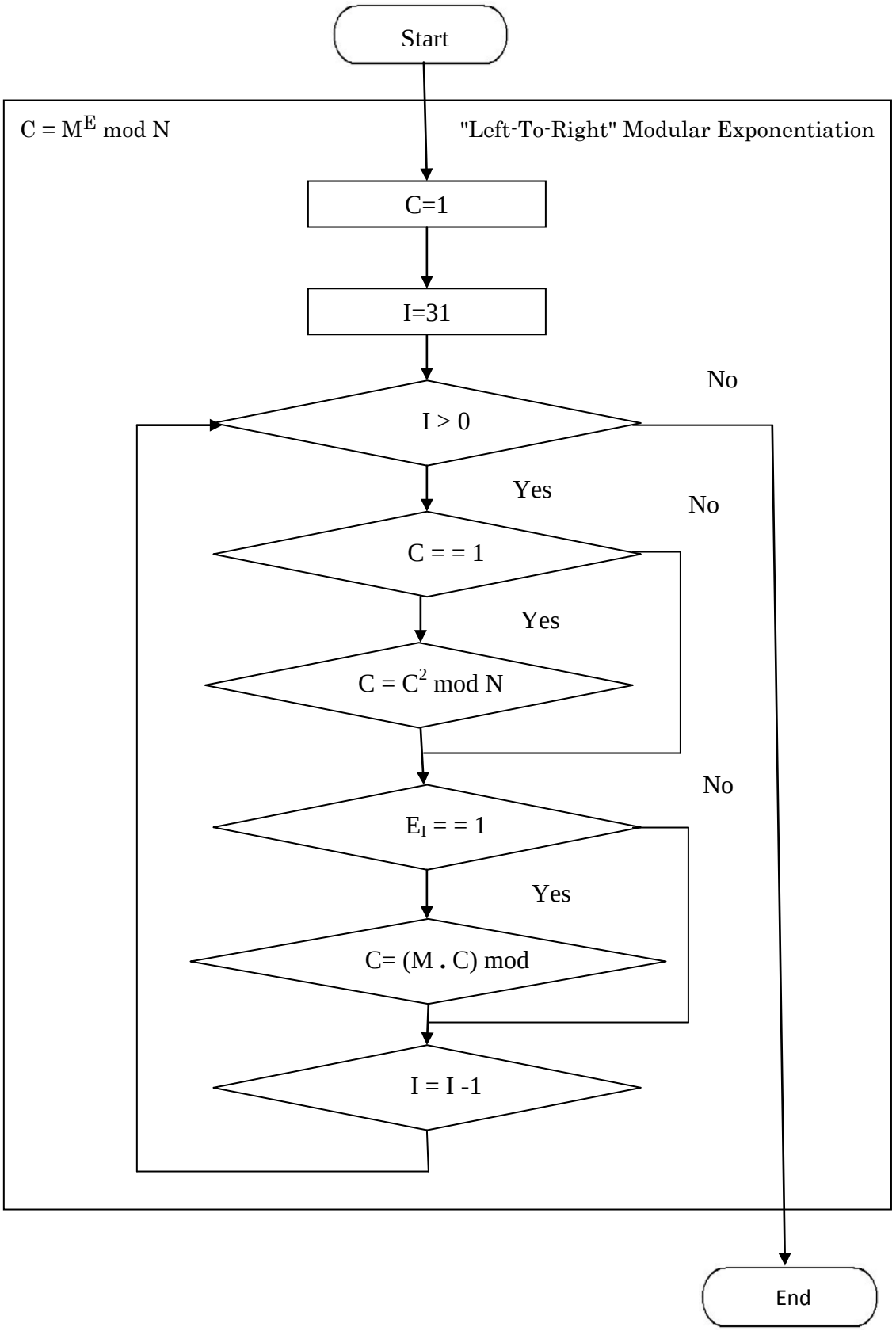


Figure 3 : RSA Encryption and Decryption Flowchart

III. Comparision

In the table below a comparative study between AES, DES and RSA is presented in to eighteen factors, which are Key Size, Block Size, Ciphering & Deciphering key, Scalability, Algorithm, Encryption, Decryption, Power Consumption, Security, Deposit of keys, Inherent Vulnerabilities, Key used, Rounds, Stimulation Speed, Trojan Horse, Hardware & Software Implementation and Ciphering & Deciphering Algorithm.

Table 1: Comparison between AES, DES and RSA

Factors	AES	DES	RSA
Developed	2000	1977	1978
Key Size	128, 192, 256 bits	56 bits	>1024 bits
Block Size	128 bits	64 bits	Minimum 512 bits
Ciphering & deciphering key	Same	Same	Different
Scalability	Not Scalable	It is scalable algorithm due to varying the key size and Block size.	Not Scalable
Algorithm	Symmetric Algorithm	Symmetric Algorithm	Asymmetric Algorithm
Encryption	Faster	Moderate	Slower
Decryption	Faster	Moderate	Slower
Power Consumption	Low	Low	High
Security	Excellent Secured	Not Secure Enough	Least Secure
Deposit of keys	Needed	Needed	Needed
Inherent Vulnerabilities	Brute Forced Attack	Brute Forced, Linear and differential cryptanalysis attack	Brute Forced and Oracle attack
Key Used	Same key used for Encrypt and Decrypt	Same key used for Encrypt and Decrypt	Different key used for Encrypt and Decrypt
Rounds	10/12/14	16	1
Stimulation Speed	Faster	Faster	Faster
Trojan Horse	Not proved	No	No
Hardware & Software Implementation	Faster	Better in hardware than in software	Not Efficient
Ciphering & Deciphering Algorithm	Different	Different	Same

IV. Experimental Design

The four text files of different sizes are used to conduct four experiments, where a comparison of three algorithms AES, DES and RSA is performed.

a) Evaluation Parameters

Performance of encryption algorithm is evaluated considering the following parameters.

A. Encryption Time
B. Decryption Time

The encryption time is considered the time that an encryption algorithm takes to produces a cipher text from a plain text. Encryption time is used to calculate the throughput of an encryption scheme, is calculated as the total plaintext in bytes encrypted divided by the encryption time. Comparisons analyses of the results of the selected different encryption scheme are performed. [11]

V. Experimental Results And Analysis

Experimental result for Encryption algorithm AES, DES and RSA are shown in table-2, which shows the comparison of three algorithm AES, DES and RSA using same text file for four experiment.

Table 2 : Comparisons of DES, AES and RSA of Encryption and Decryption Time

S.NO	*Algorithm*	*Packet Size (KB)*	*Encryption Time (Sec)*	*Decryption Time (Sec)*
1	AES	153	1.6	1
	DES		3.0	1.1
	RSA		7.3	4.9

2	AES	196	1.7	1.4
	DES		2.0	1.24
	RSA		8.5	5.9
3	AES	312	1.8	1.6
	DES		3.0	1.3
	RSA		7.8	5.1
4	AES	868	2.0	1.8
	DES		4.0	1.2
	RSA		8.2	5.1

By analyzing table-2, Time taken by RSA algorithm for both encryption and decryption process is much higher compare to the time taken by AES and DES algorithm.

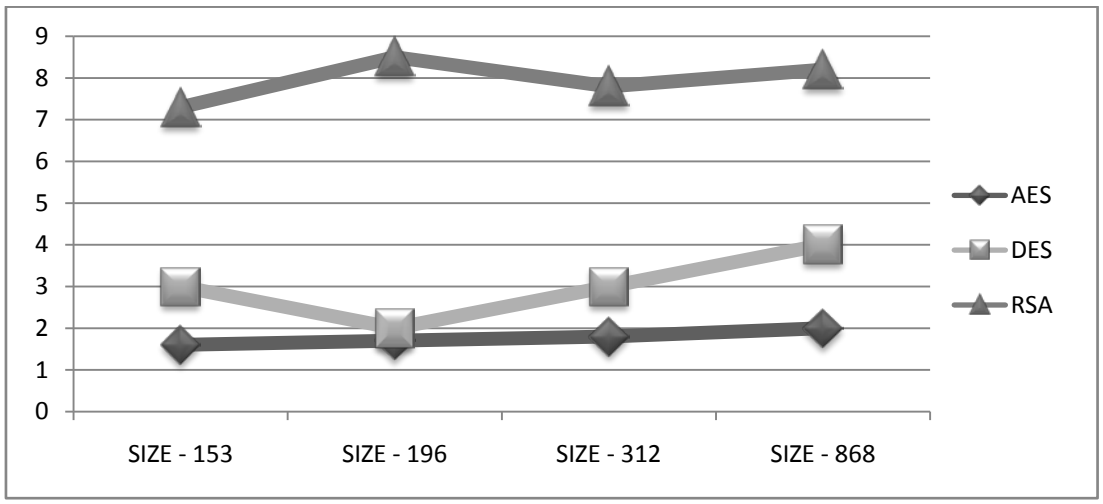


Figure 4 : Comparison of Encryption Time among AES, DES and RSA

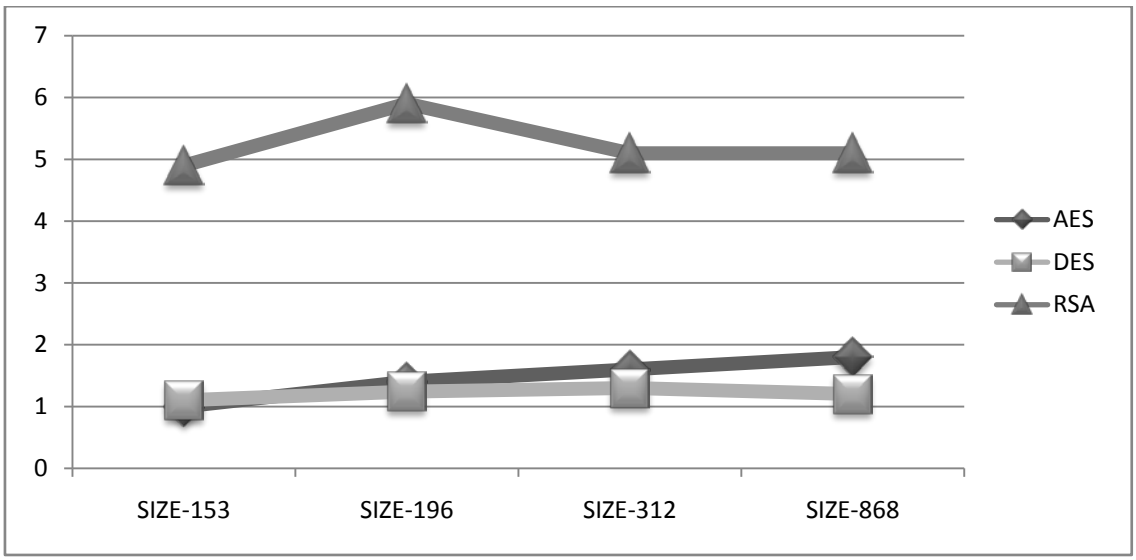


Figure 5 : Comparison of Decryption Time among AES, DES and RSA

By analyzing Fig-4 , Fig-5 which shows time taken for encryption and decryption on various size of file by three algorithms. RSA algorithm takes much longer time compare to time taken by AES and DES

algorithm. AES and DES algorithm show very minor difference in time taken for encryption and decryption process.

VI. Conclusion

Encryption algorithm plays very important role in communication security. Our research work surveyed the performance of existing encryption techniques like AES, DES and RSA algorithms.

Based on the text files used and the experimental result it was concluded that AES algorithm consumes least encryption and RSA consume longest encryption time.

We also observed that Decryption of AES algorithm is better than other algorithms.

From the simulation result, we evaluated that AES algorithm is much better than DES and RSA algorithm.

Our future work will focus on compared and analysed existing cryptographic algorithm like AES, DES and RSA. It will include experiments on image and audio data and focus will be to improve encryption time and decryption time.

References Références Referencias

1. Idrizi, Florim, Dalipi, Fisnik & Rustemi, Ejup. "Analyzing the speed of combined cryptographic algorithms with secret and public key". *International Journal of Engineering Research and Development*, *e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com Volume 8, Issue 2 (August 2013)*, pp. 45
2. Abdul.Mina, D.S, Kader, H.M. Abdual & Hadhoud, M.M. "Performance Analysis of Symmetric Cryptography". pp. 1.
3. Chehal Ritika, Singh Kuldeep. "Efficiency and Security of Data with Symmetric Encryption Algorithms". *International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X , Volume 2, Issue 8, August 2012,* pp. 1.
4. Hardjono, "Security In Wireless LANS And MANS," Artech House Publishers 2005.
5. Elminaam, Diaa Salama Abd, Abdual Kader, Hatem Mohamed & Hadhoud, Mohiy Mohamed. "Evaluating The Performance of Symmetric Encryption Algorithms". *International Journal of Network Security, Vol.10, No.3, May 2010*, pp. 216.
6. Padmapriya, Dr.A, Subhasri, P. "Cloud Computing: Security Challenges & Encryption Practices". *International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 3, Issue 3, March 2013,* pp. 257.
7. Prashanti.G, Deepthi.S & Sandhya Rani.K. "A Novel Approach for Data Encryption Standard Algorithm". *International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-5, June 2013,* pp. 264.
8. Das Debasis, Misra Rajiv. "Programmable Cellular Automata Based Efficient Parallel AES Encryption Algorithm". International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011, pp. 204.
9. Kalpana Parsi, Singaraju Sudha. "Data Security in Cloud Computing using RSA Algorithm". International Journal of Research in Computer and Communication technology, IJRCCT, ISSN 2278-5841, Vol 1, Issue 4, September 2012. pp. 145.
10. Sunitha K, Prashanth K.S. "Enhancing Privacy in Cloud Service Provider Using Cryptographic Algorithm". IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 12, Issue 5 (Jul. - Aug. 2013). pp. 64.
11. Singh Narjeet, Raj Gaurav. "Security On Bccp Through Aes Encryption Technique". International Journal Of Engineering Science & Advanced Technology Volume-2, Issue-4, 813 – 819. pp. 817.

.

Global Journals Inc. (US) Guidelines Handbook 2013

www.GlobalJournals.org

FELLOW OF ASSOCIATION OF RESEARCH SOCIETY IN COMPUTING (FARSC)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

MEMBER OF ASSOCIATION OF RESEARCH SOCIETY IN COMPUTING (MARSC)

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

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

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

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

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

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

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

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

It is mandatory to read all terms and conditions carefully.

AUXILIARY MEMBERSHIPS

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

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

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

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

The Institute will be entitled to following benefits:

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

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

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

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

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

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

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

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

The following entitlements are applicable to individual Fellows:

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

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

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

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

Other:

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

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

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

Note :

"

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

"

Process of submission of Research Paper

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

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

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

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

(II) Choose corresponding Journal.

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

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

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

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

Preferred Author Guidelines

MANUSCRIPT STYLE INSTRUCTION (Must be strictly followed)

Page Size: 8.27" X 11'"

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

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

1. General,

2. Ethical Guidelines,

3. Submission of Manuscripts,

4. Manuscript's Category,

5. Structure and Format of Manuscript,

6. After Acceptance.

1. GENERAL

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

Scope

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

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

2. ETHICAL GUIDELINES

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

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

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

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

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

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

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

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

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

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

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

Please mention proper reference and appropriate acknowledgements wherever expected.

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

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

3. SUBMISSION OF MANUSCRIPTS

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

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

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

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

4. MANUSCRIPT'S CATEGORY

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

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

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

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

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

5. STRUCTURE AND FORMAT OF MANUSCRIPT

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

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

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

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

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

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

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

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

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

(h) Brief Acknowledgements.

(i) References in the proper form.

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

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

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

Format

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

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

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

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

Structure

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

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

Abstract, used in Original Papers and Reviews:

Optimizing Abstract for Search Engines

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

Key Words

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

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

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

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

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

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

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

Acknowledgements: Please make these as concise as possible.

References

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

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

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

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

Tables, Figures and Figure Legends

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

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

Preparation of Electronic Figures for Publication

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

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

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

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

6. AFTER ACCEPTANCE

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

6.1 Proof Corrections

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

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

(Free of charge) from the following website:

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

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

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

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

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

6.3 Author Services

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

6.4 Author Material Archive Policy

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

6.5 Offprint and Extra Copies

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

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

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

TECHNIQUES FOR WRITING A GOOD QUALITY RESEARCH PAPER:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Informal Guidelines of Research Paper Writing

Key points to remember:

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

Final Points:

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

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

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

General style:

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

To make a paper clear

· Adhere to recommended page limits

Mistakes to evade

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

In every sections of your document

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

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

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

· Align the primary line of each section

· Present your points in sound order

· Use present tense to report well accepted

· Use past tense to describe specific results

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

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

Title Page:

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

Abstract:

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

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

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

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

Approach:

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

Introduction:

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

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

Approach:

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

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

Procedures (Methods and Materials):

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

Materials:

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

Methods:

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

Approach:

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

What to keep away from

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

Results:

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

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

Content

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

What to stay away from

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

Approach

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

Figures and tables

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

Discussion:

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

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

Approach:

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

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

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

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

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

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

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

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

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

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

INDEX

save our planet

Global Journal of Computer Science and Technology

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

ISSN 9754350