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

Global Journal

of Computer Science and Technology: E

Network, Web & Security

Highlights

- Analysis of DSDV, AODV
- Multicasting Overlay Protocol
- Wireless Sensor Network
- Fixed and Mobility Network

Discovering Thoughts, Inventing Future

VOLUME 14 ISSUE 6 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 14 Issue 6 (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: *investors@globaljournals.org*
Technical Support: *technology@globaljournals.org*
Media & Releases: *media@globaljournals.org*

Pricing (Including by Air Parcel Charges):

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

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

Contents of the Issue

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 14 Issue 6 Version 1.0 Year 2014
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Infrastructure Requirements and Outsourcing

By Richard Scroggins
Capella University, United States

Introduction- Out-of-band Management, or Lights-out Management, is an important tool to manage devices like servers, core routers, and switches. This is facilitated by a secondary card in the device that has an IP address assigned to it and it typically accessible over the network via a web browser even if the device it powered down, assuming of course that the power plug is connected to an electrified outlet. This functionality is very important for a WAN environment. Without this ability to control these devices remotely, the company would either have to employ a resource in the local offices or spend a large amount of time and money on technician travel. This is therefore a cost saving measure as well as a management tool and strategy. In initially pitching and gaining approval for projects, cost savings is often the larger selling point for management. In addition to and as an add-on to the Lights Out management, I also like monitoring the systems though SNMP, using a tool like What's Up. The Lights Out system is very valuable, but you also need a system that informs you when systems go down, and when they are responding to ping again after a restart. Network performance is very much related to network monitoring, however, monitoring is a task that we perform in service to performance, among other things.

GJCST-E Classification : D.2

INFRASTRUCTUREREQUIREMENTSANDOUTSOURCING

Strictly as per the compliance and regulations of:

Open Association of Research Society, USA
Research | Diversity | Ethics

Infrastructure Requirements and Outsourcing

Richard Scroggins

Out-of-band Management, or Lights-out Management, is an important tool to manage devices like servers, core routers, and switches. This is facilitated by a secondary card in the device that has an IP address assigned to it and it typically accessible over the network via a web browser even if the device it powered down, assuming of course that the power plug is connected to an electrified outlet. This functionality is very important for a WAN environment. Without this ability to control these devices remotely, the company would either have to employ a resource in the local offices or spend a large amount of time and money on technician travel. This is therefore a cost saving measure as well as a management tool and strategy. In initially pitching and gaining approval for projects, cost savings is often the larger selling point for management. In addition to and as an add-on to the Lights Out management, I also like monitoring the systems though SNMP, using a tool like What's Up. The Lights Out system is very valuable, but you also need a system that informs you when systems go down, and when they are responding to ping again after a restart. Network performance is very much related to network monitoring, however, monitoring is a task that we perform in service to performance, among other things. Performance, aside from truly unexpected failures, is the result of our actions like monitoring, tuning, and maintenance. For maintaining a high level of up time, an important item is regular maintenance of devices and servers through a patch management plan and a preventive maintenance cycle. This helps improves speed by keeping things running well. These two processes are very common in well functioning networks, and I have used both of them in my past environments, and I will be implementing them both in the project network. In addition to these methods, another way to be aware of problems early and respond quickly to performance issue specific to our routers at each location in the project network is the use of MRTG graphs.

"Increasingly, organizations are jumping onto the information technology (IT) outsourcing bandwagon in an effort to create value. However, evidence indicating the positive economic consequences of such initiatives has been limited. This study attempts to fill this void by synthesizing the process-oriented research in IT business value literature and the resource-based theory to develop an integrative research framework for assessing the value proposition of IT outsourcing." (Wang, Gweba, Wang, & Zhu, 2008) I have been through an IT outsourcing project, and I can say from my experience that the business value created through IT outsourcing is typically exaggerated. Not even taking into consideration the negative stigma and the damage to the reputation of the company or organization, but in house assets are more valuable and it takes multiple outside resources to make up for one in house resource. Communication by itself is a major issue with outsourcing, and the lack of communication ability might stand in the ways of resolving issues. Everyone has a story of dealing with a tech support person from India who is so hard to understand that many give up. So this supports the idea that some things are better left in house. Wang, Gweba, Wang, & Zhu (2008) make this point by separating who does better with outsourcing and to some degree what functions are more outsourceable, " With a process-oriented lens, the framework suggests that the effects of IT outsourcing are best documented at the process level and hence, it is imperative that one takes into consideration the impact of IT outsourcing on performance at both the process level as well as the firm level. Grounded in the resource-based view, the framework also accounts for the complementary role of firms' core IT capability as a critical condition for the value creation of IT outsourcing. Consistent with the process-oriented prediction, the findings suggest that the positive effects of IT outsourcing appear mostly at the process level, but not at the firm level. Moreover, it is found that the level of business value created by IT outsourcing is contingent on firms' core IT capability. Firms with superior core IT capability are found to enjoy an advantage in leveraging their outsourcing initiatives to enhance firm value" (p. 01).

My current company does outsource some specific functions, but only to local resources that have good communication skills. We also have the "core IT capability" that Wang, Gweba, Wang, & Zhu (2008) mention. For instance, we have an IT resource on retainer in one of our remote offices that has a limited need for onsite support. This location is too far away to service like we do our corporate location. We are able to handle most things remotely, but this office performs critical functions for the company so we need to be able to provide same day service. We do not outsource our core functions, nor do we give any external resource sole access to any of our systems. For us, outsourcing is a function of augmenting, not replacing. I have observed many companies use the model of

Author : Capella University, United States.
e-mail: mr_scroggins@yahoo.com

Global Journal of Computer Science and Technology (E) Volume XIV Issue VI Version I Year 2014

outsourcing as a replacement and this can be dangerous. I was recently working with a third party who had outsourced there phone system to a consultant. When the relationship was severed to the consultant, the company lost all access, passwords, configurations, etc. to their phone system. This was very short sighted on their part. I know that this was done on the direction of the management who thought that they were saving a few bucks, but look at the eventual cost.

References Références Referencias

1. Wang, L., Gwebu, K. L., Wang, J., and Zhu, D. X. (2008). The Aftermath of Information Technology Outsourcing: An Empirical Study of Firm Performance Following Outsourcing Decisions. Journal of Information Systems, 22(1), 125–159.

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 14 Issue 6 Version 1.0 Year 2014
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Application Layer Multicasting Overlay Protocol- NARADA Protocol

By G. Sankara Rao, E. Jagadeeswararao & N. Sai Prathyusha
Jawaharlal Nehru Technological University, India

Abstract- The conventional wisdom has been that Network Layer Internet protocol(IP) is the natural protocol layer for implementing multicast related functionality but it is still plagued with concerns pertaining to scalability, network management, deployment and support for higher layer functionality such as error, flow and congestion control. In this context, an alternative architecture is, Application layer multicast (End Systems Multicasting), where at Application layer, implements all multicast related functionality including membership management and packet replication. This shifting of multicast support from routers to end systems has the potential to address the most problems associated with IP multicast. In Application-layer multicast, applications arrange themselves as a logical overlay network and transfer data within the overlay network (between end hosts). In this context, we study these performance concerns in the context of the NARADA protocol (an application layer multicasting protocol). In Narada, end systems self-organize into an overlay structure using a fully distributed protocol. We present details of NARADA and evaluate it using NS-2 simulations.

Keywords: multicast, end system multicast, graph, network, random numbers, routers, links, bandwidth, latency, minimum cost spanning tree, unicast , datagram, ip- multicast, narada, performance, dvmrp.

GJCST-E Classification : C.2.2

APPLICATIONLAYERMULTICASTINGOVERLAYPROTOCOLNARADAPROTOCOL

Strictly as per the compliance and regulations of:

Application Layer Multicasting Overlay Protocol – NARADA Protocol

G. Sankara Rao [α], E. Jagadeeswararao [σ] & N.Sai Prathyusha [ρ]

Abstract – The conventional wisdom has been that Network Layer Internet protocol(IP) is the natural protocol layer for implementing multicast related functionality but it is still plagued with concerns pertaining to scalability, network management, deployment and support for higher layer functionality such as error, flow and congestion control. In this context, an alternative architecture is, Application layer multicast (End Systems Multicasting), where at Application layer, implements all multicast related functionality including membership management and packet replication. This shifting of multicast support from routers to end systems has the potential to address the most problems associated with IP multicast. In Application-layer multicast, applications arrange themselves as a logical overlay network and transfer data within the overlay network (between end hosts). In this context, we study these performance concerns in the context of the NARADA protocol (an application layer multicasting protocol). In Narada, end systems self-organize into an overlay structure using a fully distributed protocol. We present details of NARADA and evaluate it using NS-2 simulations. Our results indicate that the performance penalties are low both from the application and the network perspectives. We believe the potential benefits of transferring multicast functionality from routers to end systems, significantly outweigh the performance penalty incurred.

Keywords: multicast, end system multicast, graph, network, random numbers, routers, links, bandwidth, latency, minimum cost spanning tree, unicast , datagram, ip- multicast, narada, performance, dvmrp.

I. Introduction

Recently, more and more group communication applications (e.g., video-conferencing, online-gaming, and long-distance education) have emerged with the increasing popularity of the Internet. To support such multi-user applications, multicast is considered as a very efficient mechanism since it uses some delivery structures (e.g., trees or meshes) to forward data from senders to receivers, aiming to reduce duplicate packets, whereas a separate delivery path is built for each sender-receiver pair when simple unicast scheme is adopted.

Initially, multicast is implemented at the IP layer,in which a tree delivery structure is usually employed, with data packets only replicated at branching nodes. In IP multicast, the multicast tree nodes are network routers. However, due to many technical and marketing reasons, such as the lack of a scalable inter-domain multicast routing protocol, the requirement of global deployment ofmulticast-capable IP routers and the lack of appropriate pricing models, etc., IP multicast is still far from being widely deployed.

To resolve the deployment issues of IP multicast, application layer multicast has been proposed as an alternative solution to realize multicast in the Internet.

This paper is organized as follows: Existing System and its Disadvantages, Advantages of the proposed system, Narada features, Narada Design, Our implementation of Narada.

II. Existing System

IP multicast (Fig.1) is a bandwidth-conserving technology that reduces traffic by simultaneously delivering a single stream of information to potentially thousands of corporate recipients and homes. IP Multicast delivers application source traffic to multiple receivers without burdening the source or the receivers while using a minimum of network bandwidth.

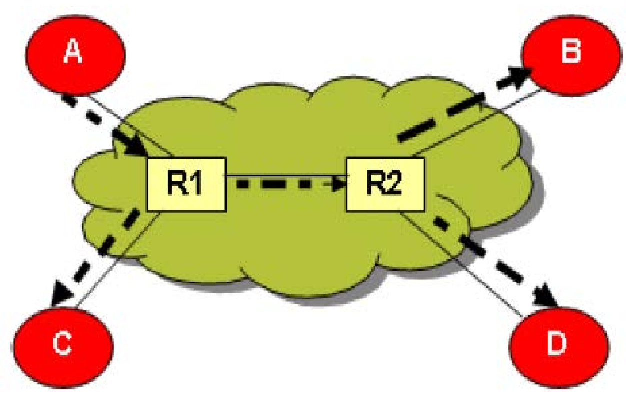


Figure 1 : IP Multicasting

Advantage of IP Multicast is that

No duplicate packets are sent across any physical link and hence there is efficient bandwidth utilization.

a) *Disadvantages of IP Multicast*

- The first problem is that IP Multicast requires every router to maintain the group state information. This violates the initially envisioned "stateless" principle

Author α: Assistant Professor, Dept. of CSE GVP College of Engg. for Women. Kommadi, Visakhapatnam, India.
e-mail: sankararao@gvpcew.ac.in
Author σ: Lecturer,School of IT, JNTUH Kukatpally, Hyderabad, India.
e-mail: jagadish@jntuh.ac.in
Author ρ : e-mail: nsaiprathyusha@gmail.com.

and it is also introduces a lot of complexity and has scalability constraints.

- The second problem is that IP Multicast tries to conform to the traditional separation of network and transport layers. This worked well in the unicast context but other features like reliability, congestion control, flow control and security are difficult to implement.
- The third and final problem is that it requires changes at the infrastructure level and hence it is not easy to deploy.

III. Proposed System

An alternative to this proposed system is the Application Layer Multicast (Fig.2) in which all the functionality of multicast is pushed to the end systems or end hosts. Application layer multicasting can implement many complex features of multicast functionality basically constructs an overlay structure among all hosts in the network and then sends messages to the either end hosts in the overlay structure, implementing all other features of multicast is easier at application layer rather tat network layer.

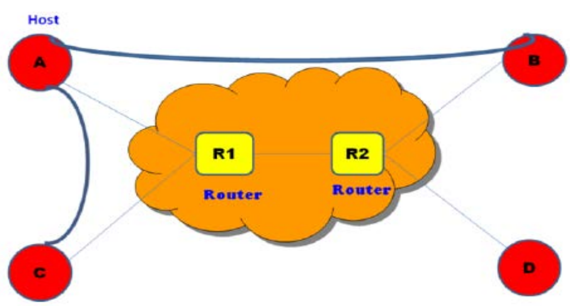


Figure 2 : Application Layer Multicasting

a) Advantages of Application Layer Multicast

- The overlay structure is built on existing physical links. so we may have multiple overlays over a single physical link hence there will be redundant traffic across the links.
- No more routers need to maintain the per group state information. And the end systems or end hosts take up this responsibility. Since these end systems are part of very few groups it becomes easy to scale the systems.
- Supporting higher layer features such as error, flow, and congestion control can be significantly simplified by leveraging well understood unicast solutions for these problems, and by exploiting application specific intelligence.

IV. Narada Features

Narada is the protocol to implement End System Multicasting. It has many features like:

a) Self organizing

The construction of the end system overlay in fully distributed fashion and is adaptive to dynamic changes in group membership.

b) Overlay efficiency

The tree constructed is efficient both from application and network perspective and the number of redundant packets transmission is kept minimal. However the definition of efficiency differs for every application.

c) Self Improving

The end systems gather network information in a scalable fashion. So the overlay structure improves as more information becomes available.

d) Adaptive to network dynamics

The overlay created adapts to long term variations in internet path characteristics and it is resilient to the inaccuracies in the measurement of these quantities.

V. Narada Protocol Design

a) Tree and Mesh Creation

Narada creates a mesh, a highly connected graph between all the nodes (end systems) in the group. It then creates a minimum cost spanning tree among all the end hosts using the mesh. A mesh based approach is used for multi source applications. Also a single shared tree is susceptible to a central point of failure. They are not optimized for a single source. It is important to create a good mesh for creating good trees. A good mesh has the following properties: *Firstly*, quality of a path between any two members is comparable to the unicast path between the two members. *Secondly*, each member is connected to a limited number of neighbors in the mesh. Narada runs a variant of standard distance vector routing algorithms and it creates reverse shortest path spanning trees for each source.

b) Group Management

Narada keeps the mesh connected, to incorporate new members into the mesh and to repair possible partitions that may be caused by members leaving the group or by member failure. The burden of group maintenance is shared jointly by all members. To achieve a high degree of robutness, our approach is to have every member maintain as list of all other members in the group. Since Narada is targeted towards medium sized groups, maintaining the complete group membership list is not a major overhead. Every member's list needs to be updated when a new member joins or an existing member leaves. The challenge is to disseminate changes in group membership efficiently, especially in the absence of a multicast service provided by the lower layer. We tackle this by exploiting the mesh to propagate such information.

c) Member Join

The joining member randomly selects a few group members from the list available to it. And sends the messages requesting to be added as neighbor, it repeats the process until it gets a response from some member, when it has successfully joined the group. Having joined, the member then starts exchanging refresh messages with its neighbors.

d) Member Leave and Failure

When a member leaves a group, it notifies its neighbors, and this information is propagated to the rest of the group members along the mesh. We also need to consider the difficult case of abrupt failure. In such a case, failure should be detected locally and propagated to the rest of the group. In this project, we assume a fail-stop failure model, which means that once a member dies, it remains in that state, and the fact that the member is dead is detectable by other members.

e) Mesh Performance

The constructed mesh can be quite sub -optimal, because

1. Initial neighbor selection by a member joining the group is random given limited availability of topology information at bootstrap.
2. Partition repair might aggressively add edges that are essential for the moment but not useful in the long run.
3. Group membership may change due to dynamic join and leave.
4. Underlying network conditions, routing and load may vary.

Narada allows for incremental improvement of mesh quality by adding and dropping of overlay links.

VI. Data Delivery

On the top of the mesh, Narada runs the distance vector protocol. Each member maintains a routing cost to the destination and also the path that leads to that node. A member M that receives a packet from source S through a neighbor N forwards the packet only if N is the next hop on the shortest path from *M* to *S*. Further, M forwards the packet to all its neighbors who use M as the next hop to reaches (fig. 7).

VII. Narada Implemenation & Results

a) Mesh Creation

We use the network entities given by JNS (Java Network Simulator) to create a mesh (Fig. 3). We create entities like nodes, links, routers etc. We'll assign weights to the links manually or can be done using a random number generator. The nodes have names 1, 2 …etc. the number of edges in the network for a number of nodes is also generated by random numbers. We try to have a highly connected graph. All those nodes which are not connected have a weight of a constant high valued number.

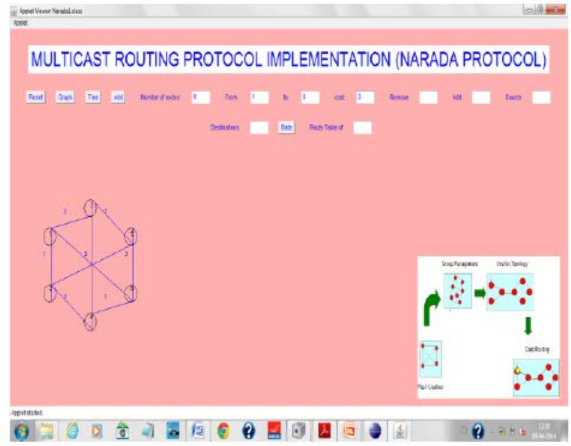


Figure 3 : Mesh Creation

b) Group Creation

In Narada every member of the group contains a list of all members in the group to which it is connected. So a Group Member object has a Node object and an array of nodes and costs to reach them in it. If a member is not connected to a node it has the constant value representing an unreachable node in it. A group is defined as a list of Group Member objects.

c) Member Join

When a new node wants to join a group, it brings along with it some information about its distance to any existing group member with it. The group join algorithm works as follows (fig.4).

In the first step, the list of the joining node is updated. All those elements to which it's not connected are added with unreachable weight to its list. Then it is added to the lists of all existing group members with corresponding weights. Finally it is added to the list of members of a group. When data routing has to be done a new spanning tree will be created with this node.

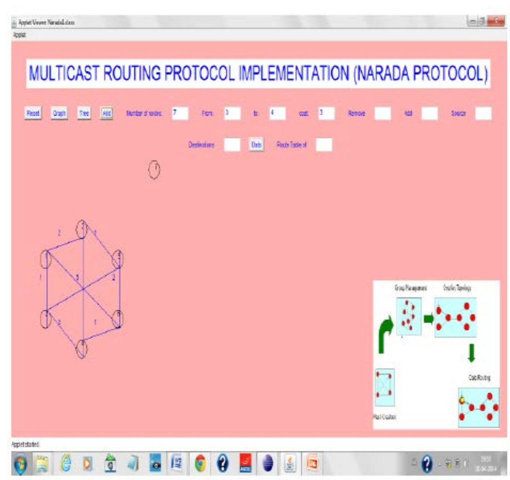


Figure 4 : Member joining the group

d) Member Leave

When a member leaves the group gracefully it informs other group members that it is leaving. Accordingly when he leaves his list is deleted and his record is deleted from the its of all other existing group members(fig.5).When data routing has to be done a new spanning tree will be created without this node.

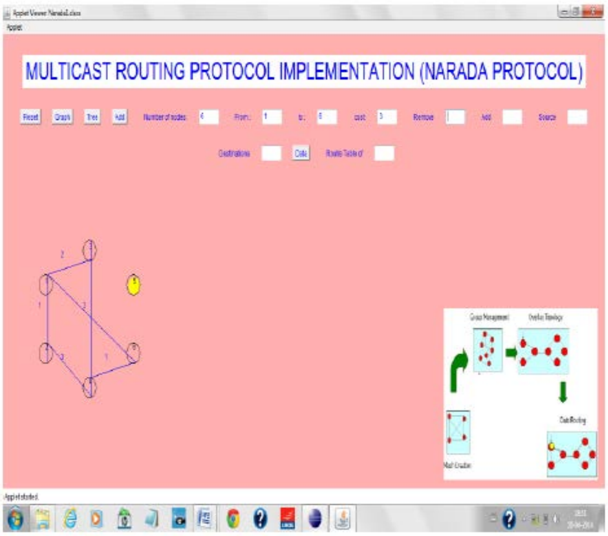


Figure 5 : Member leaving the group

e) Tree Creation

The entire structure of network consisting of all nodes and weighted edges is given to the spanning tree algorithm. We then use the Kruskal's algorithm to construct the minimum cost spanning tree (fig.6) among these nodes. We also calculate the start and end times for each message of the spanning tree and also the hop number in the tree.

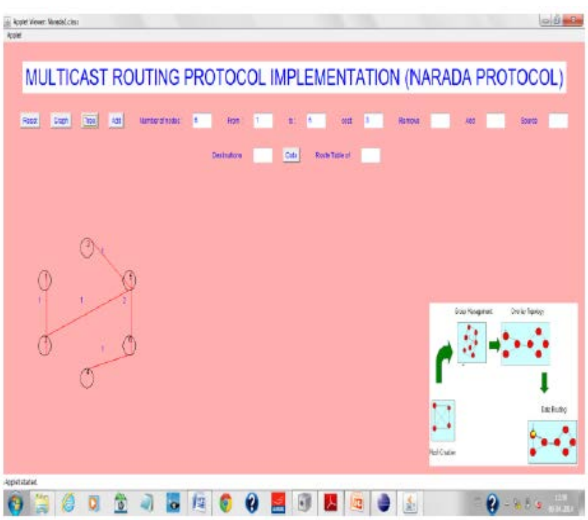


Figure 6 : Spanning Tree Construction

f) Data Delivery

The user enters a source and we consider the last node as the destination. We then extract a path from the spanning tree from the source to the destination. We then give the edges in the path to the simulator which sends the messages along those paths at the specified start times (fig.7).

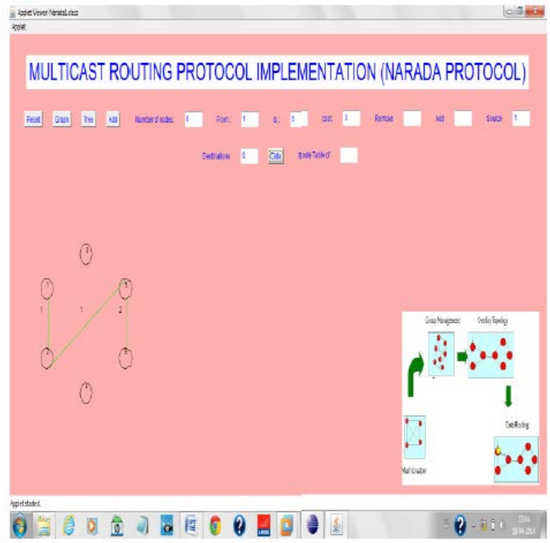


Figure 7 : Data Delivery

g) Routing Table

This DVMRP (Distance vector multicast Routing protocol)-like routing algorithm is iterative, asynchronous and parallel, and the multicast tree is generated based on the cooperative work of each node.(fig.8)

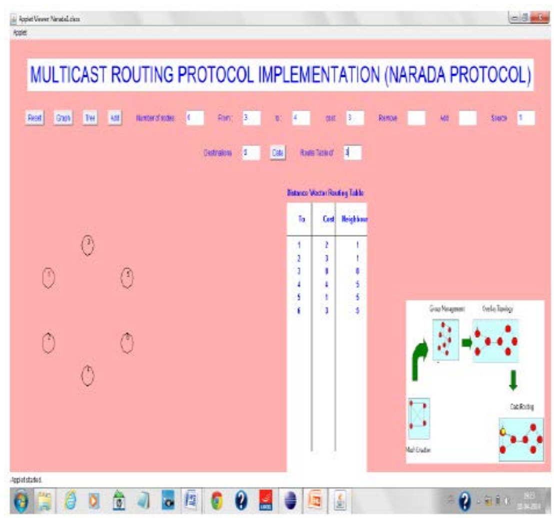


Figure 8 : Routing Table

NARADA uses DVMRP Algorithm as given below

h) DVMRP Algorithm

Initialization.

For all adjacent nodes V

$D^x(*,v)$ =infinity/* the * operator means "for all rows"*/

$D^x(v,v)=c(x,v)$

For all destinations, y

Send min $_wD^x(y, w)$ to each neighbor

Loop

Wait (until I see a link cost change to neighbor V
Or until I receive update from neighbor V)
If(c(x, V) changes by d)
For all destinations y: $D^x(y, V) = D^x(y,V) + d$
Else if
(Update received from V with respect to destination Y)
For the single destination
y:$D^x(Y,V)=c(X,V)+$ newval
If we have a new min ${}_wD^x(Y, w)$ for any destination Y
Send new value of min ${}_wD^x(Y, w)$ to all neighbors
Forever

i) NS2 SIMULATOR & NAM

Ns-2 is a discrete event simulator targeted at networking research. Ns-2 provides substantial support for simulation of TCP, routing, and multicast protocols over wired and wireless (local and satellite) networks. Ns-2 is written in c++ and an Object oriented version of Tcl called OTcl.

Nam is a Tcl/TK based animation tool for viewing network simulation traces and real world packet traces. It is mainly intended as a companion animator to the ns simulator.

NS-2 is a discrete event simulator and supports various flavors of TCP, many different models of unicast and multicast routing, along with different multicast protocols. It supports mobile networking including local and satellite networks. It also supports applications like web caching. And NS-2 uses NAM, an animation tool, developed in Tcl/Tk, to visualize the simulation packet traces which are created by running ns scripts. Thus ns-2 and nam could be used together to easily demonstrate different networking issues in a classroom environment.fig.9 shows the topology creation with ns-2 simulator.

Now, we make use of these to show the flow of packets (data delivery) over the network from one member to another member (fig.10)

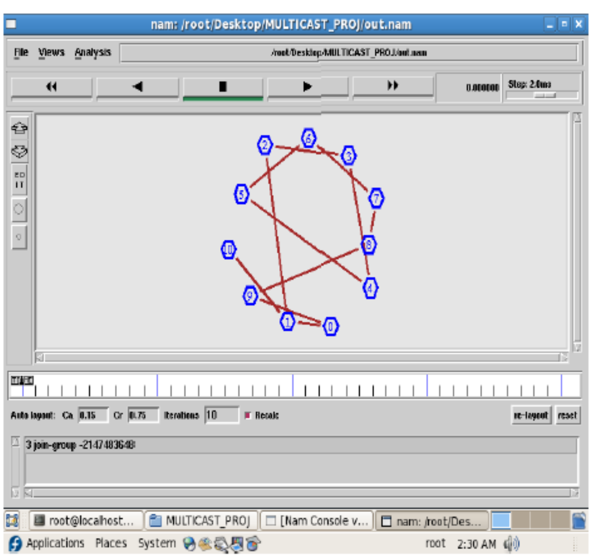


Figure 9 : Network Topology

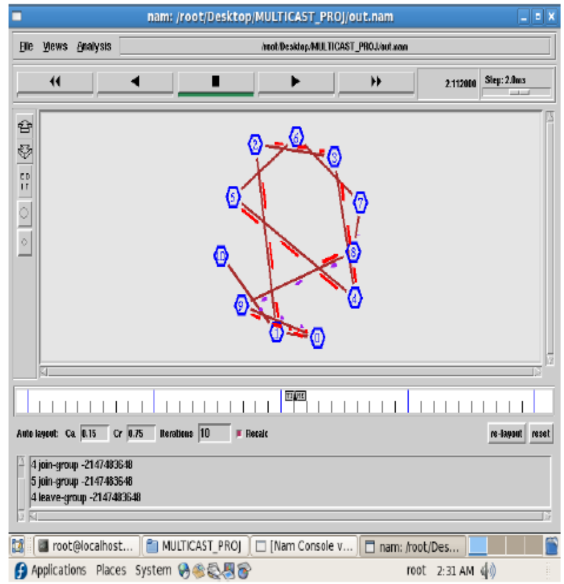


Figure 10 : Delivery of Multicasting packets

VIII. Results Analysis

We have considered two Parameters to measure the mesh (network) performance. One is the Throughput. And the other is the Latency(Delay). Throughput is nothing but, number of packets sent per unit time successfully. Latency refers to the time taken for a packet to reach the destination after their transmission. We conducted several Experiments to observe the mesh performance. Fig.11 shows the results generated for throughput with respective time. NARADA achieves better throughput as compared others for medium sized group member's mesh. Fig.12 shows the delay vs group size, but for small size groups delay is neglible while using narada protocol.

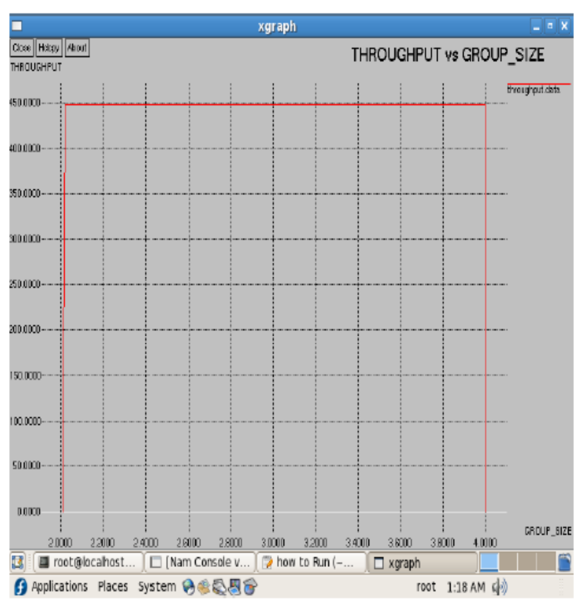


Figure 11 : Resultant Graph of Throughput vs Time

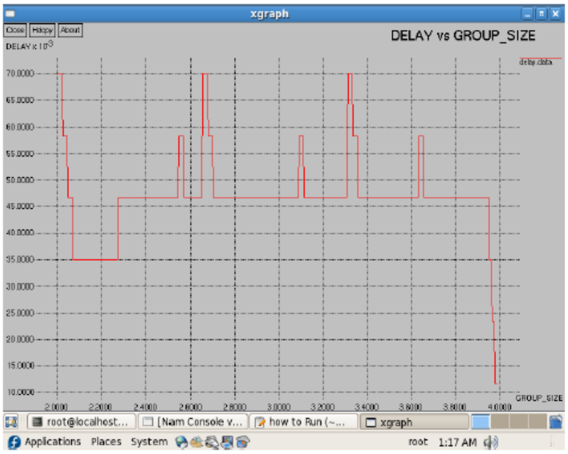


Figure 12 : Resultant Graph for Delay vs GroupSize

a) Application Layer Multicasting Applications

End system Multicasting is used *in Group Communication (i.e* Multiparty Conferencing session, Audio Conferencing, Video Conferencing). And these are also used in small to medium group size. And multiple sources

IX. Conclusion

End systems overlay is feasible. End Systems (Application Layer) Multicasting Addresses the problems associated with IP multicasting. Application layer Multicasting is easy to maintain. NARADA is Better for small sized groups from the results we drawn.

References Références Referencias

1. C. Partridge, D. Waitzman, and S. Deering. Distance Vector Multicast Routing Protocol. RFC 1075, 1988.
2. S. Banerjee, C. Kommareddy, and B. Bhattacharjee. Scalable application layer multicast. In Proceedings of ACM SIGCOMM, Aug. 2002.
3. Y.-H. Chu, S. G. Rao, and H. Zhang. A case for end system multicast. In Proceedings of ACM Sigmetrics, June 2000.
4. J. Liebeherr, M. Nahas, and W. Si. Application-layer multicasting with delaunay triangulation overlays. IEEE Journal on Selected Areas in Communications.
5. P. Francis. Yoid: Extending the Multicast Internet Architecture. White papar, http://www.aciri.org/yoid/.
6. S. Shi and J. S. Turner. Routing in overlay multicast networks. In Proceedings of IEEE INFOCOM, June 2002.
7. D. Pendarakis, S. Shi, D. Verma, and M.Waldvogel. ALMI: An application level multicast infrastructure. In Proceedings of the 3rd USNIX Symposium on Internet Technologies and Systems, Mar. 2001.
8. Y. Chawathe. Scattercast: An Architecture for Internet Broadcast Distribution as an Infrastructure Service. Fall 2000. Ph.D. thesis.
9. J. Jannotti, D. Gifford, K. L. Johnson, M. F. Kaashoek, and J. W. O'Toole Jr. Overcast: Reliable Multicasting with an Overlay Network. In Proceedings of the Fourth Symposium on Operating System Design and Implementation (OSDI), October 2000.
10. J. Jannotti, D. Gifford, K. L. Johnson, M. F. Kaashoek, and J. W. O'Toole Jr. Application-layer Multicast with Delaunay Triangulations. In IEEE Globecom, November 2001.

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 14 Issue 6 Version 1.0 Year 2014
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Performance Analysis of DSDV, AODV AND AOMDV Routing Protocols based on Fixed and Mobility Network Model in Wireless Sensor Network

By Romana Rahman Ema, Ashrafi Akram, Md. Alam Hossain & Subrata Kumar Das

Jessore University of Science and Technology, Bangladesh

Abstract- Wireless sensor networks (WSN) is capable of autonomously forming a network without human interaction. Each node in a WSN acts as a router, forwarding data packets to other nodes. Without routing protocols, these routers cannot work together in phase. A central challenge in the design of WSN is the development of routing protocols that can efficiently find routes in a network. The question is which criteria should be considered when selecting a routing protocol, for instance, energy consumption (battery life), bandwidth, or security? We selected energy consumption as this is the most important criterion in WSN. To find out the best routing protocol, we analyzed three routing protocols namely AODV (Ad-hoc On Demand Distance Vector), AOMDV (Ad-hoc On Demand Multiple Distance Vector), and DSDV (Destination Sequence Distance Vector). Overall performance of these protocols was analyzed by comparing end-to-end delay, throughput, normalized routing load, and energy consumption of the network.

Keywords: AODV, AOMDV, DSDV, end-to-end delay, throughput, normalized routing load, energy consumption, wireless sensor networks.

GJCST-E Classification : C.2.2

PERFORMANCEANALYSISOFDSDV,AODVANDAOMDVROUTINGPROTOCOLSBASEDONFIXEDANDMOBILITYNETWORKMODELINWIRELESSSENSORNETWORK

Strictly as per the compliance and regulations of:

Performance Analysis of DSDV, AODV AND AOMDV Routing Protocols based on Fixed and Mobility Network Model in Wireless Sensor Network

Romana Rahman Ema [α], Ashrafi Akram [σ], Md. Alam Hossain [ρ] & Subrata Kumar Das [ω]

Abstract - Wireless sensor networks (WSN) is capable of autonomously forming a network without human interaction. Each node in a WSN acts as a router, forwarding data packets to other nodes. Without routing protocols, these routers cannot work together in phase. A central challenge in the design of WSN is the development of routing protocols that can efficiently find routes in a network. The question is which criteria should be considered when selecting a routing protocol, for instance, energy consumption (battery life), bandwidth, or security? We selected energy consumption as this is the most important criterion in WSN. To find out the best routing protocol, we analyzed three routing protocols namely AODV (Ad-hoc On Demand Distance Vector), AOMDV (Ad-hoc On Demand Multiple Distance Vector), and DSDV (Destination Sequence Distance Vector). Overall performance of these protocols was analyzed by comparing end-to-end delay, throughput, normalized routing load, and energy consumption of the network. This was accomplished by using the Network Simulator, NS-2.34 over IEEE 802.11. The analysis shows that AOMDV is the best routing protocol in terms of energy consumption.

Keywords : AODV, AOMDV, DSDV, end-to-end delay, throughput, normalized routing load, energy consumption, wireless sensor networks.

I. Introduction

A wireless Sensor Network (WSN) is a spatially distributed autonomous system which is a collection of many power-conscious sensor nodes, having wireless channel to communicate with each other [21]. Wireless networks are characterized by infrastructure-less, random and quickly changing network topology. This makes the traditional routing algorithms fail to perform correctly since they are not strong enough to accommodate such a changing environment [7].Efficient routing protocols can provide significant benefits in terms of both performance and reliability. Since latency, reliability and energy consumption are inter-related with each other, the proper selection of the routing protocol to achieve maximum effi-ciency is a challenging task [2]. Due to this fact, a detailed analysis becomes necessary and useful at this stage.

The application of wireless sensors in our real life such as controlling temperature and acceleration sensor is shown below.

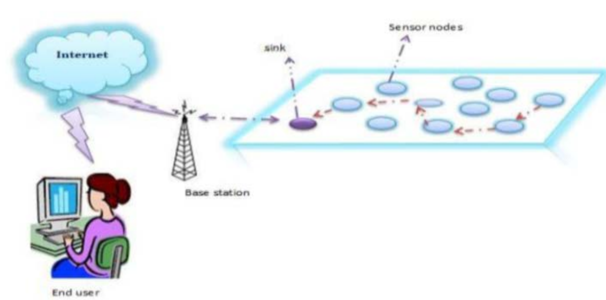


Figure 1 : Accessing WSNs through Internet

Well-organized routing in a sensor network requires that routing protocol must minimize network energy dissipation and maximize network lifetime [21]. Performance comparison of routing protocols has been done in various research papers like D. D. Chaudhary, Pranav Pawar and Dr. L. M. Waghmare [2] studied and compared performance evaluation of Wireless Sensor Network with different Routing Protocols, Adel. S. Elashheb [3] evaluated the performance of AODV and DSDV Routing Protocol in wireless sensor network environment but our simulation results are based on different simulation environment (fixed and mobility) and simulation parameters. Simulation result shows that the performance of AOMDV routing protocol is better than AODV and DSDV in terms of throughput, energy consumption, normalized routing load and end-to-end delay.

II. Related Work

Charles E. Perkins, Elizabeth M. Royer, Samir R. Das and Mahesh K. Marina compared the performance of DSR and AODV, two prominent on-demand routing

Author α: Dept. of Computer Science and Engineering (CSE) Jessore University of Science and Technology, Jessore, Bangladesh.
e-mail: romana18cse@yahoo.com.,
Author σ: Dept. of Computer Science and Engineering (CSE) Jessore University of Science and Technology, Jessore, Bangladesh.
e-mail: ashjstu@gmail.com.
Author ρ: Dept. of Computer Science and Engineering (CSE) Jessore University of Science and Technology, Jessore, Bangladesh.
e-mail: alamcse_iu@yahoo .com.
Author ω : Dept. of Computer Science and Engineering (CSE) Jessore University of Science and Technology, Jessore, Bangladesh.
e-mail: sdas_ce@yahoo.com

protocols for ad hoc networks[1]. The general observation from the simulation these is that for application-oriented metrics such as delay and throughput, DSR outperforms AODV in less "stressfulll" situations (i.e. smaller number of nodes and lower load and/or mobility). AODV, however, outperforms DSR in more stressful situations, widening performance gaps with increasing stress (e.g., more load, higher mobility). DSR, however, consistently generates less routing load than AODV.

Adel. S. Elashheb [4] evaluated the performance of AODV and DSDV Routing Protocol in wireless sensor network environment. In this paper two protocols AODV and DSDV had been simulated using NS-2 package and compared in terms of packet delivery fraction, end to end delay and throughput in different environment; varying period of pause time and the number of expired nodes. Simulation results show that AODV routing protocol had better performance in terms of packet delivery fraction and throughput but, AODV suffers from delay.

III. Description of The Routing Protocols

a) DSDV

DSDV is a proactive routing protocol and is based on the idea of the Bellman-Ford Routing Algorithm with certain improvements [2]. In DSDV, each node maintains a routing table, which lists all available destinations, next hop to each destination and a sequence number generated by the destination node to provide loop freshness [11] [12] [20]. The sequence numbers are generally even if a link is present; else, an odd number is used. Using such routing table stored in each node, the packets are transmitted throughout the network [20]. The routing table is updated at each node either with advertisement periodically or when significant new information is available to maintain the consistency of the routing table with the dynamically changing topology of the network [20]. If there is a failure of a route to the next node, the node immediately updates the sequence number and broadcasts the information to its neighbors. After receiving routing information the node checks its routing table. If it does not find such entry into its routing table then it updates the routing table with routing information it has found. If the node finds that it has already entry into its routing table then it compares the routing table entry with the sequence number of the received information with and updates the information. When a node receives a new route update packet; it compares it to the information available in the routing table and the routing table is updated based on the following criteria [13] [19]

- If the destination sequence number of receiving packets is greater, then the routing table information is replaced with the information in the new route update packet.
- When the destination sequence numbers are the same, the routing table is updated by selecting the route with better metric.

Thus, DSDV is not suitable for highly dynamic networks.

Figure 2 shown below represents the implementation of DSDV protocol. Table 3.1 illustrates the routing information stored in node 6 of Figure 2. The Destination column represents the destination nodes throughout network. Next hop field column represents the neighbor node which can forward data to the destination node. Metric column represents the number of hops the destination is away from node. Sequence number column represents the destination sequence number [9].

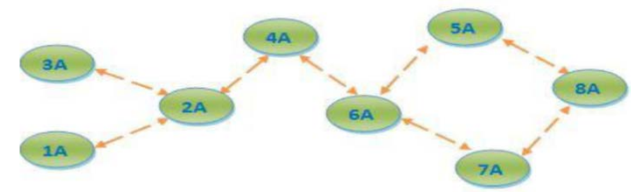


Figure 2 : Implementation of DSDV Protocol [9]

Table 3.1 : Routing Table of Node 6

Destination	Next Hop	Metric	Sequence Number
1A	4A	3	S213_1
2A	4A	2	S899_2
3A	4A	3	S343_3
4A	4A	1	S441_4
5A	5A	1	S155_5
6A	6A	0	S067_6
7A	7A	1	S717_7
8A	5A/7A	2	S582_8

b) AODV

AODV is a development on the DSDV algorithm because it decreases the number of broadcasts by creating paths on-demand. AODV discovers routes as and when necessary. For inactive communication, it is not necessary to establish routes to destination. Whenever desired routes are not getting within the expected time, time to live (TTL) of AODV get expired. The nodes of every valid route employ routing tables to store routing information. The route table stores: <destination addr, next-hop addr, hop count, routing flags, destination sequence number, network interface, life_time> [15]. Sequence numbers are used to provide up-to-date routing information for route freshness criteria and for loop prevention. Life-time is updated every time the route is used. Whenever a node wishes to send a packet to some destination, it checks its routing table to determine if it has a current route to the destination. If it has found current route, then it forwards the packet to the next node, otherwise it initiates a route discovery process [15].

AODV uses different control messages for the discovery and maintenance of routes. They are Route Request Message (RREQ), Route Reply Message (RREP), Route Error Message (RERR), HELLO Messages [7] [14]. By creating a Route Request (RREQ) message, AODV initiates Route discovery process to reach from source to destination. Every time when the source node sends a new RREQ, broadcast ID gets incremented. After receiving of request message, each node checks the request ID and source address pair. The new RREQ is rejected if there is already RREQ packet having the same pair of parameters. If a node has no route entry for the destination, it rebroadcasts the RREQ with incremented hop count parameter. RREP contains the route information about the destination which is mentioned in RREQ and it is transmitted to the sender of the RREQ If there is a link failure of a valid route, a RERR message is generated by the node upstream of a link breakage to inform other nodes about the link failure. In AODV, Hello messages are broadcasted in order to know neighborhood nodes and to notify the neighbors about the activation of the link. Absence of hello message is defined as an indication of link failure [7] [14].

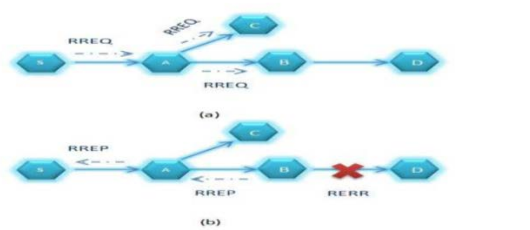


Figure 3 : AODV Route discovery process

Figure 3 shows the route discovery process of AODV. If node S needs a route to node D, then node S sends route request to A. Similarly node A broadcast route request to its neighbors. If node D receives RREQ, it makes a reverse route entry for S and sending RREP message. If link failure occurs between B and D, it sends RERR message.

c) AOMDV

The motivation for designing AOMDV is to compute multiple loop free and link disjoint paths in highly dynamic ad hoc networks where the link breakage occurs repeatedly [17]. It is the extension of AODV routing protocol [2] [10] [16]. AOMDV maintains a routing table for each node containing a list of the next-hops and its associated hop counts. Every next hop has similar sequence number for maintaining of a route. To send route advertisements, each node maintains the advertised hop count of the destination. If any node's hop count is less than the advertised hop count, then loop freshness is guaranteed for that node by receiving alternate paths to destination. In the case of a route failure, AOMDV uses alternate routes [2]. In AODV routing protocol, a route discovery procedure is needed for each link failure. Performing such procedure causes more overhead and latency also [17]. In the case of AOMDV, new route discovery process is required only when all the routes fail [10] [16]. In AOMDV, a source initiates a route discovery process if it needs a communication route to a destination. The source broadcasts a route request (RREQ) along a unique sequence number so that duplicate requests can be discarded. After receiving the request, an intermediate node record previous hop. If it has a valid and fresh route entry to the destination in its routing table, then it sends a reply (RREP) back to the source. If it has no valid and fresh route entry, it rebroadcast the RREQ. The nodes on reverse route towards source update their routing information by establishing multiple reverse paths. Duplicate RREP on reverse path is only forwarded if it contains either a larger destination sequence number or a shorter route found [10] [16].

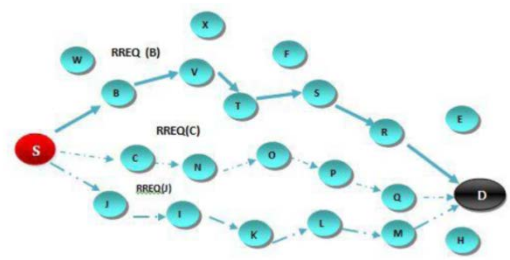


Figure 4 : Route Discovery Procedures in AOMDV

Table 3. 2 : Routing Table for Node S

Destination	Next hop	Number of hops	Destination Sequence Number
D	B	5	S1
D	C	5	S2
D	J	5	S3

Figure 4 shows the route discovery process of AOMDV and in table 3.4, it is shown that each entry in the routing table consists of all available destinations, next hop towards each destination (i.e. B, C and J), number of hops required to reach destination and a destination sequence number.

IV. Simulation Model

To configure both of the network models, we used the following simulation parameters which we have discussed in table 4.1.

Table 4.1 : Simulation Parameters

Parameters	Details
Simulator	NS-2.34
Node Placement	Random, Fixed
No. of Nodes	12,16,20,24,28,32,36
No. of sink (destination)	One(Node 0)
No. of sources	35 (Node 1 to 35)
Area of simulation	2500 m *1000m
Packets generated by each source	1000
Total packets generated in N/W	36*1000=36000
Size of each packet	1000 bytes
Model	Energy Model
Initial energy	1000J
Transmission Range	250m
Radio model	Two Ray Ground
Protocols	AODV,DSDV,AOMDV
Max speed	28m/s
Traffic type	FTP
MAC	Mac/802_11
Bandwidth	11mb
Simulation time(in sec)	1000 sec
Antenna Type	Omni directional
Link Layer Type	LL
Interface queue type	Queue/Drop tail
Channel type	Channel/Wireless channel
Network interface type	Phy/WirelesssPhy

V. Performance Results

a) Performance Metrics

i. *Average end-to-end delay*

Average end-to-end delay is the average time from the transmission of a data packet at a source node until packet delivery to a destination which includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue, retransmission delays at the MAC, propagation delay for propagation and transfer times and carrier sense delay for carrier sensors [7] [18].

ii. *Average Throughput*

Throughput is the total number of packets that have been successfully delivered from source node to destination node and it can be improved with increasing node density [7] [18].

iii. *Normalized Routing Load*

It is the number of routing packets transmitted per data packet delivered at the destination [18].

iv. *Energy Consumption*

$$\frac{\Sigma \text{Percentage Energy Consumed by all nodes}}{\text{Number of all nodes}} \quad [18]$$

v. *Remaining Energy*

Remaining Energy is defined as Initial Energy – Energy Used [18]

b) Result and Analysis

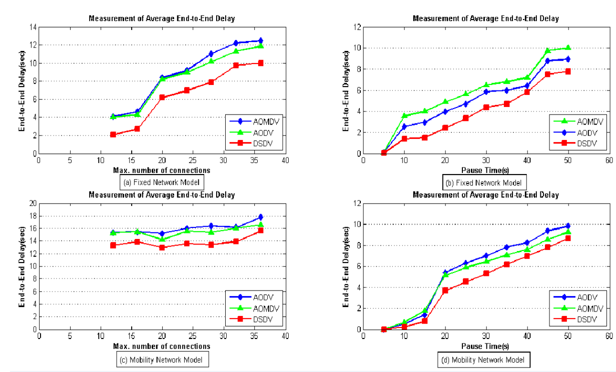


Figure 6 : Measurement of average end-to-end delay varying maximum number of connections and pause time (sec.)

Figure 6 (a, c) illustrates a comparison among AODV, DSDV, and AOMDV in terms of end-to-end delay based on fixed and mobility scenario by varying maximum number of connections (number of nodes) respectively. Figure 6 (a) shows that the average end-to-end delay of DSDV stays much lower than AODV and AOMDV. The average end-to-end delay increases with the increased number of connections. The numbers of connections were varied as 12,16,20,24,28,32,36 nodes. After increasing number of connections more than 16, end-to-end delay increase much higher because of queuing and retransmission delay. In heavy traffics load as the maximum number of connections increase, the number of packets delivery also increase. That's why queue is getting full. DSDV routing protocol tries to drop the packets if it is not possible to deliver them. This cause less delay and most dropping packets are retransmitted over again that causes retransmission delay. On the other hand, AODV and AOMDV both routing protocol allow packets to stay in the send buffer for 30 seconds for route discovery and once the route is discovered, data packets are forwarded on that route to be delivered at the destination. In this graph, result shows that AOMDV performs significant more delay than AODV after 24 connections. Due to multi paths in AOMDV there can be many stale routes which may contribute to more delay than AODV. As the number of connections increases, the end-to-end delay also increases in a fixed scenario.

To analyze the effects of mobility, figure 6 (c) shows that end-to-end delay of AODV is comparatively higher than AOMDV and DSDV at high density. When queue is getting free from 16-20 numbers of connections, the delay of DSDV is decreased because it consumes less time to deliver packets. AOMDV loses fewer packets than AODV (1-2% less) at high density in mobility cases. From 30-32 numbers of connections, the delay is almost similar in AODV and AOMDV because of less queuing delay. When a links failure is occurred in mobility scenario, the route discovery process of AODV causes very long delays for large scale networks due to the amount of control packets transmitted. These delays result in deliver packets waiting in the queues being dropped .The average end-to-end delay is 3% higher than fixed scenario because of high mobility environment, topology change rapidly.

Figure 6 (b, d) respectively shows the average end-to-end delay versus pause time by taking the each time delay which we considered as simulation time for AODV, AOMDV, DSDV routing protocol. Figure 6 (b) shows that DSDV performs less delay than AODV and AOMDV with 36 connections and with pause time varying from 0-60 second's when simulation is started. As the simulation time increases, the average end-to-end delay increases because of number of packets generates by each source increases. If there is no alternate path or unable to deliver packets from source to destination, both AODV and AOMDV allow packets to stay in buffer for 30 sec. This causes the data packets waiting to be routed. The packets are dropped if the time the packets have been in buffer exceeds the limit (30s). In the case of a link failure at a node, AOMDV can find an alternate route whereas AODV is caused to be ineffective at that point. Being a proactive routing protocol the packet drop of DSDV is maximum than the other two protocol when its fails to find a route. So delay of DSDV is less than AODV and AOMDV.

Figure 6 (d) shows the effects of mobility, each node chooses a random destination and moves there at a high speed on expiry of its pause time. The observation is that the AOMDV routing protocol outperforms AODV when the pause times varies from 10 to 20 sec .But AODV outperforms AOMDV when the pause time is high that is varying from 26 to 50 sec.

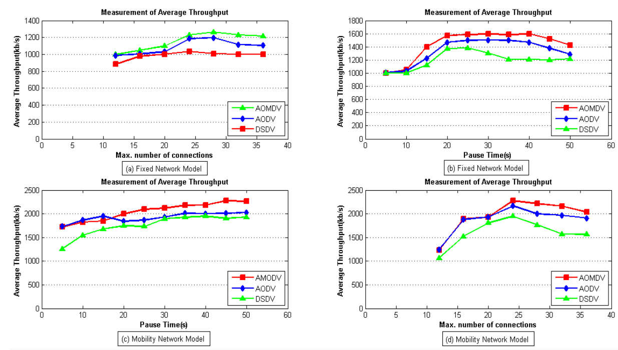


Figure 7 : Measurement of average throughput varying maximum number of connections and pause time (sec.)

Figure 7(a, d) illustrates a comparison among AODV, DSDV, and AOMDV in terms of average throughput based on fixed and mobility scenario by varying maximum number of connections (number of nodes). The numbers of connections were varied as 12,16,20,24,28,32,36 nodes respectively. It can be observed from the figure 7 (a) that the average throughput of AODV and AOMDV routing protocol increases at low density in between the number of connections from 12 to 28 and AOMDV outperforms AODV. This is because whenever the packets are dropped, most of the missing packets are retransmitted again over multiple reliable routes from source or intermediate node to destination. At high density like from 32 numbers of connections, the average throughput decreases because of packet lost. Packets loss is minimum in both AOMDV and AODV than DSDV.DSDV provides much packets drop at high density from 28 number of connections. That's why its throughput is comparatively less than AODV and AOMDV.

Figure 7(d) shows that mobility affects the throughput of AODV, AOMDV and DSDV differently. For randomly changing topology, at low density from 12 to 20 numbers of connections, the throughput of AODV and AOMDV is almost similar. But at high density from 28 connections, the possibility of link failures increases. This causes the average throughput decreases of AODV, AOMDV, and DSDV routing protocol. AOMDV is able to select multiple paths to achieve more loads balancing in a high mobility to delivery packets than AODV and DSDV respectively.

As seen in figure 7 (b), the average throughput value of AOMDV and AODV increases and maintains its value with the pause time increases from 5 to 30 sec because of the proper receiving of packets and less packet drop. The average throughput decreases with the pause time varying from 35 sec because the amount

Global Journal of Computer Science and Technology (E) Volume XIV Issue VI Version I Year 2014

of dropping packets increases at the time of interface queue, buffer is getting full. The average throughput increases comparatively in DSDV varying pause time 5 to 25 sec. Throughput decreases as it needs to broadcast periodic updates. DSDV throughput is comparatively less than AOMDV and AODV respectively.

Figure 7(c) shows that the mobility affects the throughput of AODV, AOMDV and DSDV differently varying the pause time. AODV outperforms AOMDV when pause time increases from 5 to 15 sec. The reason behind this is when mobility is low, the occurrence of link failure is less and packets drop is less than AOMDV. As the pause time increase from 16 sec AOMDV outperforms AODV. This is because if the node mobility is high, then occurrence of link failure increases and as we said before in AOMDV as if one path fails or congested, an alternate path is utilized to deliver packets and it maximizes the throughput than AODV. With respect to varied pause time as from 5 to 20 sec, throughput increases because of less periodic updates of routing table. DSDV shows more variation of throughput if the node mobility is high. Thus its throughput decreases quicker as pause time increases from 25 sec and throughput increases again when pause time is 30 sec. AOMDV provides more data packets delivery than AODV and DSDV respectively.

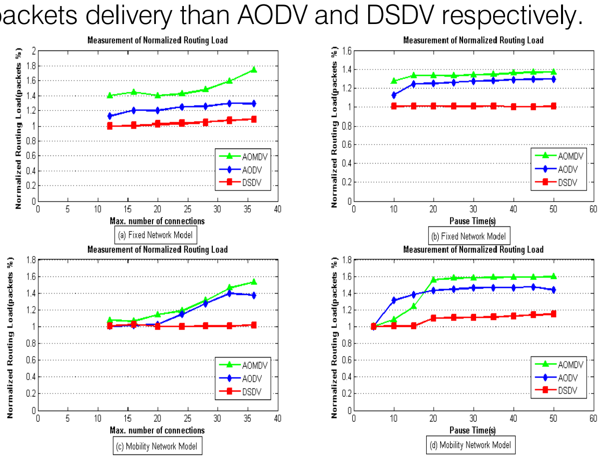


Figure 8 : Measurement of normalized routing load varying maximum number of connections and pause time (sec.)

Figure 8 (a, c) illustrates a comparison among AODV, DSDV, and AOMDV in terms of normalized routing load based on fixed and mobility scenario by varying maximum number of connections (number of nodes). The numbers of connections were varied as 12,16,20,24,28,32,36 nodes respectively. In figure 8 (a), it is observed that AOMDV has more normalized routing load as compared to the DSDV and AODV .For both AOMDV and AODV, the NRL increases as number of connections increases except number of connections 20, 30 respectively. This is because for fixed scenario with smaller number of connections, a link failure is very rare and there is less control packets to route discovery such as hello message, RREQ, RREP, and RERR. DSDV has the least NRL which remain stable than AOMDV and AODV in case of low and high numbers of connections density by varying 12,16,20,24,28,32,36. DSDV does not adapt to increase so much because the difference of routing update interval at every 15 seconds in the network is not very noticeable. AOMDV is a multipath routing protocol and if the current route breaks it searches for alternate paths by flooding the network with RREQ packets. AODV being a unipath routing protocol, the packet delivery along that route stops in the case of link breakage. So NRL of AODV is less than AOMDV.

Figure 8(c) shows the performance of NRL as a function of mobility. DSDV gives the lowest NRL, except at initially the NRL is slightly increased than AODV and AOMDV, when numbers of connections are in between 12 to 16 numbers of connections. This means DSDV sends periodic updates which increase routing load in the mobility network. In case of mobility by varying high density from 17 numbers of connections, more link failures occur than fixed scenario .To detect and handle the pressure of routing load with large number of connection, AOMDV sends HELLO packets periodically which gives higher routing packet overload than AODV.

Figure 8 (b, d) illustrates a comparison among AODV, DSDV, and AOMDV in terms of NRL based on fixed and mobility scenario by variations of pause time from 5 to 60 sec which we consider for simulation time. In figure 8 (b), AOMDV outperforms AODV and DSDV. It is clear from the figure that the NRL of AOMDV and AODV increases linearly with varying pause time 5 to 60 sec and this is because for a static network, max. Speed is of 0 m/s. That's why in the case of less link failure, DSDV's NRL is quite stable with an increasing number of pause time from 15 sec even though its delivery get increasingly worse. The effects of mobility are particularly visible in figure 8 (d). AOMDV outperforms AODV except pause time at 5 to 15 sec. Because in this case, the routing packets travel through more hops to reach the destination that increase the frequency rate of route discovery which is less than AOMDV. For DSDV the NRL remains almost unaffected by variations in pause time from 10 to 20 sec and with the increases of pause time from 20 sec, the routing load increases.

AOMDV being a multipath routing protocol and it searches for alternate paths if the current route breaks by flooding the network with RREQ packets. Hence AOMDV has more normalized routing load than AODV in both fixed and mobility scenario due to AODV being a unipath routing protocol.

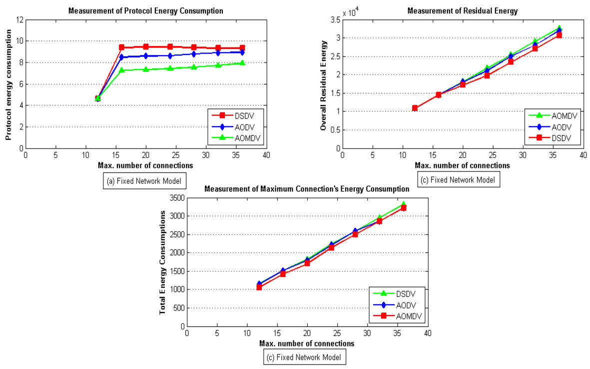


Figure 9.1 : Measurement of protocol energy consumption, residual energy and energy consumption of maximum number of connections (fixed network model)

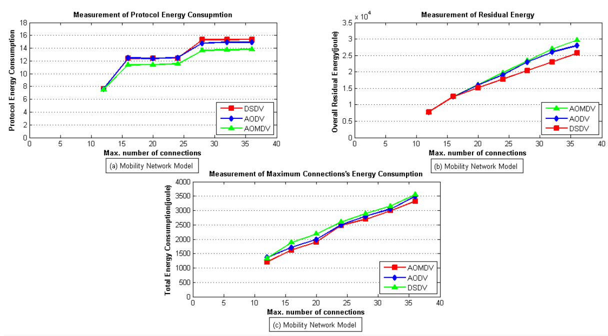


Figure 9.2 : Measurement of protocol energy consumption, residual energy and energy consumption of maximum number of connections (mobility network model)

Figure 9.1 (a, b, c) and Figure 9.2 (a, b, c) shows protocol energy, remaining energy and the maximum number of connections energy consumption respectively. Figure 9.1 (a) and 9.2 (a) shows that DSDV protocol consumes more energy compared to AOMDV and AODV. It is clear from the figure 9.2(a) that in mobility scenario, all the protocol consumes more energy than fixed scenario. The life time (battery) of the node for AOMDV is higher than other protocol. To utilize the same path for route discovery process of DSDV, the node life time expires (battery power) which consumes more bandwidth and energy than reactive protocols like AOMDV and AODV. In the case of a link failure, AOMDV has the ability to make longer battery and node's life time because of the proper utilization in choosing a path. Figure 9.1 (b) and 9.2(b) shows the overall residual energy of each route in the route discovery process. The overall residual energy of AOMDV and AODV in both cases higher than DSDV because of proper utilization stale routes and choosing alternate paths when it's needed. DSDV routing protocol is updated its all routing protocols if its need to be changed. For this reason residuals energy is less than AODV and AOMDV. Figure 9.1 (c) and 9.2(c) depicts that the maximum number of connection energy consumption. The number of sources of DSDV consumes more energy because its routing table updated at every 15 seconds in the network. For mobility cases in DSDV lots of link failure occurs and mostly drop packets are needed to retransmit on a same path which expires a sensor node battery life time than on-demand routing protocols (AODV and AOMDV). Both on-demand protocols have the ability to choose alternative path if link failure occur.

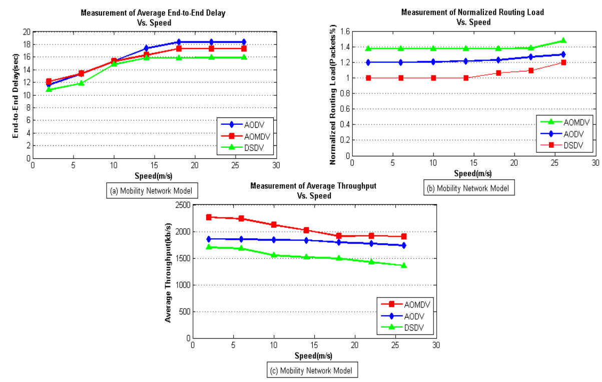


Figure 10 : Measurements of Speed vs. Average Throughput, Speed vs. Normalized Routing Load and Speed vs. Average End-to-End Delay

Figure 10 (a, b, c) show the comparison among AODV, DSDV, and AOMDV in terms of speed vs. end-to-end delay, normalized routing load and throughput respectively by varying speed such as 2,6,10,14,18,22, 26 m/s (average speed 4 m/s). Figure 10 (a) shows average end-to-end delay vs. speed. End-to-End delay increases as speed increases. AODV outperforms AOMDV and DSDV respectively except as the speed of nodes is varied from 2 to 10 m/s. In case of a link failure at a node, AOMDV can find an alternate route whereas AODV is caused to be ineffective at that point. DSDV shows less delay because it immediately drops the packets when there is a link failure. The results show that in "low mobility" situation, AODV protocol gives approximately same end-to-end delay as that of AOMDV protocol but in "high mobility" situation, AODV outperforms AOMDV protocol. Figure 10 (b) shows Normalized routing load vs. speed. AOMDV has the highest normalized routing load than AODV and DSDV. As we seen from the figure, the NRL value for AOMDV and DSDV increases very less (the difference is unnoticeable) till 2 to 14 m/s. If any route fails in AOMDV, AOMDV tries to find alternate multiple routes which tend to incur greater routing packets. While a node moves at a high speed, a source node generate more RREQs to find an alternate route. For DSDV protocol as node speed increases, the topology changes occur quickly, and thus DSDV has fewer chances to make available routes at once.

Figure 10 (c) shows the effect of average throughput, throughput decreases as speed increases. If speed of each mobile nodes increases, the source to destination distance increases which makes less packets delivery and causes more packets drop. This is because it has gone out of packets transmission ranges since finding the route requires more and more routing traffic as speed increases. AOMDV outperforms AODV and DSDV. As AOMDV and AODV both are on demand routing protocols, they have the ability to deal with high mobility speed for delivering good numbers of packets.

VI. Conclusion and Future Work

This paper evaluated the performance of the well-known routing protocols in wireless sensor network on the basis of fixed and mobility network model in terms of average throughput, average end- to-end delay, normalized routing load, energy consumption, protocols residual energy, total energy consumption of each nodes, speed vs. throughput, speed Vs. end-to-end delay, speed vs. normalized routing load with different simulation period and maximum number of connections. Being a proactive routing protocol, DSDV immediately drops the packets in the case of a link failure. Therefore, it has less delay than AOMDV and AODV in both fixed and mobility scenario. In mobility network scenario, the average end-to-end delay is 3% higher than fixed scenario because of high mobility environment and frequent topology changes. DSDV is not suitable for larger networks. In terms of average throughput and normalized routing load, both reactive protocols (AODV, AOMDV) performs better than DSDV. This is because AODV and AOMDV both chooses the alternate path if link failure occurs. Therefore, packet loss ratio of AODV and AOMDV protocols is lower than DSDV. The number of received packets for fixed scenario is 87-90% whereas the number of received packets for mobility scenario is 70-75%. In mobility scenario, received packets ratio is always less than fixed scenario due to the repeated update of the position of the sensor nodes and frequent link failures. AOMDV and AODV have higher normalized routing load than DSDV, because of maintaining stale routes and alternate paths. In both fixed and mobility scenario, AOMDV is energy efficient routing protocol than AODV and DSDV respectively. AOMDV has much residual energy along with the hop count. To utilize the same path for route discovery process of DSDV, the node life time expires (battery power) which consumes more bandwidth and energy than reactive protocols like AOMDV and AODV. In the case of a link failure, AOMDV has the ability to make longer battery and node's lifetime because of the proper utilization in choosing a path. So our performance analysis among DSDV, AODV and AOMDV routing protocol depicts that the applications where throughput, residual energy are important and delay can be tolerated; then the AOMDV routing protocol can be the best solution. We also observed that in a high speed movement of nodes, AOMDV can be the best choice. Though AOMDV routing protocol performs better in our simulation environment considering energy consumption and throughput, still it has some limitations like more delay, more routing load in the network. The future work would be to improve AOMDV routing algorithm so that these limitations can be removed.

References Références Referencias

1. Charles E. Perkins, Elizabeth M. Royer, Samir R. Das and Mahesh K. Marina "Performance Comparison of Two On-Demand Routing Protocols for Ad Hoc Networks" , IEEE Personal Communications Magazine, Volume: 1070-9916, Issue: February 2001, pp. 16-28.
2. GinniTonk and S.S. Tyagi, "Performance of Ad-Hoc Network Routing Protocols in Different Network Sizes," Issue: July 2012.
3. D.D.Chaudhary, Pranav Pawar and Dr. L.M. Waghmare, "Comparison and Performance Evaluation of Wireless Sensor Network with different Routing Protocols, Issue: 2011.
4. Asar Ali and Zeeshan Akbar," Evaluation of AODV and DSR Routing Protocols of Wireless Sensor Networks for Monitoring Applications," unpublished, Issue: October 2009, pp. 1-49.
5. Sherikar Krishna Reddy , Rakesh K , Sunil Rathod and Vinodha mohan "A Comparative Study of Routing Protocols vs Energy Consumption in MANETs", International Journal of Innovative Research in Computer and Communication Engineering, Volume:2, Issue: 4, April 2014,pp. 3892-3898.
6. M. Swathi, B. Pravallika and N. V. Muralidhar "Implementing And Comparison of MANET Routing Protocols Using NS2", International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal), Volume: 4, Issue:2, February 2014,pp. 194-200.
7. Pawan Kumar Verma, Tarun Gupta, Nitin Rakesh and Nitin Nitin "A Mobile Ad-Hoc Routing Algorithm with Comparative Study of Earliar Proposed Algorithm", Scientific Reaserch doi:10.4236/ijcns.2010.33037, Volume: 3, Issue: February 16, 2010, pp. 289-293.
8. Jaya Jacob and V. Seethalakshmi "EFFICIENCY ENHANCEMENT OF ROUTING PROTOCOL IN MANET", International Journal of Advances in Engineering & Technology, ISSN: 2231-1963, Volume: 3, Issue: May 2014, pp. 314-323.
9. Abdusy Syarif "Performance Analysis of AODV-UI Routing Protocol With Energy Consumption Improvement Under Mobility Models in Hybrid Ad hoc Network" , International Journal on Computer Science and Engineering (IJCSE), ISSN : 0975-3397, Volume: 3 Issue: 7 July 2011, pp. 2904-2918.

10. Gowrishankar.S, Subir Kumar Sarkar and T.G.Basavaraju "Performance Analysis of AODV, AODVUU, AOMDV and RAODV over IEEE 802.15.4 in Wireless Sensor Networks", IEEE, Volume: 978-1-4244-4520, Issue: February 2009, pp.58-63.
11. Jaya Jacob and V. Seethalakshmi" EFFICIENCY ENHANCEMENT OF ROUTING PROTOCOL IN MANET" , International Journal of Advances in Engineering & Technology, ISSN: 2231-1963, Volume: 3, Issue: May 2014, pp. 314-323.
12. Vijendra Rai" Simulation of Ad-hoc Networks Using DSDV, AODV And DSR Protocols And Their Performance Comparison" , Proceedings of the 4th National Conference; INDIACom-2010,Issue: February 26, 2010, pp. 1-6.
13. Sachin Kumar Gupta and R. K." PERFORMANCE METRIC COMPARISON OF AODV AND DSDV ROUTING PROTOCOLS IN MANETs USING NS-2",publiccation: IJRRAS, Volume: 7,Issue: June 2011, pp. 339-350.
14. M.Geetha M.C.A., M.Phil., and Dr. R. Umarani M.C.A., M.Phil., PhD*" Performance Comparison and Analysis of AODV and DSDV Gateway Discovery Protocol in MANET", International Journal of Engineering Science and Technology, ISSN: 0975-5462,Volume:2, Issue: November, 2010, pp. 6521-6531.
15. "http://www.cs.jhu.edu/~cs647/aodv.pdf "Access Date: 11-02-2014.
16. S. R. Biradar, Koushik Majumder, Subir Kumar Sarkar and Puttamadappa C "Performance Evaluation and Comparison of AODV and AOMDV , (IJCSE) International Journal on Computer Science and Engineering", ISSN : 0975-3397,Volume: 2, Issue: February, 2010, pp. 373-377.
17. Mahesh K. Marina and Samir R. Das" On-demand Multipath Distance Vector Routing in Ad Hoc Networks", in Proceedings of IEEE International Conference on Network Protocols (ICNP), pp. 1-16.
18. Abdusy Syarif "Performance Analysis of AODV-UI Routing Protocol With Energy Consumption Improvement Under Mobility Models in Hybrid Ad hoc Network", International Journal on Computer Science and Engineering (IJCSE), ISSN : 0975-3397, Volume: 3 Issue: 7 July 2011, pp. 2904-2918.
19. "http://en.wikipedia.org/wiki/Destination-Sequenced_Distance_Vector_routing" , Access Date: 01-02-2014.
20. Charles E.Perkins and Pravin Bhagwat "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers" , ACM publication, Issue: August 1994, pp.234-244.
21. "http://en.wikipedia.org/wiki/Wireless_sensor_network", Access Date: 01-02-2014.

This page is intentionally left blank

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 14 Issue 6 Version 1.0 Year 2014
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Managing DDoS Attacks on Virtual Machines by Segregated Policy Management

By E. S. Phalguna Krishna, E. Sandhya & M. Ganesh Karthik
Sree Vidyanikethan Engineering College, India

Abstract- Security is considered as most crucial aspect in cloud computing. It has attracted lots of research in the recent years. On the other hand, attackers are exploring and exploiting the vulnerabilities in cloud. The heart of the Cloud computing lies in Virtualization technology. Attackers are taking the advantage of vulnerabilities in Virtual Machines and they can able to compromise virtual machines thereby launching DDOS attacks. Services such as Saas,IaaS which are meant to support end users may get affected and attackers may launch attacks either directly or by using zombies. Generally, Data Centres own security policies for dealing with security issues. Suppose incase of DDoS attacks, only the policies which deals with it ,can only been applied. However, in datacenters, all the security policies are commonly been applied on the applications irrespective of their category or security threats that it face. The existing approach consumes lots of time and wastage of resources. In this paper, we have developed an approach to segregate the applications as per the type or threats (by adapting detection mechanisms) being faced . Based on the zone in which it is lying , only the relevant security policies will only be applied. This approach is optimized where we can efficiently reduce the latency associated with applying security policies.

GJCST-E Classification : C.2.1

MANAGINGDDOSATTACKSONVIRTUALMACHINESBYSEGREGATEDPOLICYMANAGEMENT

Strictly as per the compliance and regulations of:

Managing DDoS Attacks on Virtual Machines by Segregated Policy Management

E. S. Phalguna Krishna [α], E. Sandhya [σ] & M. Ganesh Karthik [ρ]

Abstract- Security is considered as most crucial aspect in cloud computing. It has attracted lots of research in the recent years. On the other hand, attackers are exploring and exploiting the vulnerabilities in cloud. The heart of the Cloud computing lies in Virtualization technology. Attackers are taking the advantage of vulnerabilities in Virtual Machines and they can able to compromise virtual machines thereby launching DDOS attacks. Services such as Saas,IaaS which are meant to support end users may get affected and attackers may launch attacks either directly or by using zombies. Generally, Data Centres own security policies for dealing with security issues. Suppose incase of DDoS attacks, only the policies which deals with it ,can only been applied. However, in datacenters, all the security policies are commonly been applied on the applications irrespective of their category or security threats that it face. The existing approach consumes lots of time and wastage of resources. In this paper, we have developed an approach to segregate the applications as per the type or threats (by adapting detection mechanisms) being faced . Based on the zone in which it is lying , only the relevant security policies will only be applied. This approach is optimized where we can efficiently reduce the latency associated with applying security policies.

I. Introduction

Virtualization is considered as back bone for cloud computing ,With which users can access multiple instances of apps, resources etc.Virtualization technology will allow one computer to do the job of multiple computers.This environment let one computer host multiple operating systems at the same time.It transforms hardware into software.It is emulation of a fully functional virtual computer that can run its own applications and operating system and also Creates virtual elements of the CPU, RAM, and hard disk. Hardware-independence of operating system and applications. Hence, using virtualization it is possible to run operating systems and multiply applications on the same SERVER at the same time, thereby it raises the utilization and flexibility of hardware.

Some of the virtualization technologies include VMWare, Hyper V,Virtual Iron etc.,

Author α: Assistant Professor, Dept of CSE, Sree Vidyanikethan Engineering College.
Author σ: Assistant Professor, Dept of IT, Sree Vidyanikethan Engineering College.
Author ρ: Assistant Professor, Dept of CSE, Sree Vidyanikethan Engineering College.

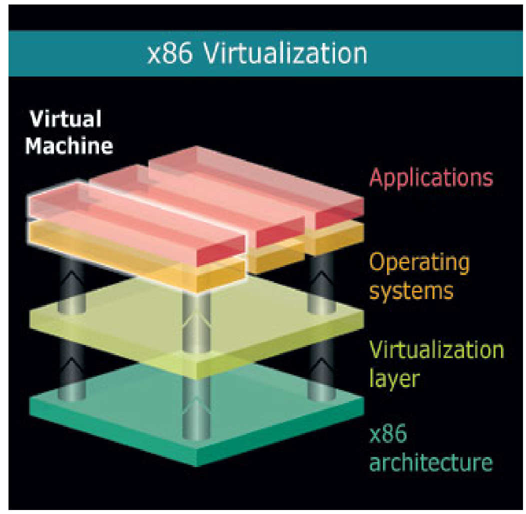


Figure 1 : Virtualization

a) Virtual Machines

These are the things that can manage OS and application as a Single unit by encapsulating them into Virtual Machines. A Virtual machine (VM) is an efficient, isolated duplicate of a real machine.
Virtual machines can be provisioned to any system.

i. *Duplicate*

The behaviour of the VM should be identical to the real machine. There is no differentiation with respect to the execution of the program at the low level.

ii. *Isolated*

Multiple Virtual Instances corresponding to different VMs execute without interfering with each other.

iii. *Efficient*

VM should operate at the speed of the under-lying hardware.

All the resources of the physical computer are shared to create the virtual machines.By virtualization, it creates an emulation that user is actually using owned resources.But at the implementation level,these resources are shared between multiple number of users at any given point in time.Further,Disks are partitioned into virtual disks and a normal user time sharing terminal serves as Virtual machine operators console.

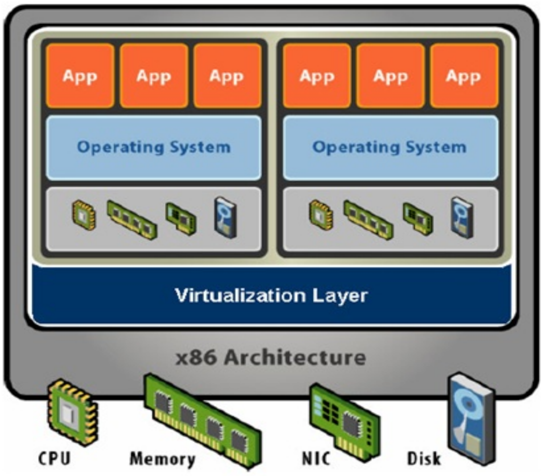


Figure 2 : Virtual Machine & Its Layers

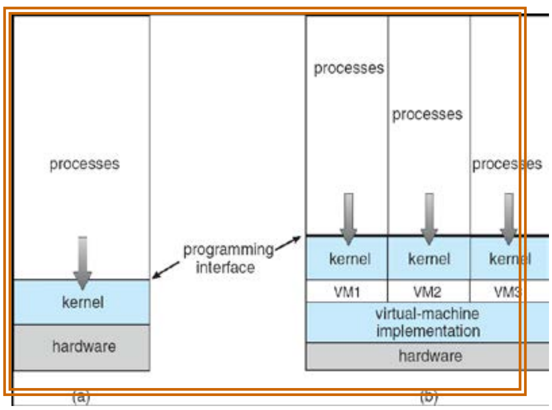


Figure 3 : VIRTUAL MACHINE

a) Types of Virtual Machines: Type 1 / Type 2

i. *Type 1*

They are also Called Hypervisors or virtual machine monitor or VMM.Hypervisors of this type is dependent of bare metal (bare machine) and always interacts with the machine. They Sit just above the HW and virtualizes the complete hardware. It runs at the physical hardware and is the real operating system. Normal unmodified operating systems, like Linux or Windows runs atop of the hypervisor. The server which is hosting Type 1 Hypervisor requires some form of persistent storage for storing the files of concern. In ESX server, the kernel uses device drives to actually get interfaced with bare metal.

- Example: Xen, VMware ESX server

b) Type 2 hypervisor

It is considered as most common type of hypervisor and depends on the underlying OS.Such hypervisors requires to be directly installed on bare metal.It runs within an OS, and rely on OS services to manage HW. A normal unmodified host operating system like Linux or Windows runs on the physical hardware.

A type 2 hypervisor like VMware Workstation runs on the host operating system.Once after installing host operating system, we can now deploy hypervisor and it doesn't modify it. Examples include QEMU, VMware Workstation etc.

II. Threats on VMs

Like any other technology, Virtual Machines are prone to different categories of threats.Some attacks against virtual machine, or VM, environments are variations of common threats such as denial of service etc. Others are still largely theoretical but likely approaching as buzz and means increase, these are the critical weaknesses.

a) VM Sprawl

VMs are easy to deploy, and many organizations view them as hardware-like tools that don't merit formal policies. This has led to VM sprawl, which is the unplanned proliferation of VMs.

Attackers can take advantage of poorly monitored resources. More deployments also mean more failure points, so sprawl can cause problems even if no malice is involved.

b) Hyperjacking

Hyperjacking takes control of the hypervisor to gain access to the VMs and their data. It is typically launched against type 2 hypervisors that run over a host OS although type 1 attacks are theoretically possible but practically difficult.

In reality, hyperjackings are rare due to the difficulty of directly accessing hypervisors. However, Hyperjacking is considered a real-world threat, and administrators should take the offensive and plan for it.

c) VM escape

A guest OS escapes from its VM encapsulation to interact directly with the hypervisor.By doing so, the attacker can gain access to all VMs and, if guest privileges are high enough, the host machine can also be targeted as well. Although few, if any instances are known, experts consider VM escape to be the most serious threat to VM security.

d) Denial of Service

Considered most common threat.These attacks exploit many hypervisor platforms and range from flooding a network with traffic to sophisticated leveraging of a host's own resources. The availability of botnets continues to make it easier for attackers to carry out campaigns against specific servers and applications with the goal of derailing the target's online services.

e) Incorrect VM Isolation

To remain secure and correctly share resources, VMs must be isolated from each other. Improper control over VM deployments can lead to isolation breaches in which VMs communicate.

Attackers can exploit this virtual drawbridge to gain access to multiple guests and possibly the host. The attacker can take the loop holes in the interfaces and can attack.

f) Unsecured VM migration

This occurs when a VM is migrated to a new host, and security policies and configuration are not updated to reflect the change. Potentially, the host and other guests could become more vulnerable. Attackers have an advantage in that administrators are likely unaware of having introduced weaknesses and will not be on alert.

g) Host and guest vulnerabilities

Host and guest interactions can magnify system vulnerabilities at several points. Their operating systems, particularly Windows, are likely to have multiple weaknesses. Like other systems, they are subject to vulnerabilities in email, Web browsing, and network protocols. However, virtual linkages and the co-hosting of different data sets make a serious attack on a virtual environment particularly damaging.

h) Dynamic environment

Tracking and updating what you have can be a challenge as people create, suspend and move virtual machines. If you don't update your golden image from which virtual machines are deployed, you can end up needing to find and patch many virtual machines.

i. *Mitigating Risk*

Inorder to overcome the existing problem with respect to the security, one can take Several steps to minimize risk.

- Characterization:The first task is to accurately characterize all deployed virtualization and any active security measures beyond built-in hypervisor controls on VMs.
- Standards: Security controls should be compared against industry standards to determine gaps. Coverage should include anti-virus, intrusion detection, and active vulnerability scanning.

Additionally, consider these action steps:

ii. *VM traffic monitoring*

Efficient monitoring of VM backbone network traffic is critical. Conventional methods will not detect VM traffic because it is controlled by internal soft switches. However, hypervisors have effective moni-toring tools that should be enabled and tested.Also , by maintaining traffic logs ,one can have vigilance over the network traffic.

iii. *Administrative control*

Procedures such as authentication, author-ization, Identity management etc must be done as a regular process by the concerned admins.Sometimes, Secure access can become compro-mised due to VM sprawl and other issues.

iv. *Customer security*

Outside of the VM, make sure protection is in place for Customer interactive interfaces such as web-sites.

v. *VM segregation*

In addition to normal isolation, strengthen VM security through functional segregation.

For example, consider creating separate security zones for desktops and servers. The goal is to minimize intersection points to the extent feasible.

III. Virualization Vulnerabilities

Virtualization has eased many aspects of IT management but has also complicated the task of cyber security. The nature of virtualization introduces a new threat matrix.

a) Single Server

- VMs run on a single server which poses serious security problems.
- Virtual monitor should be root secure meaning that no privilege within the virtualized guest environment permits interference with the host system been found in all virtualization software which can be exploited by malicious, local users to bypass certain security restrictions or gain privileges.
- For example, the vulnerability of Microsoft Virtual PC and Microsoft Virtual Server could allow a guest operating system user to run code on the host or another guest OS.
- Vulnerability in Virtual PC and Virtual Server could allow elevation of privilege.

A perfection of properties like isolation is yet to be completely achieved.

b) Ease of reconfiguration

Ability to flexibily reconfigure restart and also movement of VM's to other servers. Because of this easeness, an optimal environment to propagate vulnerabilities and unknown configuration errors has been created.

c) Dormant machines

In public-cloud environments, VM is available to any application even though it is offline.

- For example, a Web server that can access the physical server on which it resides.
- So a remote user on one VM can access another dormant VM if both reside on the same physical server.
- As Dormant machines can't perform malware scans, they are highly susceptible to malware attacks.

- Exploitation of this vulnerability is not only restricted to the VMs on a particular hypervisor but also affect other physical devices in the cloud.

For example: A Dormant machine might have been backed up or archived to another server or storage device.

d) Patch management

Generally users does the patch management in cloud computing and attackers could easily misuse this opportunity to attack VMs.

e) Cross-VM information leakage

It is the ability of a malicious instance to utilize side channels to learn information about co-resident instances.

IV. Modules

a) Packet Feeder

Packet arrives from multiple streams and they are feeded into the packet feeder module which acts as entry point for this approach. The responsibility of the packet feeder is to collect packets from various incoming streams and feed them to the module "FLOW DISCRIMINATOR".

b) Flow Differentiator

It differentiates as per the type of packets based on its properties (multimedia, text, voice, images etc).

c) Decision Maker

This Module applies "Outlier Analysis" technique to discriminate and differentiate different types of flows or vulnerablilities. For example: Normal traffic, Flash Crowd traffic, DDOS traffic etc. Our approach using Outliers requires lesser amount of computations and considered to be effective in discriminating the attacks.

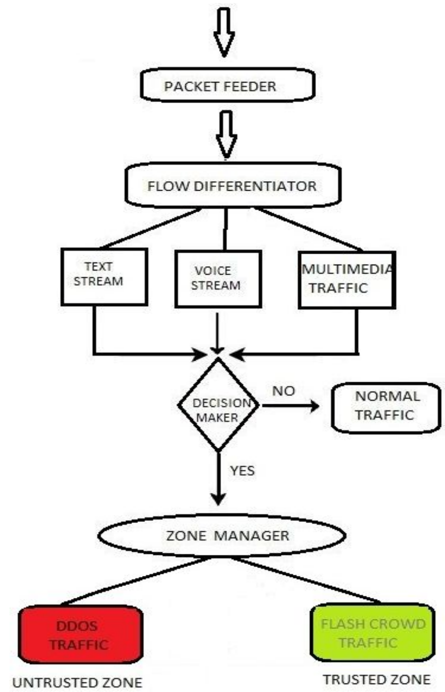
d) Zone Manager

Based upon the nature of VMs, it is prescribed to adopt necessarily relevant policies.

i. *Advantages*

- Optimizes the application of rule sets on different categories of applications.
- This approach significantly reduces the time taken by the data center admin by applying only essential set of security policies.

ii. *Block diagram*



V. Methodology

Users from various locations sends the service requests in the stream of packets to the Virtual servers/ Virtual machines, which internally utilizing virtualization technology. The packets arrived are feeded into the "*Packet Feeder*" module which acts as entry point for this approach. The responsibility of the packet feeder is to collect packets from various incoming streams and feed them to the module "*Flow Discriminator*".

The flow discriminator which takes various streams of packets as input differentiates what type of packet stream it is based on its properties like file extension, contents in the packet etc and categorizes them accordingly such as multimedia, voice, text, images etc. The discrimation is done mainly to adopt the relevant decision strategies and appropriate security policies. All categorized packet streams are given as input next module named "*Decision Maker*".

Decision Maker is the most important module which applies Outlier Analysis technique to discriminate and differentiate different types of vulnerablilities in the flow. For example : Normal traffic, Flash Crowd traffic, DDOS traffic. An advantage of using Outliers in this approach just not only requires lesser amount of computations but also considered to be effective in terms of discriminating the attacks.

Finally the identified malicious traffic from normal traffic is sent to the "*Zone Manager*" which in turn discriminates the DDOS traffic from FLASH CROWD traffic. Based upon the nature of VMs it is prescribed to adopt necessarily untypical policies to safeguard users trust.

This paper consists of three cases: Normal Traffic, DDoS, Flash Crowd. Based on the case, we apply the relevant necessary security policies. This is in converce with the previous approach, where in which the admins of the data centre used to adopt common security policies for discrete set of applications. The previous approach not only consumes time but also leads to consuming more number of processor cycles.

VI. Analogy

Normally datacenter own discrete categories of applications. Inorder to provide the security, each and every data center maintains set of security policies.It specifies what it means to be secure for a system, organization or other entity. But the scenario is like data center admins or tools apply complete set of security policies irrespective of the concept thereby consuming lots of processor cycles and raises latency.

In this paper, we have used an approach to segregate the applications as per the type or threats (by adapting detection mechanisms) being faced and we segregate them into zones. Based on the zone in which it is lying, only the relevant security will only be applied. This approach is optimized where we can efficiently reduce the latency associated with applying security policies.

Consider a scenario in which a data center hosts different set of software applications on their infrastructure. Let S be the main rule set, there exists Subsets S_i, S_j, S_k. For example A, B, C, D applications belong to a particular type of application (multimedia) or facing particular threat (DDoS). Let P, Q, R & X, Y be different categories. Then suppose, A, B, C, D, are the applications that are facing DDo S attack as a threat at this instance, Then it may be relevant to apply for example Si set of rules on those machines which are affected by it, Instead of applying S. Where Si, Sj, Sk ⊆ S. We assumed applications A,B,C,D as web apps and they are prone to DDoS attacks and Si as the subset of rule set that consists of the security policies and mitigation strategies to be applied for DDo S. Similary $S_j \in$ (P,Q,R,S) and $S_k \in$ (X,Y).

VII. Applcations

- The approach can be adopted to the data centres consisting diversified applications.
- The approach is applicable to the data centers which considers security as a service.

VIII. Security Policies

A security policy is a comprehensive document that defines a companies' methods for prevention, detection, reaction, classification, accountability of data security practices and enforcement methods.It generally follows industry best practices as defined by ISO 17799, 27001-02, PCI, ITIL, SAS-70, HIPPA , SOX or a mix of them. It is the key document in effective security practices. Following are some of the policies of data centers:

- Develop a checklist for standard operating procedures to follow in the event of an attack, including internal firewall teams, intrusion detection teams and network teams. Identify who should be contacted during an attack, what processes should be followed by each and what information is needed.
- ISPs and hosting providers might provide mitigation services. Be aware of the service-level agreement provisions.
- Identify and prioritize critical services that should be maintained during an attack so as to keep resources turned off or blocked as needed to limit the effects of the attack.
- Ensure that critical systems have sufficient capacity to withstand an attack.
- Determine whether the denial of service attack is attempting to consume:
  a. Network bandwidth resources, or
  b. Server resources.
- Separate or compartmentalize critical services, including public and private services; intranet, extranet, and Internet services and create single-purpose servers for services such as HTTP, FTP, and DNS.
- Keep network diagrams, IT infrastructure details and asset inventories current and available to help understand the environment.
- Have a baseline of the daily volume, type, and performance of network traffic to help identify the type, target and vector of attack.
- Identify existing bottlenecks and remediation actions needed.
- Harden the configuration settings of the network, operating systems and applications by disabling unnecessary services and applications.
- Implement a bogon (bogus IP address) block list at the network boundary to drop bogus IP traffic.
- Employ service screening on edge routers: very useful to decrease the load on stateful security devices such as firewalls.

a) *Mitigation Strategies of DDOS attacks in data centres*

Data centres cannot rely on their ISP alone to provide a complete DDoS solution that includes application layer protection.

To protect against application-layer DoS, several mitigation strategies can be considered:

i. Traffic subjected to rate limits, prioritization, and load balancing.
ii. Fast-expiring session aging

Global Journal of Computer Science and Technology (E) Volume XIV Issue VI Version I Year 2014

iii. Two-factor authentication to validate user roles, especially at admin levels.
iv. Advanced next generation firewalls (NGFWs), such as Fortinet's FortiGate products, offer DDoS and IPS services.
v. Dedicated DDoS Attack Mitigation Appliances: These are dedicated hardware-based devices that are deployed in a data centre used to detect and stop basic (layer 3 and 4) and advanced (layer 7) DDoS attacks.
vi. Deployed at the primary entry point for all web-based traffic, they can both block bulk volumetric attacks and monitor all traffic coming in and leaving the network to detect suspicious patterns of layer 7 threats.

b) Top three mitigation solutions

To make services more robust against a DDoS attack, the following combination of strategies are proposed, they are:

i. *Increase the barrier to entry by using a Pricing-Based Scheme*

Price of entry varies with the load level. This will throttle the machines used in the attack, thereby forcing the attacker to employ (or subvert) a larger number of machines.

ii. *Differentiated model*

Allocating a priority mechanism to desirable clients is key which Provides prioritized access to classes of users though a DDoS attack will raise the price so high that lower priority classes get locked out, higher priority clients can still access the service.

iii. *Dynamic and Differential pricing mechanism*

This will be applied to penalize clients who are responsible for a load on the server and it typically requires flow monitoring and isolation capabilities.

c) Flash Crowd Mitigation Strategies

1. Adaptive Admission Control Based on Application-Level Observations.
2. Flash Crowd Detection within the realms of an Internet Service Provider (ISP).
3. Dynamic CDN against Flash Crowds.
4. Managing Flash Crowds on the Internet
5. Handling Flash Crowds from your Garage
6. KadCache: Employing Kad to Mitigate Flash Crowds and Application Layer DDoS Attacks Against Web Servers.

IX. Conclusion

The flow differentiator is responsible to identify and discriminate attack ,normal flows.Further, we apply zone managers,which will move VM's & its applications to respective zones .Only the relevant security policies will only be applied on the VM's which are running those applications that are affected with security vulnerabilities. Our approach is considered to be effective in optimizing the security policies. Further, this approach is considered to be effective and consumes less resources and time.

References Références Referencias

1. Shui Yu, Weijia Jia, Song Guo, Yong Xiang, and Feilong Tang "Discriminating DDoS Attacks from Flash Crowds Using Flow Correlation Coefficient" IEEE Transactions On Parallel And Distributed Systems, Vol. 23, No. 6, June 2012.
2. Ke Li, Wanlei Zhou, Ping Li, Jing Hai and Jianwen Liu "Distinguishing DDoS Attacks from Flash Crowds Using Probability Metrics" Third International Conference on Network and System Security pno: 9-17 .2009.
3. Zhang Fu, Marina Papatriantafilou, and Philippas Tsigas "Mitigating Distributed Denial of Service Attacks in Multiparty Applications in the Presence of Clock Drifts" Ieee Transactions On Dependable And Secure Computing, Vol.9, No.3, May/June 2012.
4. Arbor Application Brief: "The Growing Threat of Application-Layer DDoS Attacks".2011.
5. Employing Kad to Mitigate Flash Crowds and Application Layer DDoS Attacks Against Web Servers.
6. Ari, B. Hong, E. L. Miller, S. A. Brandt,and D. D. E.Long, "Modeling, Analysis and Simulation of Flash Crowds on the Internet,"Storage Systems Research Center Jack Baskin School of Engineering University of California, Santa Cruz Santa Cruz, CA, ech. Rep. UCSC-CRL-03-15, Feb. 28, 2004 http://ssrc.cse.ucsc.edu/, 95064.

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 14 Issue 6 Version 1.0 Year 2014
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Effect of Channel Equalization Schemes in Performance Evaluation of a Secured Convolutional Encoded DWT based MIMO MCCDMA System

By Rifat Ara Shams, M. Hasnat Kabir & Mohammed Mustaqim Rahman
University of Rajshahi, Bangladesh

Abstract- In this research work, performance of different channel equalization techniques and various M-ary modulation schemes (MPSK, MQAM and DPSK) for DWT based MIMO Multi-Carrier Code Division Multiple Access (MC-CDMA) wireless communication system has been analyzed through simulation. We propose this system using convolutional coding scheme over AWGN and Rayleigh fading channel with implementation of Walsh Hadamard code as orthogonal spreading code. In this paper, we derive a generalized analytical framework to evaluate the Bit Error rate (BER) with respect to Signal-to Noise Ratio (SNR) and also use Electronic Codebook (ECB) mode as cryptographic algorithm to encrypt the actual data for security issues.

Keywords: DWT, MIMO, MC-CDMA, MMSE, ZF, SVD,Q-less QR, ECB.

GJCST-E Classification : C.2.1

EFFECT OFCHANNEL EQUALIZATION SCHEMESINPERFORMANCE EVALUATION OFASECUREDCONVOLUTIONAL ENCODED DWTBASED MIMO MCCDMASYSTEM

Strictly as per the compliance and regulations of:

Effect of Channel Equalization Schemes in Performance Evaluation of a Secured Convolutional Encoded DWT based MIMO MC-CDMA System

Rifat Ara Shams [α], M. Hasnat Kabir [σ] & Mohammed Mustaqim Rahman [ρ]

Abstract- In this research work, performance of different channel equalization techniques and various M-ary modulation schemes (MPSK, MQAM and DPSK) for DWT based MIMO Multi-Carrier Code Division Multiple Access (MC-CDMA) wireless communication system has been analyzed through simulation. We propose this system using convolutional coding scheme over AWGN and Rayleigh fading channel with implementation of Walsh Hadamard code as orthogonal spreading code. In this paper, we derive a generalized analytical framework to evaluate the Bit Error rate (BER) with respect to Signal-to Noise Ratio (SNR) and also use Electronic Codebook (ECB) mode as cryptographic algorithm to encrypt the actual data for security issues.

Keywords: DWT, MIMO, MC-CDMA, MMSE, ZF, SVD, Q-less QR, ECB.

I. Introduction

In the era of technologies the demand for wireless systems are rapidly increasing. To gain user satisfaction, multiple access technologies, high data transfer rates and flexible bandwidth allocation must be ensured by using the significant inventions of science and tech worlds [1]. Nevertheless high quality communication with low implementation cost is the centre of attraction of the users [2]. To fulfill user's requirements and to support a wide range of multimedia services, the 3rd generation or beyond wireless communication systems prefer Multi Carrier- Code Division Multiple Access (MC-CDMA) because of its high performance over multipath fading environment and increased capacity for a specified bandwidth [2,3]. MC-CDMA combines Code Division Multiple Access (CDMA) and Orthogonal Frequency Division Multiplexing (OFDM) to support multiple users at the same time as well as to ensure perfect utilization of frequency domain [1,4]. Moreover to curtail the dreadful presence of Inter Symbol Interferences (ISI) and to improve the Signal-to-Noise Ratio (SNR) performance, Discrete Wavelet Transform (DWT) based MC-CDMA is preferred over Discrete Fourier Transform (DFT) based MC-CDMA because of its ability to minimize the analytical complexity and to avoid the influence of delayed waves [2,5].

In our previous work presented in [2], the performance of Wavelet based MC-CDMA systems using Forward Error Correction (FEC) with interleaving in different modulation schemes on fading environment has been investigated. In this paper we propose this very system with Multiple-Input Multiple-Output (MIMO) where different channel equalization and different digital modulation techniques are used over AWGN and Rayleigh fading channel with implementation of convolutional coding scheme as error control coding and a cryptographic algorithm, Electronic Code Book (ECB) mode for secured transmission of data.

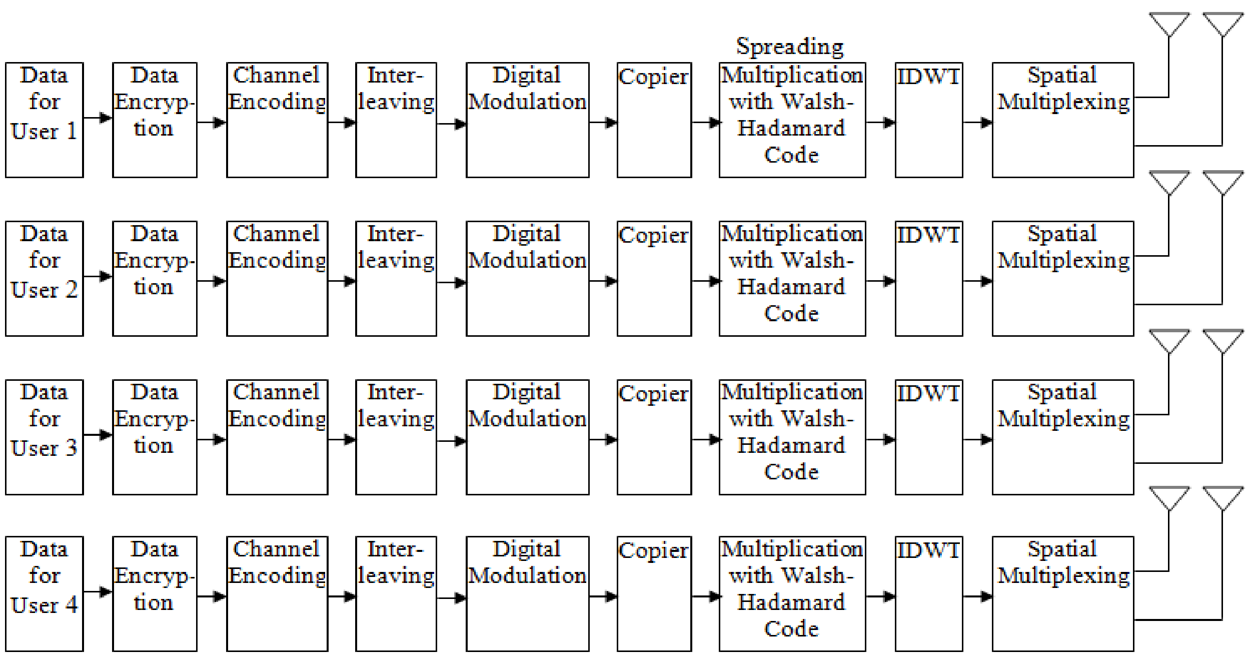
We preferred MIMO over other technologies because of its ability to increase the data rate that is to provide multiple forms of the same signal at the receiver without consuming much time [6]. Besides, the use of channel equalization schemes has enriched our proposal because it protects the data from Inter-Symbol-Interference (ISI) by adding redundant bits and exploiting the original transmitted data structure [7]. In our proposed DWT based MIMO MC-CDMA system, the Bit Error Rate (BER) performance of Minimum Mean Square Error (MMSE), Zero Forcing (ZF), Singular Value Decomposition (SVD) and Q-less QR decomposition based channel equalization techniques are compared. It may sound incredible, but with the colossal advancement of science and technology, network security faces a lot of threats. To overcome this problem, we have encrypted the original text message while transmitting using ECB algorithm where each plaintext is divided into several blocks that are encrypted using the same key and at the receiver end, the corresponding ciphertext is decrypted also using that key to retrieve the original message from its indecipherable form [8].

Author α: Department of Computer Science and Engineering Stamford University Bangladesh, Dhaka-1217, Bangladesh.
e-mail: swarna601@gmail.com
Author σ: Department of Information and Communication Engineering University of Rajshahi, Rajshahi-6205, Bangladesh.
e-mail: hasnatkabir@yahoo.com
Author ρ: Department of Computer Science and Engineering Stamford University Bangladesh, Dhaka-1217, Bangladesh.
e-mail: mustaqim.cse@gmail.com

Our attempt is to propose an efficient MC-CDMA scheme that provides the most copacetic result taking the benefits of ubiquitous presence of different channel equalization and digital modulation schemes.

II. System Model

A simulated multi-user 2 × 2 spatially multiplexed and wavelet based MC-CDMA wireless communication system that utilizes spatial diversity coding scheme has been proposed as depicted in Figure 1. In such a communication system, the text message for different users is processed for encryption with ECB cryptographic algorithm so that unauthorized access of data can be prevented. The encrypted data are converted into binary bits and then channel encoded using ½-rated convolutionally encoding schemes and interleaved for minimization of burst errors. The interleaved and channel encoded bits are digitally modulated using BPSK, DPSK, QAM and QPSK. After that, the number of digitally modulated symbols is increased eight times in copying section (as the processing gain of the Walsh Hadamard codes is eight) and subsequently multiplied with Walsh Hadamard codes. The Walsh–Hadamard and channel encoded interleaved digitally modulated symbols are passed through inverse wavelet transformation and eventually fed into Space time block encoder for processing with implemented philosophy of Alamouti's G2 Space Time Block Coding scheme. The space time block encoded signals are then transmitted from each of the two transmitting antennas. In receiving section, the transmitted signals are detected using different channel equalization schemes (MMSE, ZF, SVD and Q-less QR decomposition). The detected two signals are passed through Space time block decoder and subsequently sent to forward wavelet transformation section. Its output is multiplied with assigned Walsh–Hadamard codes for despreading purposes. The despreaded digitally modulated symbols are then decopied, digitally demodulated, deinterleaved and channel decoded scrupulously. Finally the channel decoded binary bit stream is processed for performing decryption operation using the same key as encryption for retrieving the original transmitted text properly.



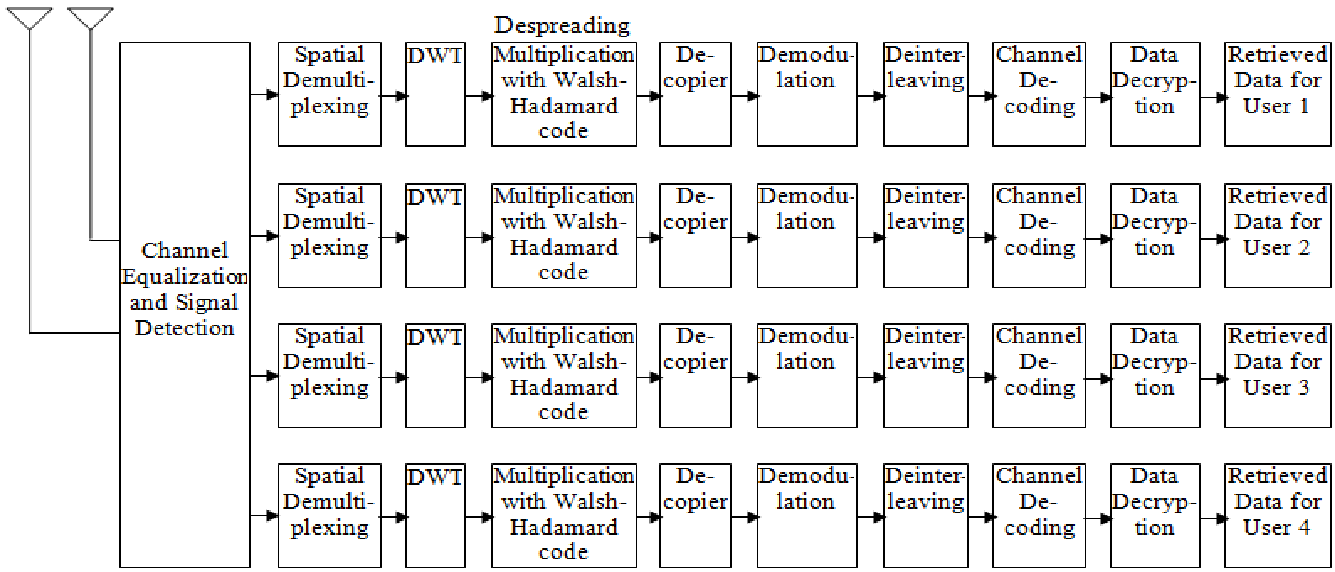


Figure 1 : Block diagram of a wavelet based MIMO MC-CDMA wireless communication system

III. Simulation Parameters

Here, we have used MATLAB 7.5 for simulation of DWT based MIMO MC-CDMA system where different graphical waveforms for different channel equalization schemes and different digital modulation techniques as well as some data for Bit Error Rate (BER) as a function of Signal-to-Noise-Ratio (SNR) per bit have been found. The proposed model for the wavelet based MIMO MC-CDMA transmitter and receiver in Figure 1 is simulated with considering the following parameters shown below in the Table 1.

Table 1 : Summary of simulation model parameters

Parameters	Types
User	4
Input Data	Text
Signal processing scheme	Wavelet
Processing gain	8
Modulation	BPSK,DBPSK,QPSK and 4QAM
SNR	0-10 dB
Spreading code	Walsh-Hadamard Code
Channel coding scheme	Convolutional
Signal detector (Equalizer)	MMSE, ZF, SVD and Q-less QR Decomposition
Channel	AWGN and Rayleigh fading
Cryptographic algorithm	Electronic Codebook (ECB)
Antenna Configuration	2 x 2

IV. Simulation Results and Discussion

In our dissertation, the performance of different channel equalization (MMSE, ZF, SVD AND Q-less QR decomposition) and digital modulation techniques (BPSK, QPSK, 4QAM and DBPSK) is compared in the perspective of bit error rate of MIMO MC-CDMA system based on DWT as a result of simulation, where convolutional coding technique and a cryptographic algorithm (Electronic Codebook Mode) are implemented for security purposes over AWGN and Rayleigh fading channel for wide range of SNR from 0 dB to 10 dB. From all the figures, it is seen that the bit error rate is decreasing with the increase of SNR as expected [2].

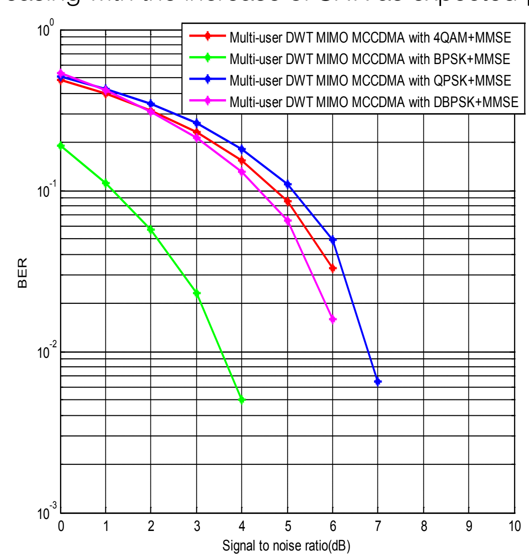


Figure 2 : Effect of different digital modulations under MMSE channel equalization technique in DWT based MIMO MC-CDMA system with implementation of convolutional coding scheme

In Figure 2, the performance of different digital modulation schemes (BPSK, QPSK, 4QAM and DBPSK) is compared in MIMO MC-CDMA system using MMSE channel equalization scheme. From the figure, it is noticeable that the system outperforms in BPSK digital modulation as compared to others (QPSK, 4QAM and DBPSK). For example, the BER values are 0.0229 and 0.2615 in case of BPSK and QPSK digital modulations respectively in a typically assumed SNR value of 3 dB as shown in Table 2, that is, the system performance achieves a gain of 10.58 dB. It is also observable from Figure 4 that at 10% BER value, the system performance with BPSK is superior to QPSK by 4 dB SNR value.

Table 2 : BER performance of the DWT based MIMO MC-CDMA system with implementation of MMSE channel equalization, convolutional coding and various digital modulation schemes

SNR (dB)	BER with MMSE Channel Equalization			
	4QAM	BPSK	QPSK	DBPSK
0	0.4893	0.1899	0.5098	0.5350
1	0.4024	0.1112	0.4301	0.4169
2	0.3151	0.0569	0.3459	0.3091
3	0.2310	0.0229	0.2615	0.2133
4	0.1535	0.0050	0.1810	0.1313
5	0.0863	0	0.1088	0.0649
6	0.0327	0	0.0492	0.0159
7	0	0	0.0065	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0

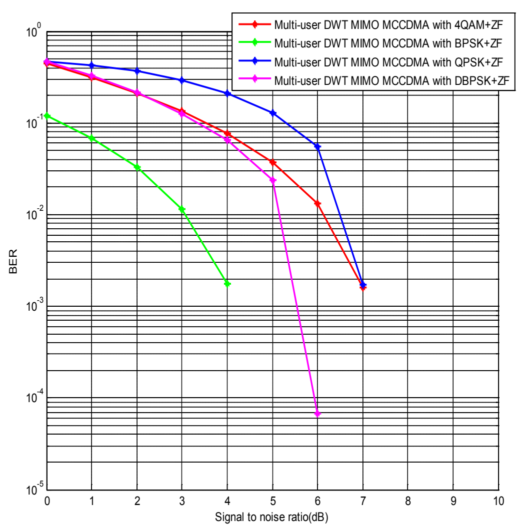


Figure 3 : Effect of different digital modulations under ZF channel equalization technique in DWT based MIMO MC-CDMA system with implementation of convolutional coding scheme

In Figure 3, it is remarkable that at higher SNR value area (5 dB – 7 dB), the estimated BER values at different digital modulations (BPSK, QPSK, 4QAM, DBPSK) ranges from minimum 0.0000 to maximum 0.0017 with implementation of Zero Forcing (ZF) channel equalization scheme (Table 3). Here, BPSK also gives the best performance among others as shown in the figure. The system shows almost identical performance in low SNR value area with 4QAM and DBPSK digital modulations. After SNR value of 5 dB, the BER value falls dramatically for DBPSK digital modulation whereas the BER of others decreases almost linearly with the increase of SNR.

Table 3 : BER performance of the DWT based MIMO MC-CDMA system with implementation of ZF channel equalization, convolutional coding and various digital modulation schemes.

SNR (dB)	BER with ZF Channel Equalization			
	4QAM	BPSK	QPSK	DBPSK
0	0.4412	0.1208	0.4668	0.4695
1	0.3131	0.0680	0.4296	0.3261
2	0.2115	0.0326	0.3686	0.2130
3	0.1336	0.0116	0.2924	0.1270
4	0.0765	0.0017	0.2092	0.0650
5	0.0373	0	0.1275	0.0237
6	0.0133	0	0.0555	0.0001
7	0.0016	0	0.0017	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0

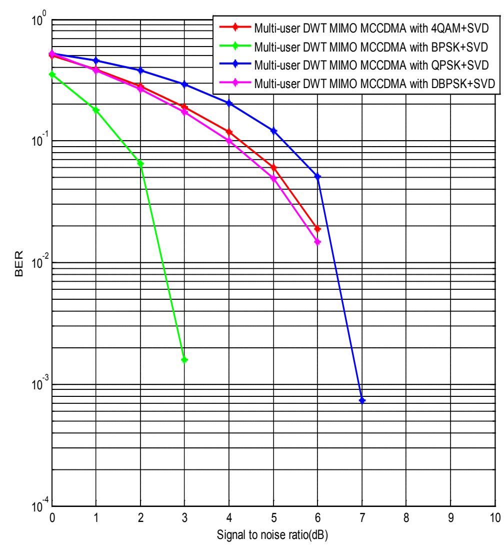


Figure 4 : Effect of different digital modulations under SVD channel equalization technique in DWT based MIMO MC-CDMA system with implementation of convolutional coding scheme

From critical examination on Figure 4, it can be unanimously mentioned that the system under investigation shows the best performance in BPSK digital modulation as compared to others (QPSK, 4QAM and DBPSK) with implementation of Singular Value Decomposition (SVD) channel equalization technique. This is because the BER value for BPSK is the lowest than others. For example, if we consider only BPSK and QPSK digital modulations, it can be shown from Table 4 that, for a typically assumed SNR value of 3 dB, the BER values are 0.0016 and 0.2920 for BPSK and QPSK digital modulations respectively viz., the system performance achieves a gain of 22.61 dB. It is also shown from the figure that, the BER values of BPSK and QPSK decrease rapidly within 2dB-3dB and 6dB - 7dB respectively whereas the decreasing rate is linear for both before these SNR values. The system shows almost identical performance in low SNR value area with 4QAM and DBPSK digital modulations.

Table 4 : BER performance of the DWT based MIMO MC-CDMA system with implementation of SVD channel equalization, convolutional coding and various digital modulation schemes

SNR (dB)	BER with SVD Channel Equalization			
	4QAM	BPSK	QPSK	DBPSK
0	0.5083	0.3544	0.5237	0.5221
1	0.3872	0.1787	0.4586	0.3805
2	0.2816	0.0650	0.3792	0.2644
3	0.1919	0.0016	0.2920	0.1718
4	0.1181	0	0.2038	0.1007
5	0.0604	0	0.1214	0.0490
6	0.0190	0	0.0515	0.0150
7	0	0	0.0007	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0

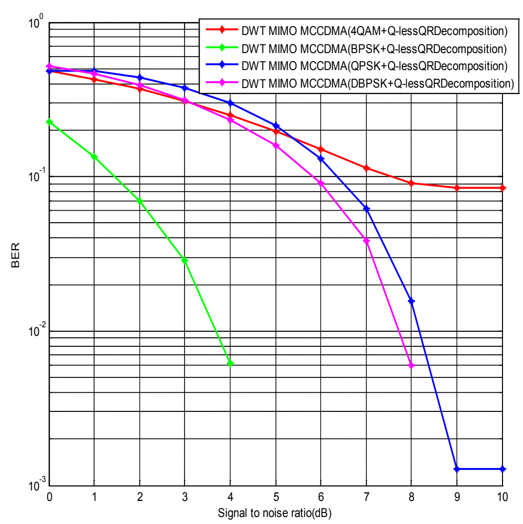


Figure 5 : Effect of different digital modulations under Q-less QR decomposition based channel equalization technique in DWT based MIMO MC-CDMA system with implementation of convolutional coding scheme

From Figure 5, it can easily be noticed that, the system using Q-less QR decomposition based channel equalization scheme provides the best performance with BPSK as before whereas it gives the worst performance with 4QAM in the perspective of the decreasing rate of BER. It is remarkable that, at higher SNR value area (4 dB –10 dB), the estimated BER values at different digital modulations ranges from minimum 0.0062 to maximum 0.0850 as shown in Table 5. As an example, it can be shown that, at 10% BER value, the system performance with BPSK is superior to 4QAM by 6.3 dB SNR value.

Table 5 : BER performance of the DWT based MIMO MC-CDMA system with implementation of Q-less QR decomposition based channel equalization, convolutional coding and various digital modulation schemes

SNR (dB)	BER with Q-Less QR decomposition based Channel Equalization			
	4QAM	BPSK	QPSK	DBPSK
0	0.4841	0.2265	0.4866	0.5214
1	0.4297	0.1340	0.4814	0.4634
2	0.3708	0.0696	0.4420	0.3926
3	0.3105	0.0286	0.3778	0.3145
4	0.2517	0.0062	0.2982	0.2346
5	0.1974	0	0.2128	0.1584
6	0.1506	0	0.1309	0.0912
7	0.1142	0	0.0621	0.0386
8	0.0914	0	0.0157	0.0060
9	0.0850	0	0.0013	0
10	0.0850	0	0.0013	0

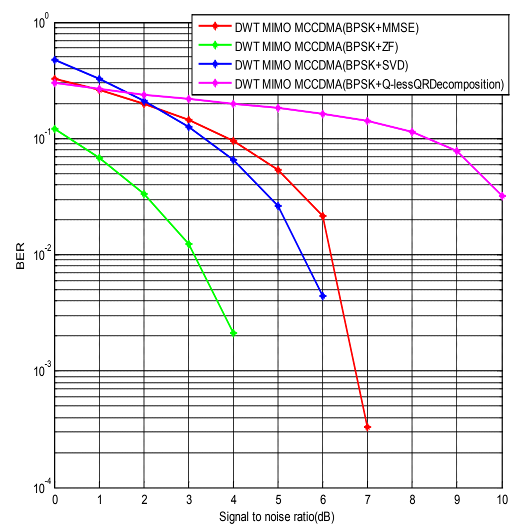


Figure 6 : Effect of different channel equalization techniques in DWT based MIMO MC-CDMA system with implementation of convolutional coding and BPSK digital modulation schemes

In Figure 6, the performance of different channel equalization schemes (MMSE, ZF, SVD, Q-less QR decomposition) in DWT based MIMO MC-CDMA system has been investigated with BPSK digital modulation incorporating with convolutional coding technique. A remarkable system performance has been observed from this figure with implementation of ZF channel equalization scheme. The system shows the worst performance in Q-less QR decomposition based channel equalization scheme as compared to others. For example, considering SNR value of 4 dB, the BER values are 0.0021 and 0.2009 in case of ZF and Q-less QR decomposition based channel equalization schemes respectively (Table 6), that is, the system performance achieves a gain of 19.81 dB. From the figure, an interesting property can be noticed that, a dramatical decreasing of BER has been occurred for MMSE channel equalization scheme after 6 dB SNR value.

Table 6 : BER performance of the DWT based MIMO MC-CDMA system with implementation of convolutional coding, BPSK digital modulation and various channel equalization schemes

SNR (dB)	BER with BPSK Digital Modulation			
	MMSE	ZF	SVD	Q-less QR Decomposition
0	0.3253	0.1202	0.4714	0.2998
1	0.2612	0.0685	0.3252	0.2664
2	0.2005	0.0335	0.2114	0.2402
3	0.1447	0.0124	0.1263	0.2191
4	0.0952	0.0021	0.0659	0.2009
5	0.0537	0	0.0266	0.1835
6	0.0215	0	0.0045	0.1648
7	0.0003	0	0	0.1424
8	0	0	0	0.1143
9	0	0	0	0.0784
10	0	0	0	0.0324

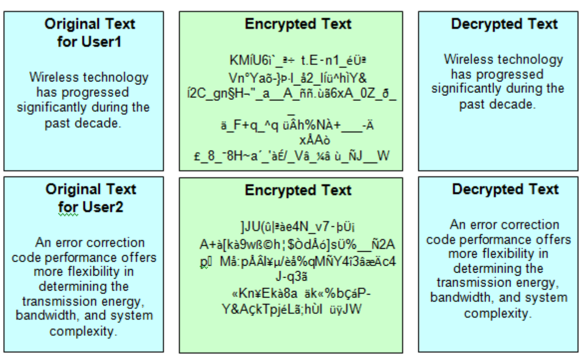


Figure 7 : Transmitted original messages, encrypted and decrypted messages using Electronic Codebook (ECB) mode of operation

In Figure 7, the transmitted, encrypted and decrypted messages for different users at SNR value of 10 dB have been presented. It is observed from the figure that, in all cases the encrypted text message is totally unintelligible, that is, it does not have any similarity to that of the original text message whereas this message can be retrieved with the decrypted one. Hence, it can be concluded that, this system ensures secured communication because it is possible to protect the transmitted data from eavesdropping of third party using this cryptographic algorithm.

V. Conclusion

In this thesis work, the performance of a 2 × 2 multi antenna supported 4G compatible DWT based MC-CDMA wireless communication system adopting convolutional coding and various channel equalization schemes with different digital modulations has been studied. In the context of system performance, it can be concluded that with BPSK digital modulation under implementation of ZF channel equalization scheme, the system provides the most satisfactory result. Furthermore, by using ECB cryptographic algorithm, confidentiality of data, which is one of the burning issues nowadays, can be ensured. Hence, by adopting this system, secured transmission of data with lower BER performance is possible.

References Références Referencias

1. Barbara M. Masini, Flavio Zabini and Andrea Conti. (2010). *MC-CDMA Systems: a General Framework for Performance Evaluation with Linear Equalization.* Chapter–6, pp-127, Communications and Networking.
2. Rifat Ara Shams, M. Hasnat Kabir, Sheikh Enayet Ullah. (2012). Effect of Interleaved FEC Code on Wavelet Based MC-CDMA System with Alamouti STBC in Different Modulation Schemes. *International Journal of Computer Science, Engineering and Information Technology (IJCSEIT),* Vol.2, No.1, 23-33.
3. National University of Singapore, Faculty of Engineering. Multi-Carrier Code Division Multiple Access (MC-CDMA). Retrieved from the Website of National University of Singapore: http://www.eng.nus.edu.sg/EResnews/0002/sf/sf_pg_6/sf_ee_3.htm
4. Wikipedia. (2013, September 27). Multi-carrier code division multiple access. Retrieved from Wikipedia, The free encyclopedia: http://en.wikipedia.org/wiki/Multi-carrier_code_division_multiple_access
5. Saleh Masum, M. Hasnat Kabir, Md. Matiqul Islam, Rifat Ara Shams and Sheikh Enayet Ullah. (2012). Impact of Different Spreading Codes Using FEC on DWT Based MC-CDMA System. International Journal of Mobile Network Communications & Telematics (IJMNCT), Vol.2, No.3, 1-10.
6. Radio-Electronics.com. What is MIMO? Multiple Input Multiple Output Tutorial. Resources and analysis for electronics engineers: http://www.radio-electronics.com/info/antennas/mimo/multiple-input-multiple-output-technology-tutorial.php
7. [Michael Tüchler, Andrew C. Singer, Ralf Koetter. (2002). Minimum Mean Squared Error Equalization Using A Priori Information. IEEE Transactions on Signal Processing, Vol. 50, No. 3, 673-683.
8. Willium Stallings. (2010). Cryptography and Network Security. pp- 182.

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 14 Issue 6 Version 1.0 Year 2014
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

LWE Encryption using LZW Compression

By M. N. M. Prasad, Mohammed Ali Hussain & C.V. Sastry

KLEF University, India

Abstract- ENCRYPTION of data has become essential, for sending confidential information from one system to another system, especially in banking sector. NTRU labs have done pioneering work using a ring of truncated polynomials which was based on the impossibility (with proper choice of parameters) of finding the polynomial with knowledge of its inverse in modular arithmetic. Recently, Learning With Errors (LWE) has been studied extensively and its hardness can be linked to the near impossibility of finding the Shortest Vector on integer lattices. In this paper we have shown that a preprocessing of input before applying the LWE algorithm greatly reduces the time of encryption and decryption.

Keywords: number theory research unit (NTRU), LWE, SVP, LZW, ring of truncated polynomials, modular arithmetic.

GJCST-E Classification : *I.4.2*

LWEENCRYPTIONUSING LZW COMPRESSION

Strictly as per the compliance and regulations of:

LWE Encryption using LZW Compression

M.N.M. Prasad [α], Mohammed Ali Hussain [σ] & C.V. Sastry [ρ]

Abstract- ENCRYPTION of data has become essential, for sending confidential information from one system to another system, especially in banking sector. NTRU labs have done pioneering work using a ring of truncated polynomials which was based on the impossibility (with proper choice of parameters) of finding the polynomial with knowledge of its inverse in modular arithmetic. Recently, Learning With Errors (LWE) has been studied extensively and its hardness can be linked to the near impossibility of finding the Shortest Vector on integer lattices. In this paper we have shown that a pre-processing of input before applying the LWE algorithm greatly reduces the time of encryption and decryption.

Keywords: number theory research unit (NTRU), LWE, SVP, LZW, ring of truncated polynomials, modular arithmetic.

I. Introduction

Secure transmission of data has become the key for successful completion of all transactions. NTRU Labs have created a bench-mark in secure transmission of data using a ring of truncated polynomials [1, 2, 3, 4]. Many attempts have been made to break the crypto-systems based in NTRU technique; but no successful attempt has ever been reported. However polynomial inversions are difficult to perform in modulo-arithmetic. Moreover, polynomials are to be repeatedly chosen until they could be properly inverted.

In the last three to four years, Learning With Errors (LWE) has emerged as a versatile alternative to the NTRU cryptosystems. All cryptographic constructions based on LWE [5, 6, 7] are as secure as the assumption that SVP (Smallest Vector Problem)[8,9] is hard on integer lattices.

The LWE problem can be stated as follows:

Recover s, given $A.s \cong b$ where $s \in Z_q^n$, $b \in Z_q^n$ and A is m × n matrix with m > n and Z_q^n is set of integer vectors of size n and modulo q. In other words, we are given a set of m equations in n unknowns and the right hand side slightly perturbed with the error vector chosen from normal distribution χ with low standard deviation. More precisely we say that an solves LWE[10] if we can recover s, given that the errors are distributed according to the error distribution χ and the elements of A are chosen uniformly at random from Z_q^n [10].

The number of equations or the number of rows in the matrix is irrelevant since additional equations can be formed that are as good as new, by adding the given equations.

One way to obtain a solution to the LWE problem is to repeatedly form new equations until we get the first row of the matrix A as (1, 0, 0, 0, ..., 0) which gives a solution to the first component of s. We can repetitively apply the same procedure for the other components of s. However the probability of obtaining such a solution is almost nil, of the order of q^{-n}, and the set of equations needed are $2^{O(n \log n)}$ and with a similar running time.

The algorithm can be stated as follows:

Private Key: s, chosen uniformly at random from Z_q^n.

Public Key: m samples of (A_i, b_i).

Encryption: for each bit of the message, we chose at random a set T from the 2^m subsets of the m equations. The encryption is $(\sum_{i\in T} A_i, \sum_{i\in T} b_i)$, if the bit is zero and the encryption is $(\sum_{i\in T} A_i, \left\lfloor \frac{q}{2} \right\rfloor + \sum_{i\in T} b_i)$ if the bit is 1.

Decryption: The decryption of the pair (a, b) is 0 if b – <a, s> is closer to 0 than to $\left\lfloor \frac{q}{2} \right\rfloor$, 1 otherwise.

However, transmitting a text with bitwise encryption will be cumber-some and time-taking. We use a slightly modified version of the algorithm to encrypt 'l' bits simultaneously. We choose A, S uniformly at random from $Z_q^{m\times n}$ and $Z_q^{n\times l}$ respectively and S is the private key. We generate the error matrix $E \in Z_q^{m\times l}$ by choosing each entry according to normal distribution$\boldsymbol{\chi}\alpha$, where α is a measure of standard deviation which is usually chosen as $\sqrt{\alpha q}$ and α is small. The public key is (A, B) where B= A.S + E.

Farther simplification is made by choosing the elements of A in the form of a circulant matrix. In other words we have chosen A as [11]

$$\begin{bmatrix} a_1 & a_2 & a_3 & a_4 & . & . & . & . & a_n \\ a_2 & a_3 & a_4 & a_5 & & . & . & . & -a_1 \\ a_3 & a_4 & a_5 & a_6 & . & . & . & -a_1 & -a_2 \\ . & & & & . & . & . & . & \\ . & & & & . & . & . & . & \end{bmatrix}$$

Let v be a vector belonging to message space Z_t^l. Choose a vector $a \in \{\mathbf{-1,0,1}\}^{\boldsymbol{m}}$ uniformly at random. The cipher text u corresponding to the

Author α: Research Scholar, Department of Computer Science and Engineering, KLEF University, Vaddeswaram, Guntur, Andhra Pradesh, India. e-mail: prasadmushini@gmail.com.
Author σ: Professor, Department of Electronics and Computer Engineering, KLEF University, Vaddeswaram, Guntur, Andhra Pradesh, India. e-mail: dralihussain@kluniversity.in.
Author ρ: Professor Department of Computer Science and Engineering, Regency Institute of Technology, Yanam, U.T. of Podicherry, India. e-mail: cvsastry40@yahoo.co.in.

message v is $(u = A^T a, C = B^T a + f(v))$ where f is an invertible mapping from the message space Z_t^l to Z_q^l and in this paper we have chosen the mapping as a multiplication of each co-ordinate by q/t and rounding to the nearest integer.

The original message can be recovered from the cipher text (u, C) using the private key S as $f^{-1}(C - S^T u)$ which can be seen as follows:

$$\begin{aligned} f^{-1}(C - S^T u) &= f^{-1}(B^T a + f(v) - S^T A^T a) \\ &= f^{-1}((AS+E)^T r + f(v) - S^T A^T a) \\ &= f^{-1}(E^T a + f(v)) \\ &= f^{-1}(E^T a) + v \end{aligned}$$

If a decryption error is to occur, say in the first letter, the first co-ordinate of $E^T a$ must be greater than $q/(2t)$ in absolute value the probability of which is shown to be negligible [11].

However, some pre-processing of data greatly helps to reduce the time for encryption and decryption as well as time for transmission. We choose to compress the data before encryption using LZW (Lemple-Ziv-Welch)[12,13,14] technique and encrypt the reduced text. The LZW method of compression is based on dictionary structure. It creates a dictionary of its own for each character or a string of the input text. It is known to be a lossless compression and the percentage of reduction in the text is approximately 40% [15].

Another frequently used compression algorithm is the well known Huffman Technique [16,17,18] which constructs a binary tree based on the frequency of the occurrence of the letters and the corresponding code is generated. We have also used Huffman algorithm on the same text and compared the two compression technique used with LWE.

II. Illustration of the Proposed Algorithm

The parameters of the proposed algorithm are chosen as q =2003, t =2, n =136, l =136, alpha = 0.0065 and m =2008 [11]

Original text message

str: wild animals, rocks, forest, beaches, and in general those things that have not been substantially altered by human intervention, or which persist despite human intervention.

The Compressed message using LZW is cmes=

$$\begin{bmatrix} 87 & 105 & 108 & 100 & . & . & . & 352 & 110 & 46 \end{bmatrix}$$

Where the integers indicate the indices to the patterns generated by the compression algorithm.

Then we convert the message vector as obtained above into a binary

v=

$$\begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & . & . & . & 0 & 0 \end{bmatrix}$$

$$f(v) = round(v \times \tfrac{q}{t}) =$$

$$\begin{bmatrix} 0 & 0 & 1002 & 0 & 1002 & 0 & 1002 & 1002 & 1002 & 0 & 0 & 1002 & 1002 & 0 & 1002 & 0 & 0 & 1002 & . & . & . & 0 & 0 \end{bmatrix}$$

$A \in Z_q^{m \times n}$ is chosen as

$$\begin{bmatrix} 1591 & 757 & 1974 & . & . & . & 1216 & 1991 \\ 757 & 1974 & 892 & . & . & . & 1991 & -1591 \\ 1974 & 892 & 1760 & . & . & . & -1591 & -757 \\ . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ 1137 & 1368 & 375 & . & . & . & -887 & -1301 \\ 1368 & 375 & 449 & . & . & . & -1301 & -1137 \\ 375 & 449 & 154 & . & . & . & -1137 & -1368 \end{bmatrix}$$

$S \in Z_q^{n \times l}$ is as follows

$$\begin{bmatrix} 1759 & 2 & 154 & . & . & . & 1044 & 1218 \\ 764 & 1434 & 996 & . & . & . & 1703 & 945 \\ 475 & 1846 & 462 & . & . & . & 956 & 1644 \\ . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ 136 & 591 & 1728 & . & . & . & 1489 & 708 \\ 782 & 945 & 84 & . & . & . & 121 & 1215 \\ 1271 & 916 & 1500 & . & . & . & 1439 & 76 \end{bmatrix}$$

$E \in Z_q^{n \times l}$ is as follows

$$\begin{bmatrix} -3 & 0 & -1 & . & . & . & 2 & 3 \\ -2 & 0 & 0 & . & . & . & 0 & 0 \\ -3 & -1 & -2 & . & . & . & -3 & 0 \\ . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ -7 & 4 & -1 & . & . & . & 8 & 1 \\ -2 & -2 & 0 & . & . & . & 2 & -6 \\ -4 & 1 & 4 & . & . & . & -1 & 2 \end{bmatrix}$$

$$B = A \times S + E (mod\ q) =$$

$$\begin{bmatrix} 1637 & 130 & 771 & . & . & . & 671 & 453 \\ 908 & 123 & 438 & . & . & . & 1399 & 264 \\ 527 & 963 & 184 & . & . & . & 1573 & 61 \\ . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ 720 & 312 & 299 & . & . & . & 1955 & 130 \\ 403 & 389 & 357 & . & . & . & 1428 & 1659 \\ 277 & 1467 & 1094 & . & . & . & 1056 & 39 \end{bmatrix}$$

Let $\boldsymbol{a} = \{-\mathbf{1}, \mathbf{0}, \mathbf{1}\}^{\boldsymbol{m}}$ where the elements are chosen randomly.

$$\begin{bmatrix} -1 & 0 & -1 & -1 & . & . & . & 0 & 1 & 1 & 1 \end{bmatrix}$$

$$\boldsymbol{C} = \boldsymbol{B}^{\boldsymbol{T}} \times \boldsymbol{a} + \boldsymbol{f}(\boldsymbol{v})(\boldsymbol{mod}\ \boldsymbol{q}) =$$

$$\begin{bmatrix} 98 & 1396 & 408 & 1049 & . & . & . & 291 & 1356 & 193 \end{bmatrix}$$

$$\boldsymbol{u} = \boldsymbol{A}^{\boldsymbol{T}} \times \boldsymbol{a}\ (\boldsymbol{mod}\ \boldsymbol{q}) =$$

$$\begin{bmatrix} 314 & 1840 & 1588 & 148 & . & . & . & 988 & 1447 & 1125 \end{bmatrix}$$

$$\boldsymbol{D} = \boldsymbol{C} - \boldsymbol{S}^{\boldsymbol{T}} \times \boldsymbol{u}\ (\boldsymbol{mod}\ \boldsymbol{q}) =$$

$$\begin{bmatrix} 1952 & 1992 & 13 & 58 & . & . & . & 15 & 1998 & 143 \end{bmatrix}$$

D/(q/t) =

$$\begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ & 1 & 0 & 1 & 0 & 0 & 1 & . & . & . & 0 & 0 \end{bmatrix}$$

Convert binary to decimal

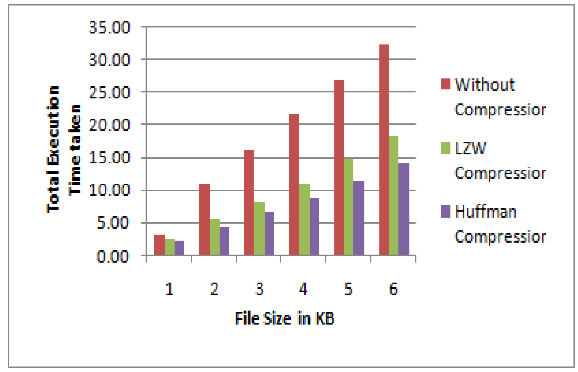
$$\begin{bmatrix} 87 & 105 & 108 & 100 & . & . & . & 87 & 105 & 108 & 100 \end{bmatrix}$$

When the compression process is reversed we get the original message:

III. Experimental Results

The following table gives the total execution time taken for a direct encryption and decryption, encryption and decryption after a LZW compression and encryption and decryption after a Huffman compression:

File Size in KB	Total Execution time without Compression	Total Execution time with LZW	Total Execution time with Huffman
1	3.13	2.4289	2.10777
2	10.84	5.3588	4.28654
3	16.26	8.1736	6.56431
4	21.63	10.9583	8.90506
5	27.00	14.7273	11.39183
6	32.43	18.2190	13.98658



IV. Conclusions

In this paper we have used ring-LWE to encrypt an input text. The text to be transmitted has been initially compressed using LZW Technique and the compressed text is encrypted using LWE. We have also used Huffman coding algorithm for compression for comparison purpose. It has been observed that compressing the input text greatly reduces the total time of transmission and Huffman coding works out to be better.

References Références Referencias

1. J. Hoffstein, J. Pipher, and J. H. Silverman. NTRU: a ring based public key cryptosystem. In Proceedings of ANTS-III, volume 1423 of LNCS, pages 267–288. Springer, June 1998.
2. J. Hoffstein, N. A. H. Graham, J. Pipher, J. H. Silverman, and W. Whyte. NTRUSIGN: Digital signatures using the NTRU lattice. In Proc. of CT-RSA, volume 2612 of Lecture Notes in Comput. Sci.,pages 122–140. Springer-Verlag, 2003.
3. J. Hoffstein, N. Howgrave-Graham, J. Pipher, and J. H. Silverman. Hybrid lattice reduction and meet in the middle resistant parameter selection for NTRUEncrypt. Submission/ contribution to ieee p1363.1, NTRU Cryptosystems, Inc., URL http://grouper.ieee.org/groups/1363/lattPK/ submissions.html#2007-02, 2007.
4. M.N.M.Prasad, Mohammed Ali Hussain, C.V.Sastry "NTRU Encryption using Huffman comprssion" , Journal of Theoretical and Applied Information Technology, Volume.59,No.2, pages 379-384,Jan 2014.
5. D. Micciancio and O. Regev. Worst-case to average-case reductions based on Gaussian measures. InProc. 45th Annual IEEE Symp. on Foundations of Computer Science (FOCS), pages 372–381, 2004.
6. D. Micciancio. Improving lattice based cryptosystems using the hermite normal form. In J. Silverman,editor, Cryptography and Lattices Conference — CaLC 2001, volume 2146 of Lecture Notes in Computer Science, pages 126–145,

Providence, Rhode Island, Mar. 2001. Springer-Verlag.

7. D. Micciancio. Lattices in cryptography and cryptanalysis, 2002. Lecture notes of a course given in UC San Diego.
8. Haviv and O. Regev. Tensor-based hardness of the shortest vector problem to within almost polynomial factors. In Proc. 39th ACM Symp. on Theory of Computing (STOC), pages 469–477, 2007.
9. S. Khot. Hardness of approximating the shortest vector problem in lattices. In Proc. 45th Annual IEEE Symp. on Foundations of Computer Science (FOCS), pages 126–135, 2004.
10. O. Regev. On lattices, learning with errors, random linear codes, and cryptography. J.ACM, 56(6),2009.
11. D. Micciancio and O. Regev. Lattice-based cryptography. In D. J. Bernstein and J. Buch-mann, editors, Post-quantum Cryprography. Springer, 2008.
12. Parvinder Singh,ManojDuhan and Priyanka (2006)" Enhancing LZW Algorithm to Increase Overall Performance", Annual IEEE Indian Conference,pp1-4.
13. Ming-Bo Lin, Jang-Feng Lee, G. E. Jan,(2006)"A Lossless Data Compression and Decompression Algorithm and Its Hardware Architecture" VLSI IEEE Transactions ,Vol.14,pp925-936.
14. Mateosian, R, "Introduction to Data Compression" (1996), vol.16.
15. V.Sulochana Verma, Design and Implementation of LZW Data Compression Algorithm, in IJIST vol2, No.4, July 2012.
16. Salomon D. Huffman Coding available at http://www.springer.com/978-1-84800-071-1, ISBN:978-1-84800-071-1,Softcover,2008
17. J. S. Vitter: Algorithm 673 Dynamic Huffman Coding. ACM Transactions on Mathematical Software, 15(2), June 1989, 158-167 (1989).
18. Lecture-15: Huffman Coding (CLRS-16.3) available at www.cse.ust.hk/~dekai/271/ *notes/L15 /L15.pdf*

Global Journals Inc. (US) Guidelines Handbook 2014

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.

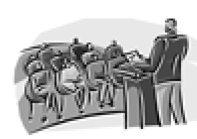
- The "FARSC" is a dignified title which is accorded to a person's name viz. Dr. John E. Hall, Ph.D., FARSC or William Walldroff, M.S., FARSC.

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.

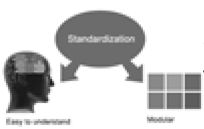


You may join as member of the Editorial Board of Global Journals Incorporation (USA) after successful completion of three years as Fellow and as Peer Reviewer. In addition, it is also desirable that you should organize seminar/symposium/conference at least once.

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.

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).

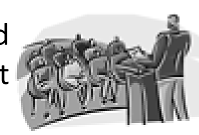
The “FARSC” is a dignified title which is accorded to a person’s name viz. Dr. John E. Hall, Ph.D., FARSC or William Walldroff, M.S., FARSC.

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%.



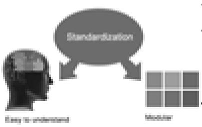
The Global Journals Incorporation (USA) at its discretion can also refer double blind peer reviewed paper at their end to the board for the verification and to get recommendation for final stage of acceptance of publication.

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 <u>(Must be strictly followed)</u>

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 <u>definite statistics</u> - if the consequences are quantitative in nature, account quantitative data; results of any numerical analysis should be reported
- Significant conclusions or questions that track from the research(es)

Approach:

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

Introduction:

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

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

Approach:

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

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

Procedures (Methods and Materials):

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

Materials:

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

Methods:

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

Approach:

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

What to keep away from

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

Results:

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

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

Content

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

What to stay away from

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

Approach

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

Figures and tables

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

Discussion:

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

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

Approach:

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

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

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

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

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

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

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

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

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

INDEX

A

E

H

L

S

V

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