iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** VIII **Month of publication:** August 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A Research Study on Efficient Management of Memory in Mobile Ad Hoc Network in Trust Management System Environment

S.Mohamed Imranul Hasan[#1], Dr.Radhika.V [#2]

#Research Scholar ,Deparment of Computer Science,Sri Krishna Arts And Science College,Coimbatore

Principal,Sri Krishna Adithya Arts And Science College,Coimbatore.

Abstract— The simple Mobile Ad hoc network has only limited storage capabilities. In order to construct an efficient Trust Management System in the Existing Mobile Ad hoc Network and make it perform the real time decisions based on the events is much difficult and at a same time a Cumbersome task. Due to the season that the mobile Ad hoc Network has only the limited infrastructure Capabilities. It had been designed and developed for simple and at the same time more efficient communication setup. To Prevent the Mobile Ad hoc Network from Various Attacks and Vulnerabilities an trust Management system has to be used. The Trust management system will perform based on large Constraints of information's. These Information's has to be made available in the particular Mobile Ad hoc Networking system for the trust management system to prevent the Mobile Ad hoc network from Attack. But it requires a most important need that large quantities of data and information's has to be stored. But the major problem in this system is that huge amount of data are to be stored and accessed from the limited storage Capacity of the Mobile Ad hoc Network. This requirement has to fulfill to make the trust management system more Cost and Performance Effective One.

Keywords— MANET.LOAD SHARING, MEGA BYTES

I. INTRODUCTION

In this research paper we focus on the most important issue that the memory management issues that are available in the mobile Ad hoc network. We need to address this problem because the reason that the mobile Ad hoc network has the limited infrastructure Capabilities. In this research paper we also have an elaborate look and analysis on the memory management techniques and planning to make use of the available Storage resources of the Mobile Ad hoc network in a most efficient manner. We have to formulate certain memory management techniques like this to make the trust management system in the Mobile Ad hoc network Much Effective One.

II. LITERATURE SURVEY

An easy way to comply with IJRASET paper formatting requirements is to use this document as a template and simply type your text into it.

A. Ad hoc Network

The Word Ad-hoc which are commonly used today originates from a Latin word , which means "for this purpose ". The Most Popular Ad-hoc network is an self operable networks that can be deployed anyplace and anytime without the need of a large and costly infrastructure. It is used for military oriented purposes.

B. Mobile Ad-hoc Network (MANET)

A mobile ad hoc network (MANET) is an combination of a group of continuously self-configuring, infrastructure-less network of movable devices connected without the help of wires. Each and every device in a MANET is free to move independently in any direction,able to communicate with each other and will therefore change its links to other devices frequently. Each and every single devices that are communicating within the mobile ad hoc network must exchange traffic unrelated to its own use, and therefore each device act as a router. The major and more important aspect and challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic.

©IJRASET 2015: All Rights are Reserved

Volume 3 Issue VIII, August 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

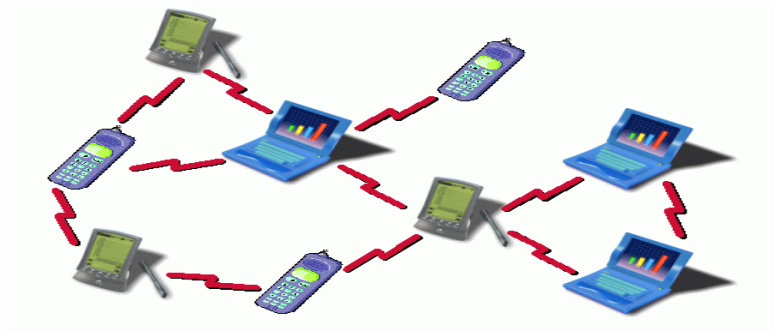


Fig. 1:A Typhical MANET Structure

In the above depicted figure both the laptops and cell phones exchange informations among themselves. They use configuration less communication gateways to establish connection among themselves. In mobile Ad hoc Network various types of telecommunication devices communicate among them.

III.TRUST MANAGEMENT SYSTEM

The trust management system are designed and developed in the mobile ad hoc network to prevent the various attacks and vulnerabilities that are affecting the Mobile Ad hoc Network. These trust management Systems are called so because the is no central Administration Unit to control all the activities of the mobile Ad hoc Network. All the Communications are based on the trust. It means the nodes participating in the communicating circle of the mobile Ad hoc Network are analysed and trusted to make data Communication.

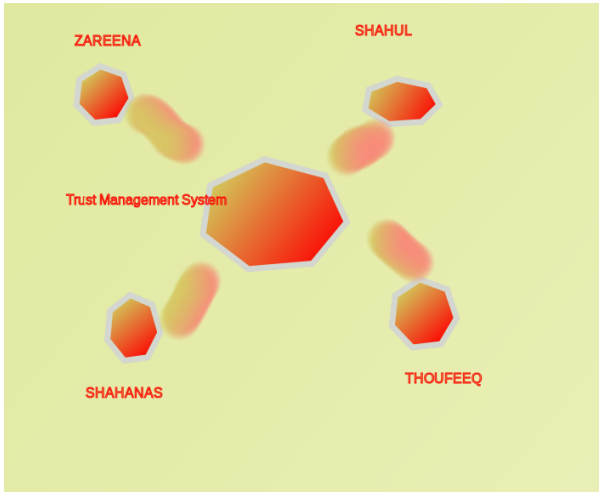


Fig.2: Trust Management System Architecture

The above Figure is an example of Trust Management System. In the Above figure the Big polygon shape is a Trust Management System. All the remaining nodes named Zareena,Shahul,Shahanas and Thoufeeq. These nodes will share all there details with the trust management System.

IV.MEMORY MANAGEMENT

The main and mast important consideration that has to be focused in deployment of information sharing based trust management System is memory management. We have already we understood the Mobile Ad hoc Network has only limited information storing power.

©IJRASET 2015: All Rights are Reserved

A. *Need for Memory*

We will now have a detailed research on a situation in where we have to effectively Control and C-ordinate the memory. For an example consider a environment that we have constructed an Trust Management System that allows the nodes participating in the Communication Environment of the Mobile Ad hoc to Communicate among themselves based on the track record of the nodes. It means it is situation the trust management system has to keep all the previous Transaction histories of the nodes that are participating in the Communication System. It is based on the principle that "Information of All, For All". It means in the real sense the trust management system is not a single controlling authority that are present in the Mobile Ad hoc Network, because this is due to the reason that Mobile Ad Hoc network does not have a Central Control Authority. So in order to achieve our aim of constructing an Trust Management System that operates based on the Previous Informations, that will make the Mobile Ad hoc Network Much Secure for communications. So there in a need for memory and memory Management to make it as a well operable Environment.

B. Memory Overflow Issue

The memory management technique can be looked very detailedly by using a certain Environment. For Example Consider a Mobile Ad hoc network Communication Environment System has five nodes. And each nodes have a Storage Capacity of 1Mb.

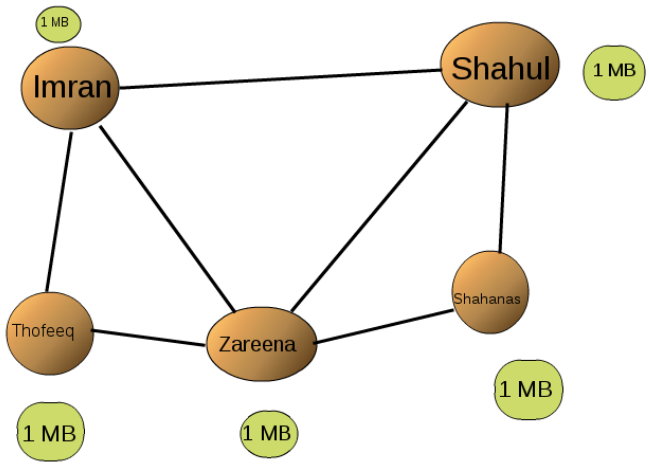


Fig.3 :Initial Memory Allocated

In the Trust Management System Environment Each and information's of the nodes like name, id, Previous Nodes, Next Nodes and Data Transmission Records Will be kept in record for future references. If each transaction takes place the nodes that are available among the source and destination will be kept as back in all the intermediate nodes that are present in between them.

In the below figure the node "imran" wants to communicate and sent data to the node "Shahanas".In the path between the nodes "imran" and "Shahanas" there lies a node "shahul" as an intermediate node. When the data are transferred from the "imran" to "Shahanas" the details of the communication are stored in both these nodes as well as in the node "Shahul" on the respectively 1MB Memory. By Using the data that are stored already the Communication can be made safer and most effective one because, through the previous operations data we can choose the the most optimal and at the same time we can avoid the paths that are Vulnerable for the attacks. In this manner the effective Communication can be done with a time efficient manner.

©IJRASET 2015: All Rights are Reserved

Volume 3 Issue VIII, August 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

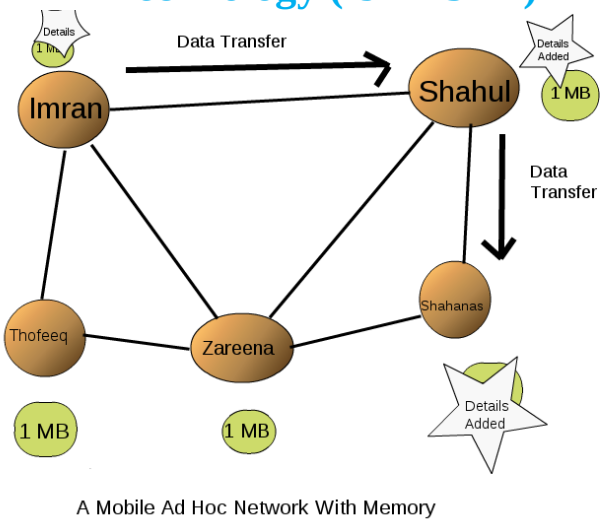


Fig.4: Data Transferring State

But Consider a situation when all the Communication nodes takes place in a simultaneous manner as follows.

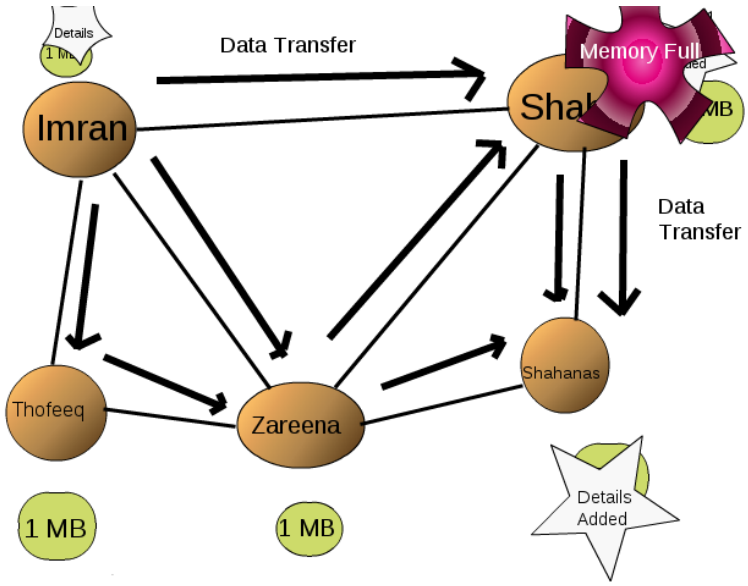


Fig.5: Memory Full Problem

In the above figure all the nodes that are participating in the Mobile ad hoc Network Communication Environment are trying to send data to the node “Shahanas” mostly by using the intermediate node “Shahul”.As we have seen already that each nodes have only 1 MB of memory and when each passing takes places that intermediate nodes will have to have the details. If the situation like above

©IJRASET 2015: All Rights are Reserved

takes place the operation will be collapsed.

C. Memory Management Technique

These memory overflow Problem has to be addressed effectively in order to make the system to function in a most efficient manner. We can tackle this memory overflow problem with a technique called "Load sharing". Load Sharing means will the available memory is full that memory space less node should and will share its data load with the nearest nodes in an encrypted format based on the private key encryption Technique. By the "Load Sharing" technique the memory full problem will be avoided and when the shared nodes memory is free it can revoke it and it can decrypt it by its own and make the data available for all the other nodes requesting the information's about the nodes for Communication. Since it is sent using the private key encryption method the helping nodes receiving the encrypted data will not be able to get to know the details of the encrypted content. In this way it make the load sharing contents much secure one.

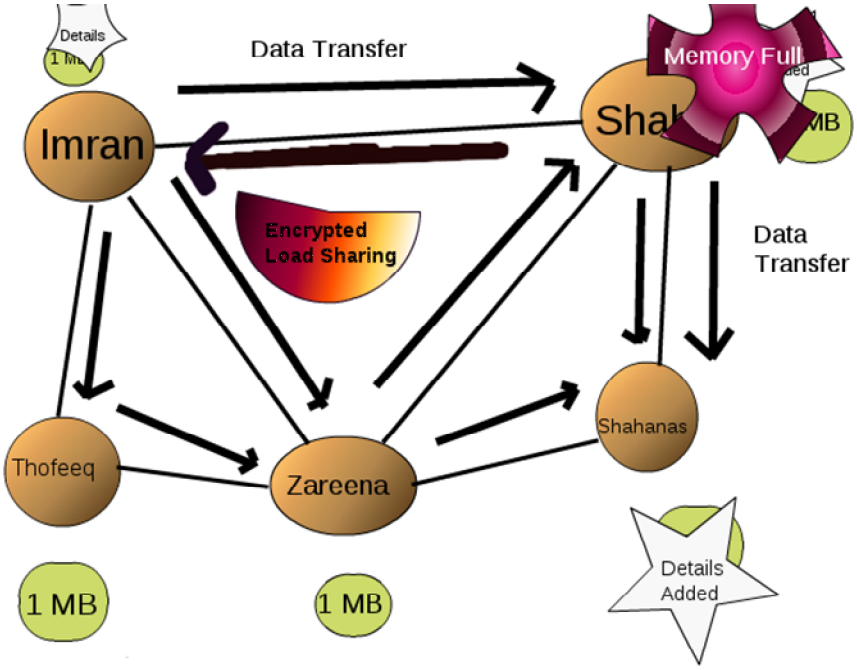


Fig.6: Encrypted Load Sharing

V. ACKNOWLEDGMENT

The word Acknowledgment is the most respectable way to express our gratitude to those who backed us in all our endeavors. We are honoured to thank our parents, family members, friends and all our teachers who has been generously giving their support in all our endeavours. We also thank the Almighty who created and protect us all.

REFERENCES

[1] Security Issues in MANET: A Review. Mahakal Singh Chandel,Arjun Institute of Advaced Studies and Research Centre, Indore,India. Rashid Sheikh,Durgesh Kumar Mishra, Acropolis Institute of Technology and Research, Indore, India,2010 IEEE.

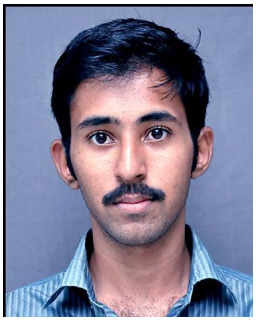
[2] Security Architecture for MANET and It's Application in m Governance,Baljeet Kaur, Bharati Vidyapeeth Deemed University, Pune. Institute of Management and Entrepreneurship Development. 2013 International Conference on Communication Systems and Network Technologies.

[3] T. H. project, "Know your enemy," July 2000. [Online].Available: http://project.honeynet.org/papers

©IJRASET 2015: All Rights are Reserved

[4] Locating the Attacker of Wormhole Attack by Using the Honeypot.T Divya Sai Keerthi and Pallapa Venkataram.Electrical Communication Engineering Department, Indian Institute of Science, Bangalore,India. 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications.
[5] L. Capra, "Toward a Human Trust Model for Mobile Ad-hoc Networks," Proc. 2nd UK-UbiNet Workshop, 5-7May 2004, Cambridge University, Cambridge, UK.
[6] J. Li, R. Li, and J. Kato, "Future Trust Management Framework for Mobile Ad Hoc Networks: Security in Mobile Ad Hoc Networks,"IEEE Communications Magazine, vol. 46, no. 4, Apr. 2008, pp. 108-114.
[7] R. Li, J. Li, P. Liu, H. H. Chen, "An Objective Trust Management Framework for Mobile Ad Hoc Networks," Proc. IEEE 65th Vehicular Technology Conf. (VTC'07), 22-25 Apr. 2007, pp. 56-60.
[8] N. C. Fernandes, M. D. D. Moreira, and O. C. M. B. Duarte, "An efficient filter-based addressing protocol for autoconfiguration of mobile ad hoc networks," in IEEE INFOCOM'09, Apr. 2009.
[9] B. Ishibashi and R. Boutaba, "Topology and mobility considerations in mobile ad hoc networks,"Ad Hoc Netw. J., vol. 3, no. 6, pp. 762-776,Nov. 2005.
[10] P. B. Velloso, R. P. Laufer, O. C. M. B. Duarte, and G. Pujolle, "HIT: a human-inspired trust model," in 8th IFIP IEEE International Conf. Mobile Wireless Commun. Netw., Santiago, Chile, Aug. 2006
[11] htttp://www.strategicaffairs.com/webmaster/other_story/images/Better transmission.jpg.

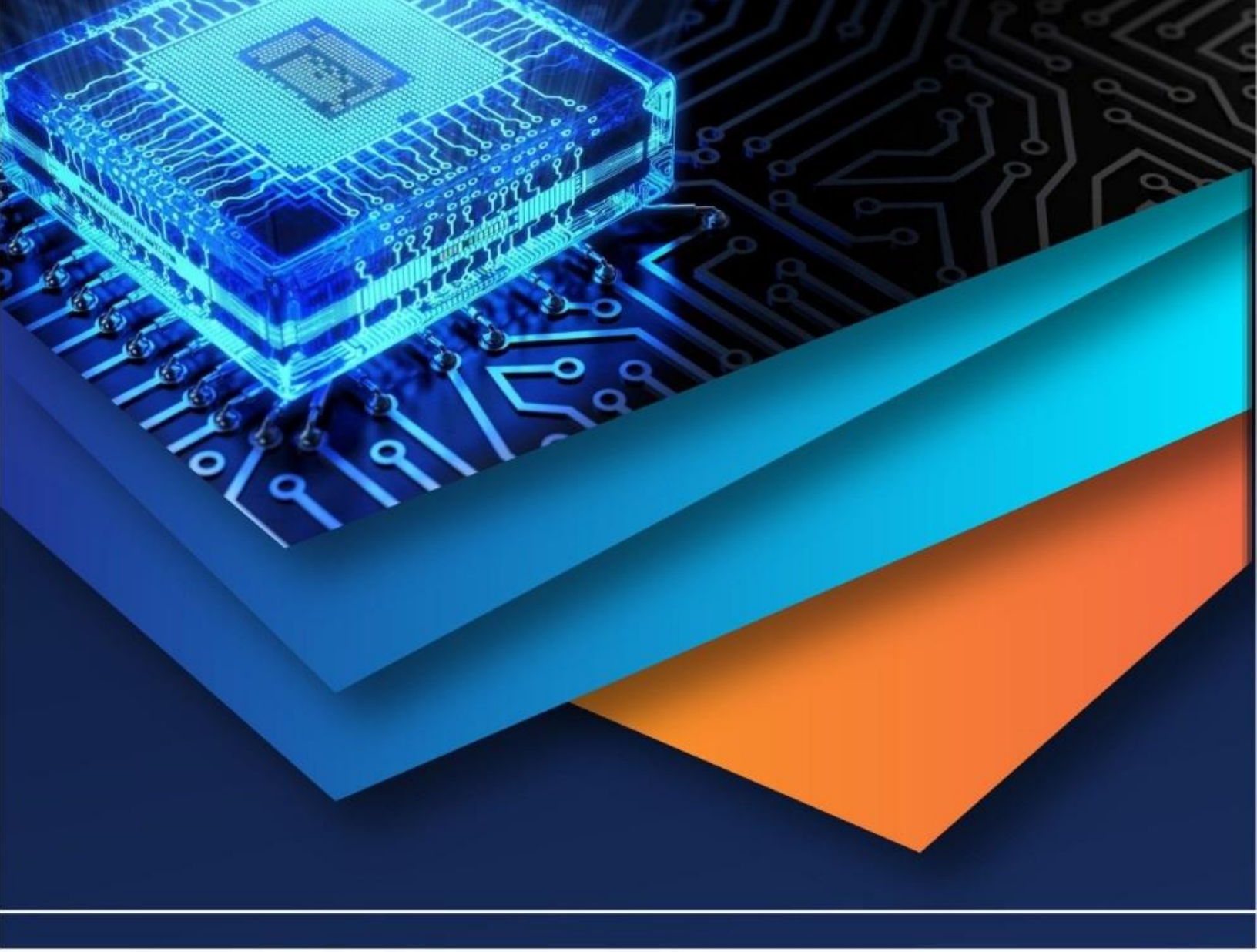
AUTHORS



S. Mohamed Imranul Hasan, received his Bachelor of Computer Applications, degree from Jamal Mohamed College, Bharadhidasan University, Trichy. He also received Master of Computer Applications, degree from SVS Institute Of Computer Applications,Anna University, Chennai. He is doing his research degree in Computer Science,Sri Krishna Arts And Science College, Bharathiar University, Coimbatore.

Radhika.V received her B.Sc (Phy) ,MCA and M.Phil degree from Bharat
hiar University Coimbatore. in 1993 ,1996 and 2003 respectively. She received her PhD from Avinashilingam university for women, Coimbatore. in 2013. She is the Principal, Sri Krishna Adithya Arts And Science College , Coimbatore. She has 18 years of teaching experience. She has more than 25 publications at national and International level.

©IJRASET 2015: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)