GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

A SURVEY ON INTRUSION DETECTION METHODS IN MULTIHOP MANETs

T. Parameswaran [1], Dr. C. Palanisamy[2], G.M. Rajasekar[3]
Department of Computer Science and Engineering, Anna University Regional Centre, Coimbatore, India[1,3]
Professor and Head, Department of Information Technology, Bannari Amman Institute of Technology, Sathyamangalam, India[2]

ABSTRACT

MANET plays a major role in next generation wireless networking technology. Information exchange in a mobile network without any infrastructure support, such networks are called Adhoc networks. This plays a major platform and used in important applications. A Mobile Adhoc Network is a mobile multihop wireless network, which is capable of autonomous operation. The self-configuring ability of nodes in MANET made popular among critical mission applications like military use or emergency recovery. Because of the open medium and wide distribution of nodes make MANET harm to malicious attackers. It is crucial to develop efficient intrusion detection mechanisms to protect MANET from attacks. We present a various types of attacks in the network layer and Intrusion Detection mechanisms are used for protecting multihop MANET. To overcome the attacks, a comparison of various types of attacks and different IDs mechanisms are made. We classify, a single type of attack can be achieved by point detection algorithm (PDA) and range of attacks can be achieved by intrusion detection systems (IDs). Our survey is based on various types of attacks on multihop MANET and investigation of problems caused through malicious nodes by various types of Active and Passive group.

Keywords— Multihop, Intrusion Detection Systems (IDs), network layer attacks, mobile adhoc networks (MANETs), Active attacks, Passive attacks, ABID, KBID, SBID, PDAs.

I. INTRODUCTION

The MANETs is less protection to various types of attacks in the network layer. Because, the design of most MANET routing protocols assumes no malicious intruder node in the network. But, due to the attacks there is no proper security protections are made. Therefore IDs and prevention approaches for network layer attacks have been made for the survey. Mobile devices working together concept was proposed in the year 1990s, since when a significant amount of research has been conducted on mobile adhoc networks (MANETs). The establishment of Mobile Adhoc Networks Working Group [1] made in 1997.During that time, the both reactive and proactive MANET protocols was developed. MANETs have wide applications in various fields. For example, they have been used in a military context since 1970s to ensure the flow of information and command in battle to the success of a mission. MANETs are also ideal for establishing communication networks and provides some rescue services following natural disasters such as earthquakes or floods. Researchers are also investigating the technologies of application scenarios for MANETs in commercial areas. For example, MANETs can be used in communication dispatch systems for taxis in a town to inform individual taxis about passenger pickups, route directions, weather conditions, etc. Finally, they can also be used in personal networking: for example, PDAs [2] notepads, and cell phones can form an adhoc network to communicate and achieve other networking capabilities. Standard information security measures such as encryption and authentication do not provide complete protection, An intrusion detection and prevention (IDP) mechanisms are widely used to secure MANETs.

Intrusion detection (ID) in MANETs is more complex and challenging than in fixed networks, because of the difficulty in fulfilling the requirements and create operational implementation complexities. The challenges for IDSs in MANETs [2] are as follows:

- MANETs lack concentration points during the time of monitoring and audit data collection can be performed.
- MANET routing protocols require different nodes to cooperate and act as routers in Multihop, creating opportunities for attacks
- Due to the node's mobility, the network topology is dynamic and unpredictable, making the process of

intrusion detection complicated.

- IDSs in MANETs are more complex because of the limited computational ability of most of the nodes.

To cover the wide range of intrusion detection and prevention techniques in MANETs, we divide the techniques into two categories: the one designed to deal with a single type of attack (which we call point detection algorithms), and another that can identify a range of attacks, which we consider to be true IDSs (INRUSION DETECTION SYSTEMS). A number of surveys of intrusion detection for MANETs have been published. The authors of presented a survey of Anomaly-based intrusion detection systems (ABID) [2] for MANETs and other systems like Knowledge-based intrusion detection systems (KBID) [2] and Specification-based intrusion detection systems (SBID) [2].

Comparison of IDSs based on the type of attack addressed in the various architecture [19]. But suggestion of that ID needs a scalable architecture based on cross-layer design to detect these attacks effectively. We classify, a single type of attack can be achieved by point detection algorithm (PDA) [2] and range of attacks can be achieved by intrusion detection systems (IDs). Based on this factor, Comparison of proposed different IDs mechanisms and drawbacks for various attacks in Multihop MANETs are made in this survey.

The rest of our paper is organized as follows. In Section II we present Attacks in MANETs then various types with examples and Classification of attacks. Section III reviews the network layer protection mechanisms are made. Section IV then considers existing IDs mechanisms and its Challenges in MANETs. Section V Compares the proposed IDs techniques and drawbacks for detecting a range of attack types. Finally, Section VI presents a Conclusion and future research directions towards this survey.

II. ATTACKS IN MANETs

In this section we first present a classification of major types of network layer attacks.

A. Classification of Network layer Attacks

The classification of network layer attacks [2] in MANETs can be divided into two main categories as shown in figure 1, namely

1. Passive Attacks
2. Active attacks.

1. Passive Attacks: Passive attacks are those where the attacker does not disturb the operation of the routing protocol, but attempts to see some valuable information through traffic analysis. This can lead to the disclosure of critical information about the network.

Example: *Eavesdropping*

Eavesdropping [20] is a type of passive attacks. In this a message sent by a node as the sender and can be heard by the node as a receiver within radio range. During this time when no encryption mechanisms are used, then attackers may get useful information. Therefore, both sender and receiver usually have no means of knowing that this attack has taken place. Due to this case Eavesdropping is not considered to be a severe attack. Our survey is to focus like this type of drawbacks in the attacks and to minimizing it.

2. Active Attacks: In active attacks the intruders launch some intrusive activities such as

- Modifying
- Injecting
- Forging
- Fabricating or dropping data.

When compared to the passive attacks. The Active attacks disturb the operations of the network. It can be so severe that they can bring down the entire network or degrade the network performance significantly.

Example: *Malicious Packet Dropping*

After Route Discovery process is made between the source and destination, the source node starts sending the data packet to the next node in a path to reach the destination. This intermediate node identifies the next hop and forwards data packets until the data packet reaches the destination node. This the Multihop is taking place while forwarding the data. During this time, a malicious node might decide to drop these data packets instead of forwarding them. This is known as a data packet dropping attack.

B. Classification of Attacks Representation:

Attacks can be classified into passive and active groups [2]. Each group has the various types of attacks in a distinguished manner. Due to disturbing operation in the network, the routing and malicious packet dropping are related to active attacks. Attacks like eavesdropping, location disclosure and traffic analysis are related to passive attacks.

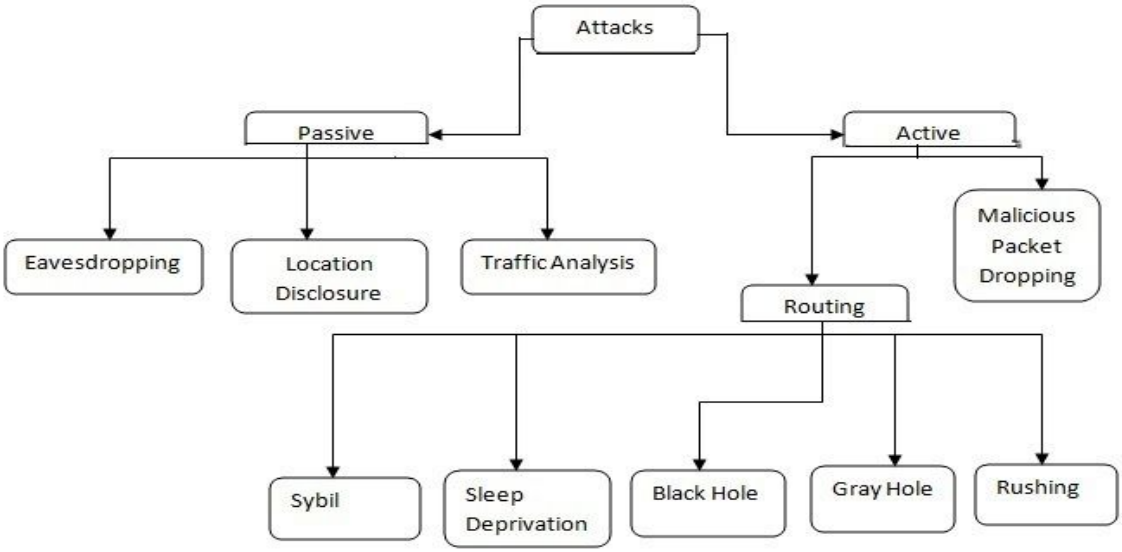

Fig.1. Classification of attacks.

III. NETWORK LAYER PROTECTION MECHANISMS

A. Taxonomy of Network layer protection mechanisms for various attacks:

The protection mechanisms of network layer can be classified into point detection algorithms and intrusion detection systems. The various types of attacks like sleep deprivation, black hole, gray hole, data packet dropping, rushing are classified by point detection algorithms [2] in the network layer. To overcome the attacks, different IDs mechanisms are used like ABID, SBID, and KBID. Hybrid mechanisms will combine the other IDs for detection.

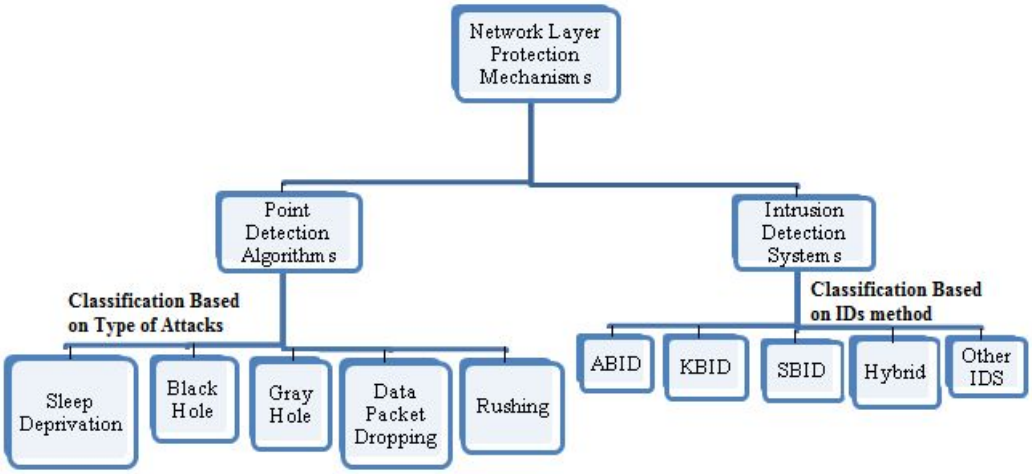

Fig.2. Network layer protection mechanisms.

ABID = Anomaly –Based IDs.
KBID = Knowledge-Based IDs.
SBID = Specification-Based IDs.

B. Intrusion Detection Systems for Various Attacks:

Intrusion Detection Systems can be split into three main classes based on the detection approach they are: (1) anomaly-based intrusion detection (ABID), also known as behavior-based intrusion detection; (2) misuse detection, which is also known as the knowledge-based intrusion detection (KBID); and (3) specification-based intrusion detection (SBID).

1) Anomaly-Based Intrusion Detection: Anomaly-based intrusion detection (ABID) systems used as anomalous observed activities that deviate significantly from the normal profile [2]. ABID systems are also known as behavior-based intrusion detection. With the help of both Testing and Training Process expected behavior can be identified and provide early warning and generate the alarms for false behavior.

2) Knowledge-based Intrusion Detection: Knowledge- based intrusion detection systems maintain a knowledge base that contains signatures or patterns of well-known attacks and looks for these patterns in an attempt to detect them. But, they can only detect attacks whose signatures or patterns are in the knowledge base and gathering the required information about attacks. And for keeping them up to date is a demanding task. [2]

3) *Specification-Based Intrusion Detection Proposals:* The SBID approach was introduced and tested in fixed networks in [21] [22] [23]. In MANETs, SBIDs describe the correct operation of the protocol by defining a set of constraints, and monitor the execution of the protocol with respect to the defined constraints to detect anomalies in the network.

IV. EXISTING IDS MECHANISMS AND ITS CHALLENGES

A. Comparison of Existing IDs Mechanisms:

The existing IDs mechanisms are made and represented by different classification methods. With the help of above three IDs method with hybrid based intrusion detection systems and other intrusion detection systems, each attack is detected with proper architecture and algorithm. Then the responses for each detection are made

successfully. From this, the source of data and routing protocol are identified during the process and finally contributions are taking place with the detection techniques.

B. Challenges of intrusion detection systems in MANETs:

IDs are not directly implementable in the wireless network environment for fixed networks. In this traffic is monitored and node can observe other within its radio range. Therefore attackers outside this radio range can escape easily. To avoid that IDs are used. Fixed networks are not directly implementable in MANETs. On realizing this difficult situation, researchers have proposed approaches of audit data collection and the application of IDs techniques using network clustering in MANETs.

C. Proposed IDs for MANETs:

We know that the above IDs methods are used for detecting the various types of attacks. In this survey the other types of IDs mechanisms are carried out and the drawbacks for each mechanism are explained. This survey illustrates the different IDs techniques for the various attacks like Black hole attack [3] [4] [5], Gray hole attack [6] [7] [8], Sybil attack [9] [10], Rushing attack [11] [12], Sleep Deprivation attack [13], and DOS attacks [14] [15] [16] [17] [18]. These each attack are detected by IDs mechanisms and drawbacks for each attack with suitable descriptions are illustrated as shown in Table I. These attacks are taking place in the multihop network layer; hence this can play a major role in the survey on intrusion detection systems in multihop MANETs.

V. COMPARISON OF PROPOSED IDS METHODS AND DRAWBACKS FOR ATTACKS IN MULTIHOP

Table. 1 Comparison of Proposed Ids Methods And Drawbacks For Attacks In Multihop

S.No	Types of Attacks	Detection Methods	Description	Drawbacks
1.	Black hole attack	1. Black Hole Attack and Detection Method	1. Analyze the Destination sequence number.	1. Additional delay due to pre-process
		2.Detection,Prevention and Reactive AODV	2. Stores the Destination sequence number of incoming route reply packets (RREPs) in the routing table and calculates the threshold value to evaluate the dynamic training data in every time interval.	2. Does not consider other attacks
		3. Defense mechanism	3. Use data routing information table and identify attacks.	3. Less performance because it does not consider resource Consumption attack and packet dropping attack.
2.	Gray hole attack	1. Security mechanism	1. This method increases the reliability of detection by Proactively invoking a collaborative and distributed algorithm involving the neighbor nodes of a malicious gray hole node.	1. High congestion occurs.
		2.Destination based group Gray hole attack detection	2. This method to detect Cooperative malicious nodes by destination based	2. Less packet delivery ratio.

		method 3. Detection & Prevention of Gray Hole Attack method	routing method. 3. This method helps to protect the network by detecting and reacting to malicious activities of any node.	 3. Less efficient in terms of security.
3.	Sybil attacks	1. Lowest ID cluster-based routing protocol 2. Mobility Based detection method 3. Mobile-id Based Sybil Attack detection	1. Based on the transmission power the attack is detected. 2. Passively monitor traffic in the network can detect a Sybil attacker that uses a number of network identities Simultaneously 3. Use these algorithms to transfer the data from source to destination without any damage or loss as well as each node to have the neighbor's node address. Depends on the address the data will be transmitted into the correct destination	1. Credibility and efficiency is less. 2. Less scalability. 3. Does not consider the use secure and avoid the attacking system on the network.
4.	Rushing attack	1. Secure neighbor detection, and secure route discovery procedure 2. Rushing Attack and Defense method 3. Rushing attack prevention (RAP)	1. In this method, When a node transmits a request is claiming a path between sender and receiver, but this score Neighbour detection cannot prevent an attacker to receiving a request. 2. Specifically, the rushing attack prevents previously published secure on-demand routing protocols to find routes longer than two-hops. 3. This work proposes Rushing attack prevention can be done by calculating the threshold time and average time and comparing it with request time.	1. High complexity 2. High cost 3. High congestion
5.	Sleep Deprivation Attack	1. Dendritic cell algorithm(DCA)	1. It utilizes the functionality of the dendritic cells in the innate immunity of the HIS. DCA proved the capability of detecting port scanning attack which certifies its qualification as an anomaly detector algorithm.	1. High false positive rates
6.	DOS attack	1.Adaptive Intrusion Detection & Prevention method 2. Intrusion detection system	1. This method uses a combination of chi-square test & control chart to first detect intrusion and then identify an intruder. 2. This method first analyzes the main vulnerabilities in the mobile ad hoc networks.	1. Does not consider other related parameters to cover all routing attacks 2. Does not apply for large-scale networks.

The above table shows the comparison of different IDs mechanisms for the various types of attacks. The Back hole attack has different IDs methods and the descriptions are made by an operation perform in IDs. The drawbacks for

each description are also used here to know the status of the black hole attack. This can also be applicable to the other type of attacks in MANETs.

VI. CONCLUSION AND FUTURE WORK

The distributed nature of MANETs is necessary to protect from many network layer attacks. In this paper, we presented a survey of IDs for network layer attacks through multihop and we commonly noticed and utilized attacks like Black hole attack, Gray hole attack, Sybil attack, Rushing attack, Sleep deprivation attack, and Dos attack. These each attacks are identified and IDs methods are used to overcome, each IDs are described for above attacks and the status are identified with drawbacks. These attacks are noticed and utilized in this survey, other than this there is a chance in formation of different attacks. That unfocused attacks should focus and related IDs should apply in the future enhancement.

VII. REFERENCES

[1] *IETF Mobile Ad-Hoc Networks Working Group (MANET), IETF website IETF Mobile www.ietf.org/dyn/wg/charter/manet- charter.html.*

[2] *Adnan Nadeem, Michael P.Howrath. "A Survey of MANET Intrusion Detection and Prevention Approaches for Network layer Attacks". IEEE Communications surveys and tutorials Vol. 15. No. 4, Fourth Quarter 2013.*

[3] *Vipin Khandelwal M. Tech IC, Dinesh Goyal Associate Professor. "Black Hole Attack and Detection Method for AODV Routing Protocol in MANETs". International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2 .April 2013.*

[4] *Vipan Chand Sharma, Atul Gupta, Vivek Dimri. "Detection of Black Hole Attack in MANET under AODV Routing Protocol". International Journal of Advanced Research in Computer Science and Software Engineering volume 3, 6 June 2013.*

[5] *Jaydip Sen1, Sripad Koilakonda2, Arijit Ukil3. "A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Ad Hoc Networks" Tata Consultancy Services Ltd.*

[6] *Jaydip Sen, M. Girish Chandra, Harihara S.G., Harish Reddy, P. Balamuralidhar. "A Mechanism for Detection of Gray Hole Attack in Mobile Ad Hoc Networks". Embedded Systems Research Group, Tata Consultancy Services.*

[7] *Avenash Kumar 1, Meenu Chawla. "Destination based group Gray hole attack detection in MANET through AODV". IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 4, No 1, July 2012.*

[8] *Onkar V. Chandure, V. T. Gaikwad. "Detection & Prevention of Gray Hole Attack in Mobile Ad-Hoc Network uses AODV Routing Protocol". International journal of computer Applications Vol 41- No 5, march 2012.*

[9] *Amol Vasudeva1 and Manu Sood. "Sybil attack on lowest id clustering algorithm in the mobile ad hoc Network". International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.5, September 2012.*

[10] *P.Kavitha, C.Keerthana, V.Niroja, V.Vivekanandhan."Mobile-id Based Sybil Attack detection on the Mobile ADHOC Network". International Journal of Communication and Computer Technologies Volume 02 - No.02 Issue: 02 March 2014.*

[11] *Satyam Shrivastava. "Rushing Attack and its Prevention Techniques". International Journal of Applied or Innovation in Engineering and Management Vol 2, 4 April 2013.*

[12]Gajendra Singh Chandel, Rajul Chowksi. "Effect of Rushing Attack in AODV and its Prevention Technique". International Journal of Computer Applications, Vol 83 No-16, December 2013.

[13]1Maha Abdelhaq, 2Rosilah Hassan, 3Mahamod Ismail, 4 Raed Alsaqour, 5Daud Israf. "Detecting Sleep Deprivation Attack over MANET Using a Danger Theory -Based Algorithm". International Journal on New Computer Architectures and Their Applications (IJNCAA), The Society of Digital Information and Wireless Communications, 2011.

[14]Adnan Nadeem, Michael Howarth. "Adaptive Intrusion Detection & Prevention of Denial of Service attacks in MANETs". Centre for Communication Systems Research University of Surrey, UK.

[15]Anurag Kumar1, Akshay Kumar2, Anubha Dhaka3 and Garima Chaudhary4. "Intrusion Detection Against Denial Of Service Attacks In Manet Environment". International Journal of Emerging Trends &Technology in Computer Science (IJETTCS) Volume 2, Issue 4, July - August 2013.

[16]Mukesh Kumar & Naresh Kumar. "DETECTION AND PREVENTION OF DDOS ATTACK IN MANET'S USING DISABLE IP BROADCAST TECHNIQUE". International Journal of Application or Innovation In Engineering & Management (IJAIEM) Volume 2, Issue 7, July 2013.

[17]S.B.Aneith kumar, S.Allwin Devaraj, J.Arunkumar. "Efficient Detection of Denial of Service Attacks in MANET". International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 5, May 2012.

[18] A. Nadeem and M. Howarth, "Adaptive Intrusion Detection & Prevention of Denial of Service Attacks in MANETs", Proc. ACM International Wireless Communication and Mobile Computing Conference (IWCMC 09), Leipzig, Germany, June 2009.

[19]M.Ghonge, P.M.Jawandhiya and M.S.Ali, "Countermeasures of Network Layer Attacks in MANETs", International Journal of Computer Appli- cations, Special Issue on Network Security and Cryptography, NSC, 2011.

[20] J.C. Kao and R. Marculescu, "Eavesdropping Minimization via Transmission, Power Control in Ad Hoc Wireless Networks", Proc. IEEE Sensors and Ad hoc Communication and Networks SECON, 2006.

[21] P. Uppuluri and R. Sekar, "Experiences with Specification-Based Intrusion Detection," Proc. Recent Advances in Intrusion Detection, (RAID), 2001.

[22]R. Sekar, A. Gupta, J. Frullo, T. Shanbhag, A. Tiwari, H. Yang, and S.Zhou, "Specification-Based Anomaly Detection: a New Approach for Detecting Network Intrusions", Proc. ACM Conference on Computer and Communications Security CCS '02, 2002.

[23] R. Sekar and P. Uppuluri, "Synthesizing Fast Intrusion Preven-tion/Detection Systems from High-Level Specifications", Proc. Usenix Security Symposium, 1999.

AUTHORS BIOGRAPHY

Parameswaran. T has received his B.E degree in Electronics and Communication Engineering from Vellalar College of Engineering and Technology, Erode, and M.E degree in Software Engineering from College of Engineering Guindy, Anna University Chennai in 2005 and 2008 respectively. He is currently pursuing his Ph.D. from Anna University, Regional Centre Coimbatore. He is currently working as Assistant Professor in the Department of Computer

Science and Engineering, Regional Centre, Anna University, Coimbatore, India. He has published more than 10 research papers in various journals and conferences. He has organized 3 national level workshops.

Dr. C. Palanisamy has received his B.E degree in Electronics and Communication Engineering from University of Madras, Chennai and M.E degree (Gold Medalist) in Communication Systems from Thiagarajar College of Engineering, Madurai, Madurai Kamaraj University in 1998 and 2000 respectively. He has received his Ph.D from the faculty of Information and Communication Engineering, Anna University, Chennai in 2009. He has more than 13 years of academic and research experience and currently he holds the post of Professor and Head of the Department of Information Technology, Bannari Amman Institute of technology, Sathyamangalam and Tamilnadu, India. He has published more than 30 research papers in various journals and conferences. He has organized more than 10 workshops and holds 2 funded projects. He is a lifetime member of ISTE. He won Best M.E thesis award at Thiagarajar College of Engineering, Madurai and best paper award titled, "A Neural Network Based Classification Model Using Fourier and Wavelet Features," Proceedings of the 2nd International Conference on Cognition and Recognition 2008, (ICCR 2008), Organized by P. E. S College of Engineering, Mandaya, Karnataka, India, pp. 664-670, 2008. His research interests include Data mining, image processing and mobile networks.

Rajasekar. G. M has received his B.E degree in Computer Science and Engineering from Dr. N.G.P. Institute of Technology, Coimbatore in 2008 to 2012. He is currently pursuing his M.E degree in Software Engineering from Anna University, Regional Centre Coimbatore. India. He has published 5 research papers in various international journals and conferences. He has organized 3 national level workshops.