Volume 2, Issue 5, May 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Efficient Detection of Denial of Service Attacks in MANET

S.B.Aneith Kumar
Lecturer
Department of ECE,
Sri Ramakrishna Institute of Technology, Coimbatore, India

S.Allwin Devaraj
Assistant Professor
Department of ECE,
Francis Xavier Engineering College
Tirunelveli, India

J. Arun kumar
Assistant Professor
Department of ECE,
PTR College of Engineering and Technology, Madurai, India

Abstract - Mobile Ad Hoc Networks (MANETs) are the set of mobile hosts operating without the aid of the established infrastructure of centralized administration. MANET is characterized by limited resources such as bandwidth, battery power, storage space and node mobility. The underlying assumption is that the intermediate nodes cooperate in forwarding packets. Due to lack of infrastructure, the network can be easily affected by several attacks. They are mostly vulnerable to the Denial of Service (DoS) attack because of its features. For this, we have developed the new algorithm called reputation based system. Here, each node would evaluate nodes recommendation, route ID and threshold packet dropping ratio. The proposed reputation system is evaluated with discrete event simulator environment. Simulation results shows that the reputation based system detects and isolates the DoS attack and provides better misbehavior detection efficiency, packet delivery ratio, and reduced packet dropping ratio, routing overhead, latency .

Keywords-MANET, Packet Delivery Ratio, Packet DroppingRatio, DoS attack, detection efficiency and overhead.

I. INTRODUCTION

In an ad hoc wireless network where wired infrastructures are not feasible, energy and bandwidth conservation are the two key elements presenting research challenges. Limited bandwidth and energy makes a network easily congested. The dynamic and cooperative nature of MANETs presents considerable challenges in offering secured services. The illustration of mobile ad hoc network is shown in figure.1

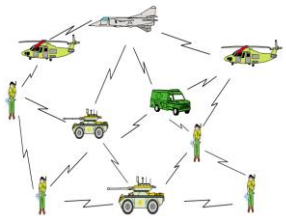

Fig.1. An example of Mobile Ad Hoc Network

In MANETs, a network is formed dynamically through the cooperation of an arbitrary set of independent nodes. There is no prearrangement regarding the specific role each node should assume. Instead, each node makes its decision independently, based on the network situation, without using a preexisting network infrastructure. Ad hoc networks have the characteristics such as dynamically changing topology, weak physical protection of nodes, the absence of centralized administration and high dependence on inherent node cooperation. When the topology keeps changing, these networks do not have a well defined boundary and thus network based access control mechanism such as firewalls are not directly applicable.

Securing wireless ad hoc networks is a highly challenging issue. There are certain specific attacks to which the ad hoc context is vulnerable. Performing communication in free space exposes ad hoc networks to eavesdrop or inject messages. Ad hoc network attacks can be classified into active and passive attacks. A passive attack does not inject any message, but listens to the channel. A passive attack tries to discover valuable information and does not produce any new traffic in the network. In the case of an active attack, messages are inserted into the network; such attacks involve actions such as replication, modification, and deletion of exchanged data. In ad hoc networks, active attacks are impersonation, Denial of Service (DOS) and disclosure attack.

DOS attacks can cause a severe degradation of network performance in terms of the achieved throughput and latency. The performance of the wireless network is degraded by DOS depends on many factors such as location of malicious nodes, their traffic pattern, fairness provided in the network resources. It attacks like routing table overflow and sleep deprivation fall.

The main aim of a DoS attack is the interruption of services by attempting to limit access to a machine or service instead of subverting the service itself. This kind of

attack aims at rendering a network incapable of providing normal service by targeting either the networks bandwidth or its connectivity. These attacks achieve their goal by sending at a victim a stream of packets that swamps his network or processing capacity denying access to his regular clients. In the not so distant past, there have been some large - scale attacks targeting high profile Internet sites. [1].

In MANET, uncooperative node is malicious node. The nodes belonging to the first category are either faulty and therefore cannot follow a protocol, or are intentionally malicious and try to attack the system. Malicious node causes packet dropping, false routing and etc. Effects of malicious nodes are given below:

- Malicious node reduces the network connectivity in MANETs.
- The result is defragmented networks, isolated nodes, and drastically reduced network performance.
- No intention for energy-saving.
- Launch all kinds of denial-of-service (DoS) attacks by replaying, reordering or/and dropping packets from time to time, and even by sending fake routing messages.

The nature of MANET makes it vulnerable to attacks. Challenges in MANET securities are discussed briefly [2];

- **Confidentiality:** should preserve certain information which is not to be opened to unauthorized parties.
- **Integrity:** The receiver should believe that the transmitted message is genuine and is never be corrupted.
- **Authentication:** Enables a node to defend the characteristics of the peer node it is communicating, without which an attacker would duplicate a node.
- **Access control** prevents unauthorized use of network services and system resources. Access control is tied to authentication attributes.
- **Availability:** should withstand survivability regardless of Denial-of-Service (DOS) attacks like in physical and media access control layer attacker uses jamming techniques for hinder with communication on physical channel.

The MANET can be applied in various applications such as:

• patient monitoring
• airplane exhaustion breakage supervision
• cyclone evolution analysis
• detection of earthquakes
• remote landscapes monitoring
• ecological danger detection
• providing security at public buildings

II. PREVIOUS WORK

In the ad hoc networks presently in operation, the nodes are required to watch their neighbors for misbehaviour and this not only necessitates promiscuous modes of operation but also overloads the nodes. Watchdog and path rater approach is proposed [3] to detect and isolate the misbehaving nodes. In this approach, a node forwarding a packet checks if the next hop also forwards it. If not, a failure count is incremented and the upstream node is rated to be malicious if the count exceeds a certain threshold. The path rater module then utilizes this knowledge to avoid it in path selection. It improves the throughput of the network in the presence of malicious nodes. However, it has the demerit of not penalizing the malicious nodes.

Buchegger and Boudec [4] suggest that despite the fact that networks only function properly if the participating nodes cooperate in routing and forwarding. However, it may be advantageous for individual nodes not to cooperate. They propose a protocol, called CONFIDANT, which aims at detecting and isolating misbehaving nodes, thus making misbehavior unattractive.Here misbehaving nodes are excluded from forwarding routes. It includes a trust manager to evaluate the level of trust of alert reports. But it is not clear how fast the trust level can be adjusted for compromised node especially if it has a high trust level initially[5].

Trust Evaluation method [6] provides an effective security mechanism based on data protection and secure routing. But it relies on global information and hence the reaction time is more. It would be preferable to reduce the reaction time.

Li Zhao et.al [7] have proposed MultipAth Routing Single path transmission (MARS) scheme to mitigate adverse effects of misbehavior. This scheme combines multipath routing and single path data transmission with end-to-end feedback mechanism to provide more comprehensive protection against misbehavior from individual or cooperating misbehaving nodes.

In the Reputation scheme [8], the reputation of the nodes is assessed based on their past history of relaying packets, and are used by their neighbors to ensure that the packet will be relayed by the node. Instead of choosing the shortest path to the destination, the source node chooses a path whose next hop node has the highest reputation. As a result, the good nodes (nodes with higher reputations) become overloaded. Once the load on the good nodes is more than what the resources can manage , they start dropping packets and start loosing reputation. As a result, their incoming traffic is reduced to a level at which they can forward all the packets they receive for relaying. Also the number of route discoveries is more with increase in the average hop length.

Tarag Fahad and Robert Askwith [9] have proposed the new mechanism called Packet Conservation Monitoring Algorithm (PCMA) to detect selfish nodes in the presence of partial dropping when the selfish node does not drop all packets but sends some of them and drops other in MANET.

Much of research on security policies focuses on policy representation and evaluation [10], [11] or building

security mechanisms based on specific policies [12] without addressing policy enforcement.

K. Sanzgiri et al [13] proposed the Authenticated Routing for Ad-hoc Networks (ARAN) secure routing protocol is an on-demand routing protocol which relies on the use of digital certificates to identifies and defends against malicious actions in the ad-hoc network.

Zapata and Asokan [14] proposed the Secure Ad-hoc On-Demand Distance Vector routing protocol. Through providing security features like integrity, authentication and non-repudiation, it effectively protects the route discovery mechanism. This scheme is based on the assumption that each node should have certified public keys of all nodes in ad hoc network.

Michiardi and Molva [15] have proposed CORE mechanism that enhances watchdog for monitoring and isolating selfish nodes based on a subjective, indirect and functional reputation. The reputation is calculated based on various types of information on each entity's rate of collaboration. Since there is no incentive for a node to maliciously spread negative information about other nodes, simple denial of service attacks using the collaboration technique itself are prevented.

Our aim in this paper is to arrive at a simple protocol which strikes a balance between defending against DoS attacks and energy consumption.

III. OVERVIEW OF THE PROPOSED SCHEME

We propose a Reputation Based System (RBS) in MANETs without using any centralized infrastructure. It uses trust table to favor packet forwarding by maintaining a trust vector for each node. Each intermediate node marks the packets by adding its recommendation about the neighborhood node, Packet Dropping Ratio (PDR) and route ID towards the destination node. The destination node verifies the recommendation about nodes experience and knowledge. Once the destination node's verification is completed, the checks the number of packets received at the destination. Thus the node recommendation, PDR and route id are verified. If the nodes packet dropping ratio value falls below a trust PDR threshold value, the corresponding the intermediate node is marked as malicious node which is caused by means of DoS attack.

IV. REPUTATION BASED SYSTEM

A. Reputation Based System (RBS)

In the proposed system, we have focussed on reducing the effects of Denial of Service (DoS) attack. For that, we have developed one misbehavior table list and also the packet format. This packet format is totally 8 bytes which contains source and destiantion address, Sequence number, Hop Count, Cyclic Redundancy Check (CRC) and Route ID. The proposed misbehavior table list which is used to identify the malicious node. When the malicious node is detected, it will be automatically entered in the table list. While comparing with the existing results, the proposed system achieves high perfomrance interms of misdetection efficiency, latency and packet delivery ratio.

B. Stimulating Reputation Based System to defend against DoS attacks

The proposed system mainly focused on reducing the effects of DoS attacks. So the system is developed to reduce malicious nodes and selfish nodes in the network environment.

The proposed packet format is shown in figure.2

Source ID 1	Destination ID 1	Route ID 1	Sequence Number 2	Data (0-25) bytes	MAC 4 bytes	CRC 1

Fig.2. Proposed packet format

In MANET, different routing protocols use different metrics to forward the data packets from the source to the destination. The metrics are delay, link-quality, path-length, link stability, location-stability, and power.

The proposed packet format contains the fields like source and destination nodes id, Route id which is used for identifying the particular intended route, sequence number is stored in all packets which is for identification purpose, Data occupies 25 bytes which is defined by the source, Message Authentication Code (MAC) is for authentication in order to avoid malicious activities, finally CRC (Cyclic Redundancy Check) is used for error detection and correction which occupies 1 bytes.

The proposed system consists of following steps;

Step1:

Source node sends the packet to the destination node via intermediate nodes.

Step 2:

Once the intermediate node receives the packet, first it will check the route id and source id and sequence number. If the route id is not valid, then it will drop the packet.

Step 3:

Intermediate nodes also verify the packet dropping ratio which will be stored in the misbehavior list table.

The Packet Dropping Ratio is calculated by,

$$\frac{No.ofPacketsDropped}{No.ofPacketsSent} x100$$

Here, we have set the threshold dropping ratio t_{pdr}. If any packet dropping ratio is greater than the t_{pdr}, the whole route will be considered as invalid, otherwise valid.

Nodes recommendation is also used to identify the malicious behaviors. Evaluating the recommendation is given by R_B^A which is node A's evaluation to node B by collecting recommendations,

$$R_B^A = \frac{\sum_{\upsilon \in \gamma} V|A \to C| * V|C \to B|}{V|A \to C|}$$

γ is a group of recommenders.

$V|A \rightarrow C|$ is trust vector of node A to C.

$V|C \rightarrow B|$ is trust vector of node C to B.

Invalid route ID, false node recommendation about neighborhood node and more packets dropping that indicates the presence of malicious node.

Once the presence has been identified, it will be isolated automatically by means of misbehavior detection list table.Thus the node is injected by means of DoS attack.

Step 4:

Once all the fields are verified, the intermediate node sends the Route Reply (RREP) packets to source, or any problem occurs, it will send the Route Error (RERR) packet.

Step 5:

Finally the destination node will check the no. of packets received. Thus the behavior of DoS attack can be successfully detected by means of proposed RBS system. Another scheme has also been proposed which is used to reduce the energy consumption of the node.

V.INTEGRATING RBS SCHEME IN TO DSR PROTOCOL

Trust vector is evaluated based on the how many out-coming packets can be measured that the immediate neighboring node had been sincerely sent. Participation of the nodes in the packet forwarding is monitored. So nodes are placed in the immoral mode all the time whether a node transmits control packets or data packets. When it eavesdrops its immediate neighbor nodes forwarding the packet, it should first check the integrity of the packet in order to make sure the packet had not been modified by other malicious nodes. Neighbor node should be incremented if it passes integrity test. However if the integrity test fails or the neighbor node refuse to cooperate to forward packets it supposed to, its corresponding forwarding counter would not change. After a period of time, its experience value would be extremely low as a result of malevolent behavior. The reputation based system is integrated in to DSR routing protocol.

VI. ENERGY CONSUMPTION REDUCTION USING TOPOLOGY CONTROL APPROACH

In MANETs, the topology is dynamic not static. Due to the dynamic topology, node consumes more energy while roaming. For this, the topology control approach has been introduced. In this approach, we have considered two cases,

i) Energy consumption of the node and routes.
ii) Link stability and location stability.

Case i)

In first case, the dynamic and adaptive topology is proposed. It will adopt, according to the node moves with in the network. For this each node will keep on nearest level with in the cluster. The number of links connected to a node is very kept low. The link with the low transmission power is also taken in to the consideration for the energy consumption of the route.

Case ii)

For link stability and location stability, each node carrying link with highest density and efficient transmission power with adaptable location. The location stability which implies node is on the stable state which is ready state to send the number of packets to the intended destination node with degrading the network performance.While implementing these two cases, the energy consumption of the whole network can be effectively reduced.

VII. PERFORMANCE EVALUATION

A.Simulation Model and Parameters

The Proposed scheme is implemented with the object oriented discrete event simulator. In our simulation, 101 mobile nodes move in a 1000 meter x 1000 meter square region for 50 seconds simulation time. We assume each node moves independently with the same average speed. All nodes have the same transmission range of 100 meters. The simulated traffic is Constant Bit Rate (CBR). Our simulation settings and parameters are summarized in table 1

No. of Nodes	100
Area Size	1000 X 1000
Mac	802.11
Radio Range	100m
Simulation Time	50 sec
Traffic Source	CBR
Packet Size	80 bytes
Mobility Model	Random Way Point

B. Performance Metrics

We evaluate mainly the performance according to the following metrics.

Detection Efficiency: The ratio of detected malicious nodes to the total number of nodes.

Latency: The latency is averaged over all surviving data packets from the sources to the destinations.

Average Packet Delivery Ratio: It is the ratio of the number .of packets received successfully and the total number of packets transmitted.

Routing Overhead: The control overhead is defined as the total number of routing control packets normalized by the total
number of received data packets.

Packet Dropping Ratio: The number of packets dropped to the number of packets sent in the network. In general, the PDR level should be kept minimum.

The simulation results are presented in the next part. We compare our RBS scheme with the existing technique Mobiltiy Oriented Reputation System (MORS) and CONFIDANT (Cooperative of Nodes Fairness in Dynamic Ad hoc NeTwork) Scheme in presence of malicious node environment.

C. Results

Nodes actual behaviors comply with the Bernoulli trial, which means that the probability that a node acts good is

predetermined. If a node acts well for less than 40 percent of the interactions, it is considered as a malicious node. The default percentage of malicious node in the network is 20 percent. In our First experiment, we vary the speed as 20, 30 up to 100.

Figure 3 show the results of detection efficiency for the 20, speed. Clearly our RBS scheme achieves more detection rate than the MORS scheme and CONFIDANT model.

Figure 4 shows the results of No.of Nodes Vs overhead. From the results, we can see that RBS scheme achieves low overhead than the MORS scheme and CONFIDANT model.

In our Second experiment, we vary the THROUGHPUT and No.of nodes as 20, 40,60. 80,100.

Figure 5 show the results of packet delivery ratio for the throughput. Clearly our RBS achieves more packet delivery ratio than the MORS scheme and CONFIDANT model.

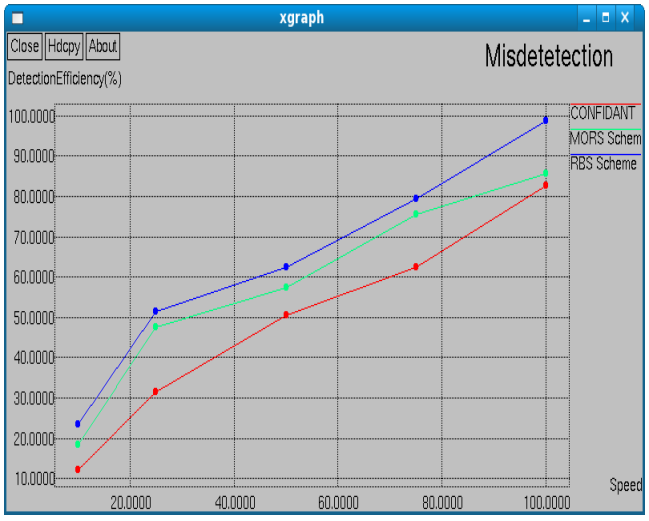

Figure 3. Misdetection Efficiency

Figure 4. No.of Nodes Vs Overhead

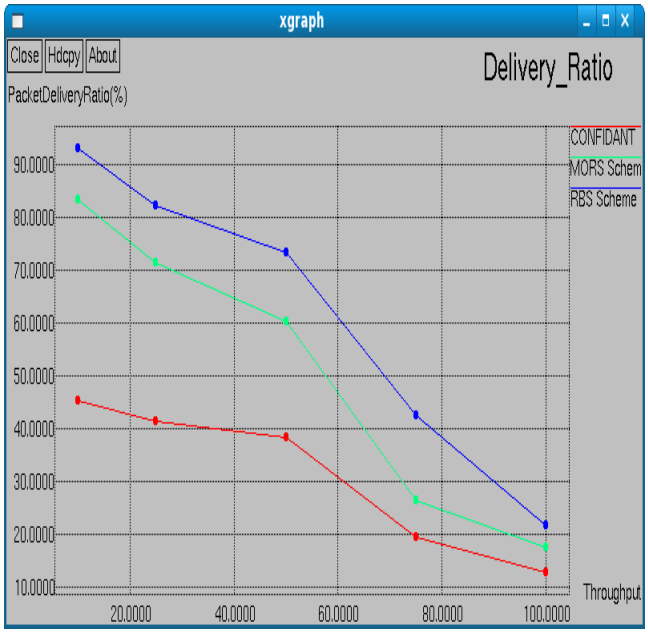

Figure 5.Throughput Vs Packet Delivery Ratio

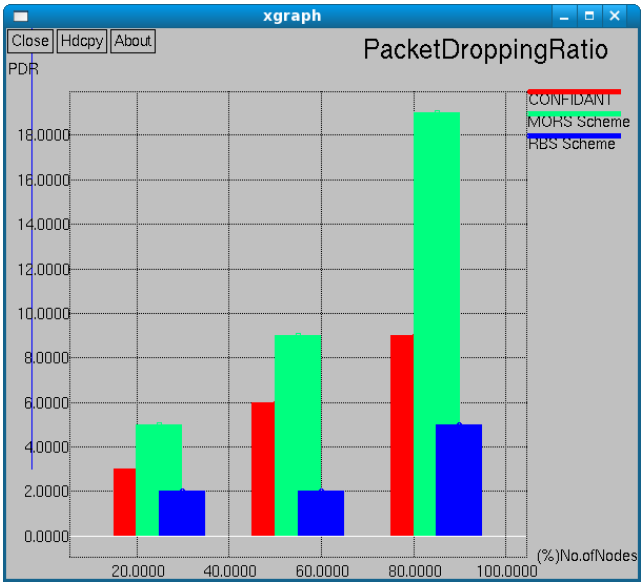

Figure 6.No.of Nodes Vs Packet Dropping Ratio

Figure 6 shows the results of No. of nodes Vs Packet Dropping Ratio. From the results, we can see that RBS scheme has fewer packets dropping ratio than the MORS scheme and CONFIDANT model.

VII.CONCLUSION

It is easy to deploy DoS attack to impersonate another node in MANET. Mobile ad hoc network has no clear line of defense, so, it is accessible to both legitimate network users and malicious nodes. In this paper, we have developed a reputation based system which attains authentication and reduce energy consumption to the mobile nodes. In the first phase of the scheme, detection of the DoS attack is

achieved. It uses trust table to favor packet forwarding by maintaining a packet dropping ratio and route id for each node.Thus the node recommendation, PDR and route ID are verified. If the nodes packet dropping ratio value falls below a trust PDR threshold value, the corresponding the intermediate node is marked as malicious node which is caused by means of DoS attack. For reducing the energy consumption of whole network, we focused on two cases i.e., energy consumption of the nodes and routes, link and location stability. By simulation results, we have shown that the Reputation Based System achieves better misdetection efficiency, good packet delivery ratio while attaining low latency, routing overhead, false positive and energy consumption.

REFERENCES

[1]. Douligeris and A. Mitrokotsa 2004. DDoS attacks and defense mechanisms: classification and state-of-the-art. In Comput. Netw. 44, 5 (Apr. 2004), 643-666.DOI=http://dx.doi.org/10.1016/j.comnet.2003.10.003.

[2]. P Narayan, V R. Syrotiuk,"Evaluation of the AODV and DSR Routing Protocols Using the MERIT Tool", In In proceeding or ADHOC-NOW 2004, pp. 25-36.

[3]. S.Marti,T.J.Giulli,K.Lai and M.Baker mitigating routing misbehavior in mobile adhoc network Mobile computing and networking,2000,pp. 255-265

[4]. S. Buchegger and J. Boudec, "Performance Analysis of the Confidant Protocol," Proc. Int'l Symp, Mobile Ad Hoc Networking and Computing, 2002.

[5]. Y.Huang and W.Lee A cooperative IDS for adhoc network Security of adhoc and sensor networks ACM 2003,pp.135-145

[6]. Li Zhao and José G. Delgado-Frias, "MARS: Misbehavior Detection in Ad Hoc Networks", in Proceedings of IEEE GLOBECOM 2007,pp. 941-945.

[7]. Zheng Yan and peng Zhang, "Trust Evalution based security solution in Adhoc network", pp 1-14.

[8]. Prashant Dewan, Partha Dasgupta,Amiya Bhattacharya On using Reputation in Adhoc network to counter malicious nodes Proceeding of Parallel and distributed system, 10th International Conference on (ICPAD'S 04), July2004, pp 665 – 672.

[9]. Tarag Fahad and Robert Askwith "A Node Misbehaviour Detection Mechanism for Mobile Ad-hoc Networks", in proceedings of the 7th Annual Post Graduate Symposium on The Convergence of Telecommunications, Networking and Broadcasting, June 2006.

[10]. M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized Trust Management," Proc. IEEE Conf. Privacy and Security, pp. 164-173, 1996.

[11]. M. Blaze, J. Feigenbaum, J. Ioannidis, and A.D. Keromytis, "The Keynote Trust-Management System, Version 2," RFC 2704, Sept. 1999.

[12]. P. Dinsmore, D. Balenson, M. Heyman, P. Kruus, C. Scace, nd A.Sherman, "Policy-Based Security Management for Large Dynamic Groups: An Overview of the dccm Project," Proc. DARPA Information Survivability Conf. and Exposition (DISCEX '00), pp. 64-73, Jan. 2000.

[13]. K. Sanzgiri et al., "A Secure Routing Protocol for Ad Hoc Networks," Proc. 10th IEEE Int'l Conf. Network Protocols (ICNP '02), IEEE Press, 2002, pp. 78–87.

[14]. M. Guerrero Zapata and N. Asokan, "Securing Ad Hoc Routing Protocols," Proc. ACM Workshop on Wireless Security (WiSe), ACM Press, 2002, pp. 1–10.

[15]. P. Michiardi and R. Molva, "CORE: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks," Proc. IFIP TC6/TC11 Sixth Joint Working Conf. Comm.and Multimedia Security, 2002.

AUTHORS PROFILE

S.B. Aneith Kumar received the **B.E.** degree in electronics and communication engineering from the Karpagam College of Engineering, Coimbatore, Anna University, Chennai, India, in 2009. He earned **M.E.** in electronics and communication engineering (Communication Systems) in Anna University of technology, Coimbatore, India, 2011. His research interest includes wireless communication (**WiFi,WiMax**), Mobile Ad hoc networks ,Sensor Networks, Communication networks.

S.Allwin Devaraj received the **B.E.** degree in electronics and communication engineering from Karunya University, 2009. He earned the **M.E.** year in electronics and communication engineering (Communication Systems) in Anna

University of technology, Coimbatore, India, 2011. His research interest includes MANET, Wireless Communication, Sensor networks, Digital Image Processing.

J.Arun kumar received the **B.E.** degree in electronics and communication engineering in Raja College of Engineering and Technology, Madurai, Anna University, Chennai, 2008. He earned the **M.E.** year in electronics and communication engineering (Communication Systems) in Anna University of technology, Coimbatore, India, 2011. His research interest includes MANET, Networking, Principles of Communication, Information Theory and Coding and Mobile Communication.

