International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Intrusion Detection Techniques in MANET: A Review

Navneet Dhillon[1], Amardeep Singh[2]

[1]Department of Computer Engineering, Master of Engineering, UCOE, Punjabi University Patiala

[2]Professor, Department of Computer Engineering, UCOE, Punjabi University Patiala

Abstract: ***In today's world, wireless communication has rapid enhancement as demand for wireless network goes on increasing. It is one of the most popular and growing network i.e. Mobile AdHoc Network as no of mobile users are incremented day by day. Mobile AdHoc Network (MANET) is infrastructure-less network i.e. It doesn't require any central (base) station, so it is applicable in various fields for communications such as rescue operations and in critical situations like battlefields .To secure such demanding network is itself a big challenge. Due to some unique characteristics of MANETs like lack of infrastructure and central authority, node mobility and change of dynamic topology, prevention methods alone are not sufficient to make them secure therefore, detection should be added as another defence line before the system could be penetrated. To secure network we have to detect the attacks and take appropriate action on it. This paper reviews the performances of various detection techniques used to detect the malicious/selfish node in the network.***

Keywords: MANET, IDS, TWOACK, EAACK.

1. Introduction

Mobile Ad hoc Network is a collection of wireless mobile nodes where each node acts as both transmitter as well as receiver i.e. each node acts as router in itself, communicating with other nodes in its communication radio range as shown in the Figure1.For a node to forward a packet to a node that is out of its radio range, the cooperative behavior is needed by other nodes in the network is needed which is known as multi- hop communication. Therefore, each node must act as both a host and a router at the same time. The network topology keeps on changing frequently due to the mobility of nodes as they move in and out of the network.

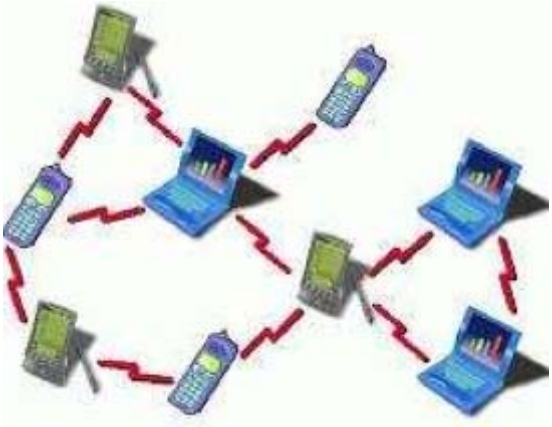


Figure 1: Mobile Ad-hoc Network

As MANETs become widely used, the security issue has become one of the primary concerns. For example, most of the routing protocols proposed for MANETs assume that every node in the network is cooperative and not malicious [1]. Therefore, only one compromised node can cause the failure of the entire network.

A selfish node is one that tries to utilize the network resources for its own profit but is avoid to spend its own for others. If such behaviour persists among large number of the nodes in the network, it may eventually lead to obstruction of network; this minimizes the efficiency of packet transfer and maximizes the packet delivery time and packet loss rate that causes the partition of network. This paper reviews the various techniques which can be used for detection of Selfish/malicious node and their comparative analysis [10].

There are both passive and active attacks in MANET. In passive attacks, packets containing secret information might be eavesdropped, which violates confidentiality. Active attacks, including injecting packets to invalid destinations into the network, removing the packets, changing the contents of packets violate availability of resources, network integrity, authentication, and non-repudiation. Proactive approaches such as cryptography and authentication [6] were first brought into consideration, and many techniques have been proposed and implemented. As these applications are not sufficient so Intrusion Detection system is introduced to detect new attacks in the network. It is a process of monitoring activities in a system. An IDS collects activity information and then analyses it to determine whether there are any activities that violate the security rules or any activity which deviates from the normal behaviour of network system. Once an IDS determines that an unusual activity occurs, it then generates an alarm to alert the security administrator. In addition, IDS can also initiate a proper response about the malicious activity.

2. Background

2.1 Routing Protocols in MANET

Dynamic source Routing Protocol (DSR): It is on demand routing protocol which uses source routing to deliver packets through MANET i.e. the sender of a data packet finds a source route and includes it in the packet header [2].The protocol operates on two mechanisms: route discovery and route maintenance. Route discovery: It is used when the packet sender is yet not clear with the correct path to the packet destination. It then broadcast a ROUTE REQUEST

message throughout the network in a controlled manner until it is answered by a ROUTE REPLY message from either the destination itself or an intermediate node that knows a valid path to it. Route maintenance: Finally, route maintenance mechanism is used to notify source and trigger new route discovery events when changes in the network topology does not validate the cached route.

AdHoc on-Demand Distance Vector Routing Protocol (AODV): Ad-hoc on Demand Distance Vector Routing (AODV) is an improvement of Destination sequenced distance vector routing (DSDV) as it reduces the number of required broadcasts since it creates routes in an on- demand basis, in contrast to Destination Sequenced Distance Vector routing (DSDV) which maintains a complete set of routes Ad hoc On- demand Distance Vector Routing Protocol uses an on demand approach for finding routes, that is, a route is established only when it is required by a source node for transmitting data packets. It uses sequence numbers for the destination to identify the most recent path [4,13].

2.2 Vulnerabilities of the Mobile Ad Hoc Networks

The mobile ad hoc network is insecure by its nature: as nodes can move freely in the network,there is no such a clear line of defense . some of the nodes may be compromised by the adversary and thus perform some malicious behaviors that are hard to detect; lack of centralized machinery may cause some problems when there is a need to have such a centralized coordinator; restricted power supply can cause some nodes to behave in selfish manner and continuously changing area of the network has set higher requirement to the scalability of the protocols and services in the mobile ad hoc network. As a result, as compared to the wired network, the mobile ad hoc network will require more robust security scheme to ensure the security of it [5, 18].

2.3 Attack Types in Mobile Ad Hoc Networks

There are two types of attacks occur in system called Passive and Active Attacks. In a passive attack an unauthorized node monitors and aims to find out information about the network. The attackers do not need to communicate with the network. Hence they do not interrupt communications or cause any direct damage to the network [6, 8].However, they use the that information for future harmful attacks.

Eavesdropping Attacks: These are passive attacks also called disclosure attacks, by external or internal nodes. The attacker can analyze broadcast messages to find out some useful information about the network [14]. Traffic Analysis Attack: Traffic analysis is about monitoring the traffic flow between the nodes by the malicious node which may reveal:
1. Location of nodes.
2. The communications network topology.
3. The current sources and destination in network.
4. The current location of specific individuals .

An active Attacks cause the unauthorized state changes in the network. This includes the following attacks:

Dropping Attack: Malicious node drops the packet intentionally instead of forwarding to desired destination or intermediate node. It may cause the retransmission of data packets which reduces the network performance , new routes need to discovered to the destination.

Distributed Denial of Service: A DDoS attack is a form of DoS attack but difference is that DDoS is performed by the combination of many nodes instead by only one node. All nodes simultaneously attack on the victim node(s) by sending them huge packets,which totally consume the victim bandwidth and this will not allow victim to receive the important data from the network.

Modification Attack: Insider attackers modify packets to disrupt the network. For example, in the sinkhole attack the attacker tries to attract nearly all traffic from a particular area through a compromised node by making the compromised node attractive to other nodes.

Fabrication Attacks: In this attack, the attacker forges a Route Reply message after receiving a Route Request message. The reply message contains false routing information showing that the node has a fresh route to the destination node in order to overcome the real routes to the destination. It causes route disruption by causing messages to be sent to a wrong node or putting the attacker itself into the route between two endpoints of a channel.

Rushing Attack: If the RREQs for a discovery forwarded by the attacker are the first to reach each neighbor of the target node, then any route discovered by this route discovery will include a hop through the attacker. An attacker that can forward RREQs more quickly than desired nodes can do so, which may increase the probability of the routes that include the attacker rather than other valid routes.

Masquerade: It is an intruder who acts as an authenticate user and gain the privilege of any one system by stolen user password, through finding security gaps in programs, or through bypassing the authentication mechanism [15].

3. Intrusion Detection Systems

As the system become more complex, there are also more security concerns attached to it. Intrusion detection can be used as a second wall of defense to protect the network from such problems after prevention techniques. If the intrusion is detected, a response can be initiated to prevent damage to the system. Intrusion detection can be classified based on audit data as either host- based or network-based. A network-based IDS captures and analyses packets from network traffic while a host-based IDS uses operating system or application logs in its analysis. Based on detection techniques, IDS can be classified into three categories [2, 4].

3.1 Classification of IDs

Anomaly Detection Systems: The normal profiles (behaviour) of users are kept in the system. The system compares the collected data with these stored profiles, and then checks for any activity that deviates from the baseline as a possible intrusion by informing system administrators or initializing a proper response. Misuse Detection Systems: The system keeps patterns (or signatures) of known attacks and uses them to compare with the collected data. Any matched pattern is treated as an intrusion. It is unable to detect new kinds of attacks. Specification-based Detection:

The system defines a set of constraints that describe the normal operation of a program or protocol. So, it monitors the execution of the program in comparison to the defined constraints.

3.2 Architectures for IDs In MANETs

Intrusion Detection System: An Intrusion Detection system is run on each node individually to determine any intrusion. Every decision made is based only on information collected at its own node, as there is no cooperation among nodes in the network. Therefore, no data is exchanged. Besides, nodes in the same network do not know anything about the situation on other nodes in the network so no alert information is passed. This architecture is more suitable for flat network infrastructure than for the multi-layered network infrastructure [12].

Distributed and Cooperative Intrusion Detection System: Every node participates in intrusion detection and response by using their individual IDS agent running on them. An IDS agent is responsible for detecting and collecting local activities and data to identify any possible intrusion, as well as initiating a response independently, if needed. However, neighbouring IDS agents can cooperatively participate in intrusion detection actions at global level when the evidence is inconclusive. This architecture is also more appropriate for flat network infrastructure than multi-layered.

Hierarchical Intrusion Detection System: Here the network is divided into clusters. Cluster- heads of each cluster performs more than one functionality than other members in the clusters, for example transferring packets between the clusters. Thus, these cluster-heads act as control points which resembles to the switches, routers, or gateways in wired networks. Each IDS agent runs on every member node and is responsible locally for its node, i.e. Monitoring the locally detected intrusions. A cluster head is responsible both for local as well as global detection for its cluster, e.g. monitoring network packets and participating in a global response when network intrusion is detected[1,17].

4. Intrusion Detection Techniques for Node Cooperation in MANETs

Since there is no infrastructure in mobile ad hoc networks, each node rely on other nodes for cooperative behavior in routing and forwarding packets to the destination. Intermediate nodes might agree to forward the packets during route discovery process but actually drop or modify them as they become selfish to preserve their resources. It is observed that only a few misbehaving nodes can degrade the performance of the entire system. Several techniques and protocols are proposed to detect such misbehavior in order to avoid these misbehaving nodes [6, 7, 16].

4.1 Watchdog Scheme

Watchdog serves as an intrusion detection system for MANETs. It detects malicious nodes misbehavior in the network. Watchdog detects malicious misbehavior by promiscuously listens to its next hop's transmission. If Watchdog node overhears that its next node fails to forward the packet for the particular duration of time , it increases its failure counter [1]. Whenever a node's failure counter exceeds a predefined fixed threshold, the Watchdog node reports that node as misbehaving. In this case, the Pathrater informs the routing protocols to avoid the reported nodes in future route making decisions. Watchdog scheme is proven to be an efficient technique. Furthermore, compared to some other schemes, Watchdog detects malicious nodes rather than malicious links. These advantages have made Watchdog scheme a popular choice in the field. Many MANET IDS are developed as an improvement to the Watchdog scheme. Watchdog improves throughput of network in the presence of malicious nodes. As shown in the figure 3, suppose there exists a path from node S to D through intermediate nodes A, B and C.Node A cannot transmit directly to node C, but it can listen to node B's traffic. So, when A transmits a packet for B to forward to C, A can check if B transmits the packet. Watchdog's weaknesses are that it might not detect a misbehaving node in the presence of collisions at receiver side, limited transmission power and false misbehavior [3].

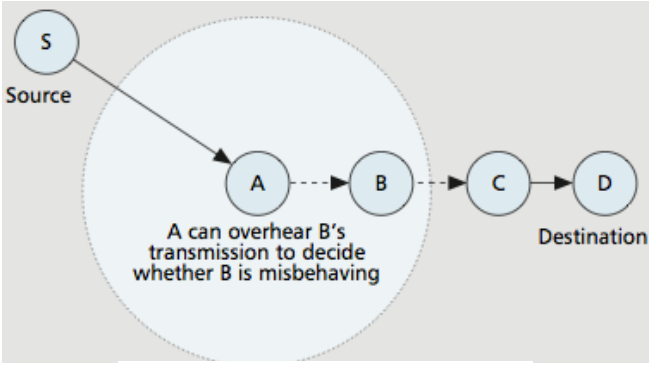


Figure 3: Watchdog-Pathrater Scheme

4.2 TWOACK Scheme

Aiming to resolve the receiver collision and limited transmission power problems of Watchdog, TWOACK detects misbehaving links by acknowledging every data packets transmitted over each three consecutive nodes along the path from the source to the destination. Upon retrieval of a packet, each node send back an acknowledgement packet to the node that is two hops away from it in the opposite direction of the route. TWOACK works well on routing protocols such as Dynamic Source Routing (DSR).

The working process of TWOACK is demonstrated in Figure 4. Node A first forwards packet1 to node B, and then node B forwards Packet1 to node C. When node C receives Packet1, as it is two hops away from node A, node C is required to generate a TWOACK packet, which contains reverse route from node A to node C,and sends it back to node A. The retrieval of this TWOACK packet at node A indicates the transmission of Packet1 from node A to node C is successful. Otherwise, if this TWOACK packet is not received in a predefined time period, both nodes B and C are reported malicious. TWOACK scheme successfully solves the receiver collision and limited transmission power problems which are present in Watchdog. However, the acknowledgement process required in every packet transmission process added a significant amount of unwanted network overhead. Due to the limited battery power of nodes of MANETs, such a repetitive transmission process can easily degrade the life span of the entire network.

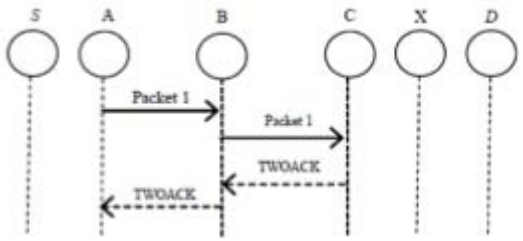


Figure 4: TWOACK Scheme

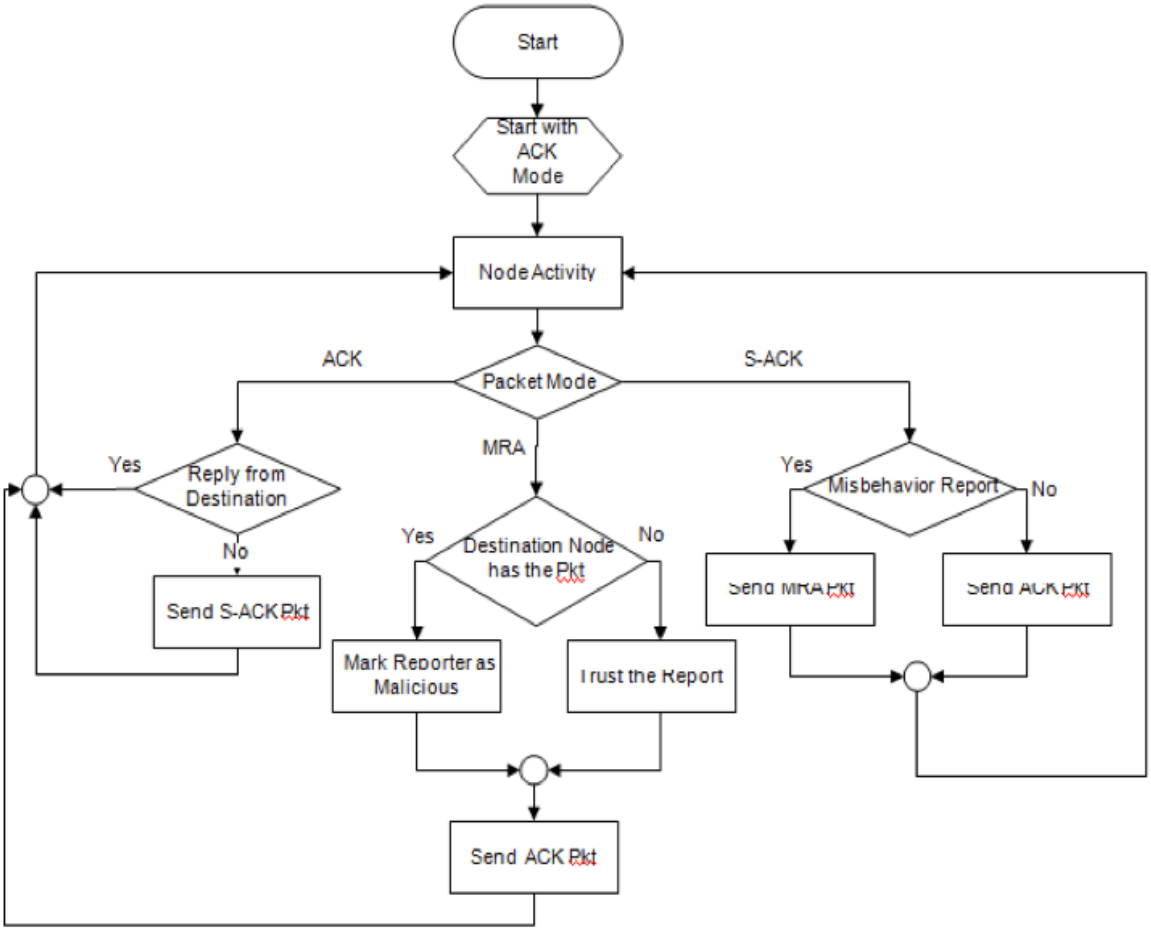
4.3 Enhanced Adaptive Acknowledgement (EAACK) Scheme

It consists of three major parts, namely: Acknowledge (ACK), Secure-Acknowledge (S- ACK) and Misbehavior Report Authentication (MRA).EAACK is designed to handle three of the six weaknesses of Watchdog scheme, which are false misbehavior, limited transmission power and receiver collision.

ACK: It is basically an end-to-end acknowledgement scheme. In ACK mode, node S first sends an ACK data packet ad1 to the destination node D. If all of the intermediate nodes along the route between node S and node D show cooperative behavior and node D successfully receives ad1 , node D is required to send back an ACK acknowledgement packet ak1 along the same route but in a reverse order. Within a predefined duration of time, if node S receives ak1, then the packet transmission from node S to node D is successful. Otherwise, node S will switch to S-ACK mode by sending an S- ACK data packet to detect the misbehaving nodes in the route.

S-ACK:This scheme is an improved version of TWOACK scheme. It follows the same criteria of TWOACK, but the difference lies in the fact that unlike TWOACK scheme, where the source node immediately trusts the misbehavior report, EAACK requires the source node to go for MRA mode and confirm this misbehavior report. This is a important step to detect false misbehavior report in our proposed. The whole activity of EEACK can be viewed in figure 5.

MRA: The Misbehavior Report Authentication (MRA) scheme is designed to remove the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehavior report. This False misbehavior report can be generated by malicious attackers to falsely report that innocent nodes as malicious. To initiate MRA mode, the source node first searches its local knowledge base and seeks for alternative route to the destination node. If there is no other path exists, the source node initialize a DSR routing request to find another route. In case of MANETs, it is common to find out multiple routes between two nodes. By adopting an alternative route to the destination node, we find out the misbehavior reporter node. When the destination node receives an MRA packet, it searches its local knowledge base and compare if the reported packet was received. If it is already received, then it is safe to conclude that this is a false misbehavior report and who generated this report is marked as malicious. Otherwise, the misbehavior report is trusted and accepted. By the adoption of MRA scheme, EAACK helps in detecting malicious nodes despite the existence of false misbehavior report.



5. Performance Evaluation

For comparison of performances through simulation among Watchdog, TWOACK and EAACK schemes following performance metrics are used.

Simulation Methodology: In this simulation scenario, we will consider a basic packet dropping attack. Malicious nodes drop all the packets they receive,which will effect the network performance.
Simulation Configurations: Simulation is conducted within the Network Simulator (NS) 2.35 environment on a platform with Ubuntu v12.Various parameters are set in order to create a MANET with required no. of nodes having specific node speeds and traffic. In order to measure and compare the performance of different schemes, the following two performance metrics are considered [13].

Packet Delivery Ratio (PDR): PDR is the ratio of the number of packets received by the destination node and the number of packets sent by the source node.

Routing Overhead (RO): RO defines the ratio of the amount of routing-related transmissions. (RREQ, RREP, RERR, ACK, S-ACK and MRA)

Throughput: Ratio of number of packets sent by the source or an intermediate node to the total time taken. Evaluation results will show that Watchdog Pathrater is the simplest technique which can be used to detect the malicious node whereas TWOACK detects the misbehaving links.TWOACK approach adds on the extra overhead to the network by making use of ACK packets, which lowers the limited battery power of the mobile nodes. All of the above EEACK approach overcomes all the weaknesses of Watchdog-Pathrater and TWOACK in the case of limited transmission power, collision at receiver side and false misbehavior report.

Table1: Overall Performance Comparison among Intrusion Detection Techniques.

Parameters Techniques	*Performance*	*Receiver Collision*	*Transmission Power*	*False Misbehaviour Report*
Watchdog Parameter	Good in finding misbehaviour Node	Unable to detect	Unable to detect	Unable to detect
TWOACK	Good in finding Misbehaving Link	Can detect	Unable	Unable
EAACK	Better in finding misbehaving link and node	Can detect	Can detect	Can detect

6. Conclusion

In this paper, an introduction to mobile ad hoc networks is provided along with its various vunerabilities. We firstly survey various attacks and problems Different types of attacks called Active and Passive are discussed. After that a survey is conducted regarding intrusion detection techniques which can find out misbehaving links in reliable manner like Watchdog-Pathrater, TWOACK and EAACK and their performance analysis in context of MANETs. Intrusion detection systems can effectively identify malicious activities and help to offer adequate protection. Therefore, an IDS has become an unavoidable and important component to provide defense-in-depth security mechanisms for MANETs.

References

[1] U. Sharmila Begam, Dr. G. Murugaboopathi "A Recent Secure Intrusion Detection System For Manets" International Journal of Emerging Technology and Advanced Engineering Vol 3, Special Issue 1, January 2013.
[2] D. Johnson and D. Maltz. "Dynamic Source Routing in Ad hoc Wireless Networks" Mobile Computing, Kluwer Academic Publishers, Chapter 5, pp. 153-181, 1996.
[3] N. Kang, E. Shakshuki and T. Sheltami. "Detecting Misbehaving Nodes in MANETs" The 12th International Conference on Information Integration and Web-based Applications & Services iiWAS2010, ACM, pp. 216-222, November, 8-10, Paris, France, 2010.
[4] Mugdha Kirkire, Poonam Gupta"Intrusion Detection in Mobile Ad-hoc Network "International Journal of Computer Science and Mobile Computing, Vol.3 Issue.2, pp. 869-876 ,February- 2014.
[5] Yang.H Luo, Zhang, L "Security in Mobile ad hoc networks: challenges and solutions" IEEE Wireless Communications, January 2004.
[6] Djamel DJENOURI, Nadjib BADACHE "A Survey on Security Issues in Mobile Ad hoc Networks" February 2004
[7] Renu Dalal,Yudhvir Singh and Manju Khari "A Review on Key Management Schemes in MANET" international journal of Distributed and Parallel Systems Vol.3,No.4,July 2012.
[8] Sevil Sen, John A.Clark, Juan Tapiador "Security Threats in Mobile Ad hoc networks"
[9] Marco Conti, Body, Personal and Local Ad Hoc Wireless Networks, in Book The Handbook of Ad Hoc Wireless Networks (Chapter 1), CRC Press LLC, 2003.
[10] P. Kyasanur, and N. Vaidya, "Detection and Handling of MAC Layer Misbehaviour in Wireless Networks,"
[11] DCC, 2003.
[12] Srdjan Capkun, Levente Buttyan, and Jean-Pierre Hubaux. Self-organized public-key management for mobile ad hoc networks. IEEE Transactions on Mobile Computing, Vol.2, No.1, pp. 52–64, January 2003.
[13] R.Heady, G.Luger, A.Maccabe, and M.Servilla."The architecture of a network level intrusion detection system" In Technical report, Computer Science Department, University of New Mexico, August 1990.
[14] Kimaya Sanzgiri, Bridget Dahill, Brian Neil Levine, Clay Shields, and Elizabeth Belding-Royer."A secure routing protocol for ad hoc networks"In Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP 02), November 2002.
[15] Mayur C.Patel, Arpit J.Kuche "Different Attacks in MANET", IJMIE Vol.2, Issue 9, September, 2012
[16] Prajeet Sharma, Niresh Sharma and Rajdeep Singh "A Secure Intrusion detection system against DDOS attack in Wireless Mobile Ad-hoc Network" Vol. 41-No.21,

pp.16- 21, March 2012.
[17] A.M.Kurkure, Bhakti Chaudhari "Selfish Node Detection techniques in Manet: A Review" International Journal of Computer Science and Management Research, pp. 88-94, October 2013.
[18] Tiranuch Anantvalee, Jie Wu "A survey on Intrusion Detection in Mobile Ad Hoc Networks"Y. Xiao, X. Shen, and D.-Z. Du (Eds.) pp. 170 – 196, 2006.
[19] Wenjia Li and Anupam Joshi "Security Issues in Mobile Ad Hoc Networks - A Survey".