World Journal of Engineering Research and Technology
WJERT
www.wjert.org
SJIF Impact Factor: 4.326

SECURE ROUTING OF MANET USING MDSR WITH SNUPM ALGORITHM

C. Manjula Devi and S. Padma Priya*

Assistant Professor Department of Information Technology, K.L.N College of Engineering, Sivagangai, Tamil Nadu, India.

Article Received on 14/11/2017 **Article Revised on 05/12/2017** **Article Accepted on 26/12/2017**

***Corresponding Author**
S. Padma Priya
Assistant Professor Department of Information Technology, K.L.N College of Engineering, Sivagangai, Tamil Nadu, India.

ABSTRACT

Security is a decisive request in Mobile Ad-Hoc Network (MANETs) when evaluated to wired Network. MANETs are more suspicious to security attacks due to the need of a reliable centralized cloud and scanty resources. In MANET, We have malicious nodes that overcome the network protocols thereby diminishing the network's performance. The development of portable networks has implicated the need of new IDS models in order to deal with new security issues in these communication environments. In this paper, we proposed a Secured Network using Promiscuous Mode (SNuPM) which is a piece of Intrusion Detection System where it can repair the malicious nodes and change over back them into a normal node for effectual network performance.

KEYWORDS: MANET, IDS, AODV, Malicious node, Promiscuous mode, MDSR.

INTRODUCTION

The statute limit of a network to exchange data among the user that are appended to the network Wireless communication is practically utilized as a part of homes to keep away from the way toward presenting links is shown in Fig 1.

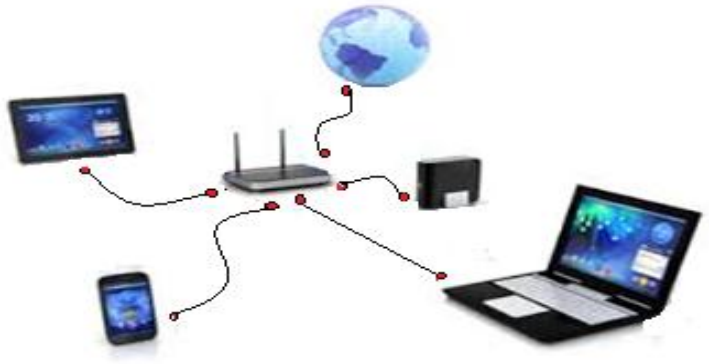

Fig. 1: Wireless network communication.

MANET is one of the vital factor in the network. A MANET is a type of ad hoc network that could alternate locations and form itself on the fly. A MANET is generally defined as a network that has many loosened or restricted nodes, frequently made out of mobile devices or other mobile pieces, that can arrange themselves in various ways and operate without infrastructure or centralized administrator.[1] MANETs as a rule are utilized for communication in event of natural disasters, on business conferences, and battle field, shows the significance of ensured safety of data transfer between two nodes.[2] A malicious node directs fake routing data in a MANET, asserting that it has an ideal route and other good node to route information packets through the malicious one. Most secure routing protocols are designed to prevent hazards to safety properties, such as: (1) Personality verification and non-repudiation; (2) resource availability; (3) plenitude; and (4) covertness and privacy by way of forging a routing message, a malicious node is intended to scramble the path, and then, further eavesdrop or drop the packets, posing a possible chance to protection properties (2), (3), and (4). An Intrusion Detection System (IDS) passively screens network visitors at more than one areas inside your system with the guide of utilizing IDS sensors. This nursing is referred to as promiscuous mode in view that it includes placing a network interface into promiscuous mode after which viewing all of the site visitors by means of the interface.

Related Works

Yi-an Huang and Wenke Lee[1] approach is proposed report our progress in developing intrusion detection (ID) capabilities for MANET. Building on our prior work on anomaly detection, we investigate how to improve the anomaly detection approach to provide more details on attack types and sources. For several well-known attacks, we can apply a simple

rule to identify the attack type when an anomaly is reported. In some cases, these rules can also help identify the attackers.

Sushma Kushwaha and Vijay Lokhande approach a Novel intrusion detection technique with the help of routing protocols in MANET (mobile ad hoc network). MANET is very popular and efficient, easy and secure way of communication between two or more mobile user ends and we can send and receive data, information, updates and signals from one end to another known end securely by using Novel Intrusion Detection System technique and by blocking unknown nodes in MANET.

Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, And Nei Kato approach we investigate the state-of-the-art of security issues in MANET. In particular, we examine routing attacks, such as link spoofing and colluding misrelay attacks, as well as countermeasures against such attacks in existing Manet protocols.

Nidal Nasser and Yunfeng Chen[7] approach we overcome the weakness of Watchdog and introduce our intrusion detection system called Ex Watchdog. The main feature of the proposed system is its ability to discover malicious nodes which can partition the network by falsely reporting other nodes as misbehaving and then proceeds to protect the network. Simulation results show that our system decrease the overhead greatly, though it doe not increase the throughput obviously.

Latha Tamilselvan[3] approach Computer simulation using GLOMOSIM shows that our protocol provides better security and also better performance in terms of packet delivery than the conventional AODV in the presence of Black holes with minimal additional delay and Overhead.

Overview of DSR

Dynamic Source Routing (DSR) is a routing protocol for wireless mesh networks. It is similar to AODV and it is an on-demand routing protocol. Periodic routing protocol[4] is not used in DSR. The source knows the entire hop-by-hop route to the destination.[5] These routers are stored in a route cache is shown in Fig 2. DSR is just like AODV except every intercede nodes broadcast a route request.[6] This route request incorporates destination deal with, supply handle and unique identification number. This protocol divided into two constituents: (1) Route discovery, (2) Route maintenance.

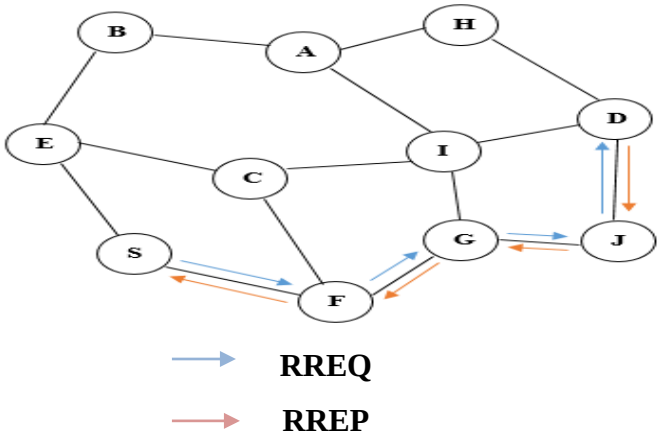

Fig. 2: Determines shortest path using Dynamic Source Routing.

Route discovery: In MANET, if a node is in need of sending data packets to a destination, at first it checks whether it has a pre-existing route for that destination. If so then it starts sending the data packets by that route. But if it could not find any pre-existing route, it starts route discovery process with Route Request (RREQ) packets and simple floating technique is used.[4] Every node receiving this request rebroadcasts until it achieves the exact destination or the route to destination.[5]

Route maintenance: The sender detects if network topology has changed, then it no longer uses its route from source to destination. Route error (RERR) packet identifies the source node,[4] if any link is failed in source route. So that source node can utilizes any other known route to the destination. Else the route discovery is done to find new route to destination. No termination of routers-Using old route causes loss of data packets and network bandwidth.

- **Data salvaging**-If an intercede node encounters a failed or broken link, it can use an equivalent route from its own cache.[5]
- **Gratuitous replies**-Sends a gratuitous reply to the source of route with better route[5] if the packet be routed with another node.

Promiscuous Mode

Promiscuous mode is a type of computer networking operational mode in which all network data packets can be routed and observed by all network adapters operating in this mode. It is a mode for a wireless network interface controller (WNIC) that causes the controller to pass all the traffic it gets to the Central Processing Unit (CPU) instead of passing only the frames that the controller is intended to receive. This mode the most part utilized packet sniffing that takes location on a router or on a computer related to a hub (instead of switch) or one being a

piece of a WLAN. Promiscuous mode is frequently used to analyse the network connectivity issues. Promiscuous mode permits a network device to block and read each network packet that arrives in its entirety. First, it enables accumulation of nearby data without any additional communication overhead. Second, the process of adjacent traffic observations without disturbing the other node is made easier. Promiscuous mode mechanism deals the new method which has two parts: By using the Performance analysis part which gives the probability of packet received by the sender or the next hop i.e., packet drop.

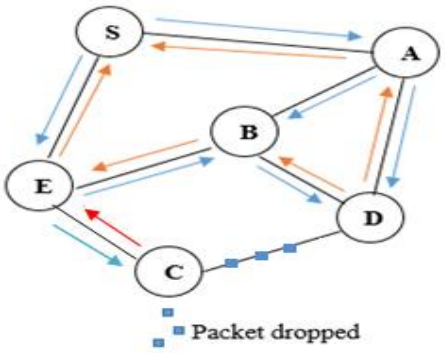

Fig 3: Packet drop by malicious node.

The next mechanism is Quick local repair scheme which makes use of nodes working in the adaptive promiscuous mode. The Promiscuous mode is activated to convert back the node to a normal node, if probability of packet received is low than the threshold value. Else the promiscuous mode is maintained at the deactivated state. In Fig 3., the node C (malicious node) gets the information from the destination in the form of packets, drop the packets and send fake information to the source So that, it is referred as malicious node.

PROPOSED METHODOLOGY

Network Formation

Simulation is regulated using NS2 2.35.No route overhead was considered in our simulation, because of the link stability and route lifetime. In 500X500 area mobile nodes exist. Square area is used to increase average hop length of a route with relatively small nodes. Every portable node is moving based on the mobility data files that were generated by mobility generator module. A 100 nodes are created. The transmission range is fixed at 100 meters. 100 nodes have destinations and try finding routes to their destination nodes. Maximum speed of node is set to 20m/sec. The nodes are assigned with an initial position. All nodes do not stop moving and the simulation time is 500 seconds.

Table 1: Simulation Parameters.

Parameter	Value
Coverage area	500x500
Simulation Time	600ms
No of nodes	100
Traffic Type	UDP-CBR
Packet Size	512 Bytes
Maximum Speed	20 m/s
Routing Protocol	MDSR
Mobility model	Random way point
Antenna Type	Omni antenna

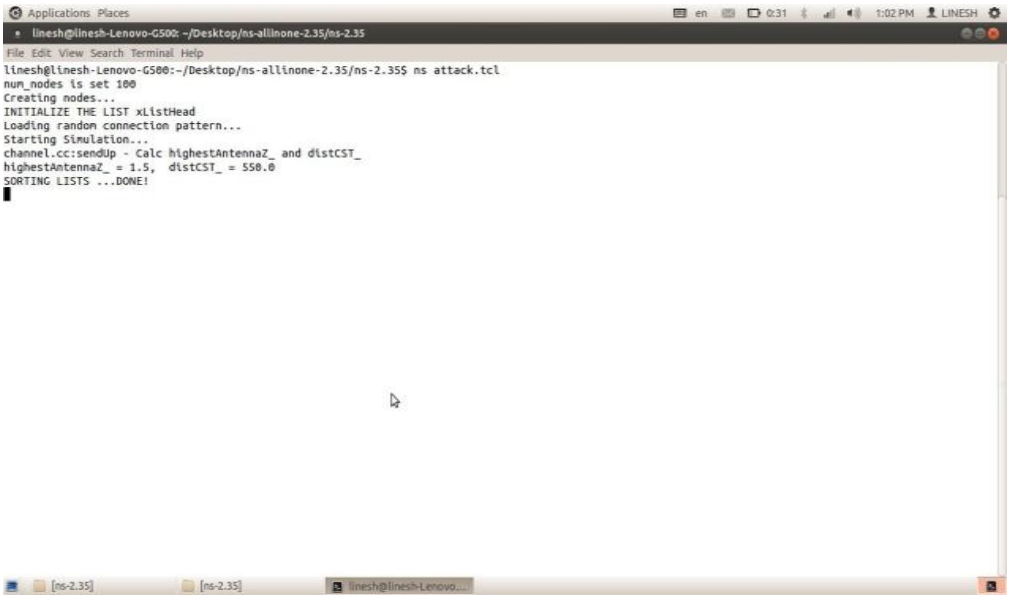

Fig. 4: Creating 100 nodes.

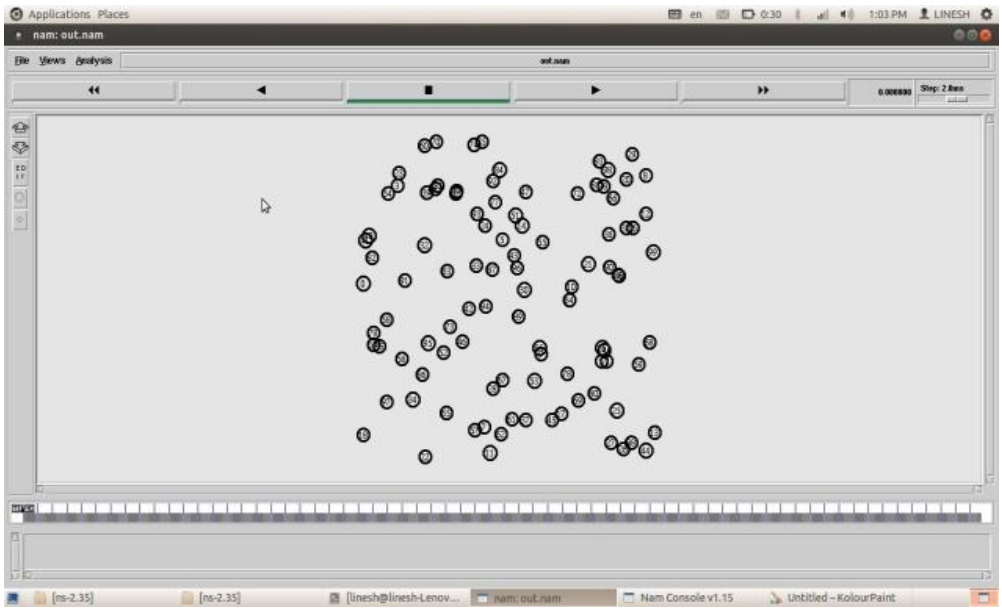

Fig. 5: Initial position of the nodes.

Modified DSR

In MANET, security and data integrity must provide by the routing protocol. Modified Dynamic Source Routing (MDSR) is one such routing protocol that incorporates AMN (Anti-Malicious Node) algorithm which continuously monitors the behaviour of nodes in the network. With the following assumptions, the AMN algorithm identifies the malicious nodes present in the network.

Anti-Malicious Node Algorithm

In this algorithm, to compute the performance of a network, Packet Drop Ratio and Energy level are considered to be the important parameters. In this paper a node is considered to be inactive or vulnerable to attack when its packet Drop ratio and energy level drops down below a threshold value. Trust based IDS works as the following assumption of calculating PDR (packet Drop ratio) and energy level.

Case 1: Energy level computation

Some initial energy value is assigned for every node in the network. For every transmission and reception of packets, the energy of a node is reduced. The difference between the initial energy level and obtained energy level gives the final energy level of the node. If the energy level goes beyond 40% then the node is considered to be vulnerable to attacks and such nodes are noted. So continuous monitoring of node's energy has been carried out throughout the simulation.

Power Consumption

In the MANET, every node computes its power consumption for every transaction and finds the remaining energy periodically. Each node may operate in any of the following modes.[9]

a) Transmission mode

The power consumed for transmitting a packet is given by the Eq (1)

$$\text{Consumed energy} = Pt * T \quad (1)$$

Where Pt is the transmitting power and T is transmission time.

b) Reception mode

The power consumed for receiving a packet is given by Eq (2)

$$\text{Consumed energy} = Pr * T \quad (2)$$

Where Pr is the reception power and T is the reception time.

The value T can be calculated as

T= Data size / Data rate (3)

Hence, the remaining energy of each node can be calculated using Eq (1) or Eq (2) based on the mode of operation.

Remaining energy = Current energy – Consumed energy…….. (4)

Other two modes like sleep and idle are not considered in our proposal since energy reduction is negligible. Initially every node has full battery capacity say 100% which is assigned to current energy.[10] The remaining energy is found using the Eq (4), on each transmission or reception of a data packet. If the remaining energy falls below 40%, that node will not act as a router to forward the packets.

Case 2: Packet Drop Ratio Computation

The quantity of dropped packet can be estimated by the following formula when packets are forwarded from source to destination.

Pr=Nr/Nf

Where number of packets forwarded to destination = Nf, number of packets received at destination = Nr, probability of Packets received =Pr.[11]

Case 3: Confirmation of Malicious Behaviors

From the above two cases calculated, If packet drop ratio is greater than 20 % and energy level is less than 40% for a particular node then the node is demonstrated to be a node that cannot effectively involve in transactions anymore and it simply called as a malicious node. From results obtained by above two tables the node with minimum energy level (i.e, less than 40%) and PDR (greater than 20%) is to be treated with promiscuous mode. This will lead to the re-enforcement (which converts them back into a normal node after a periodic interval by local repair scheme) of such nodes that will certainly increase the energy level of the node and the capacity to transfer packets in Trust based IDS.

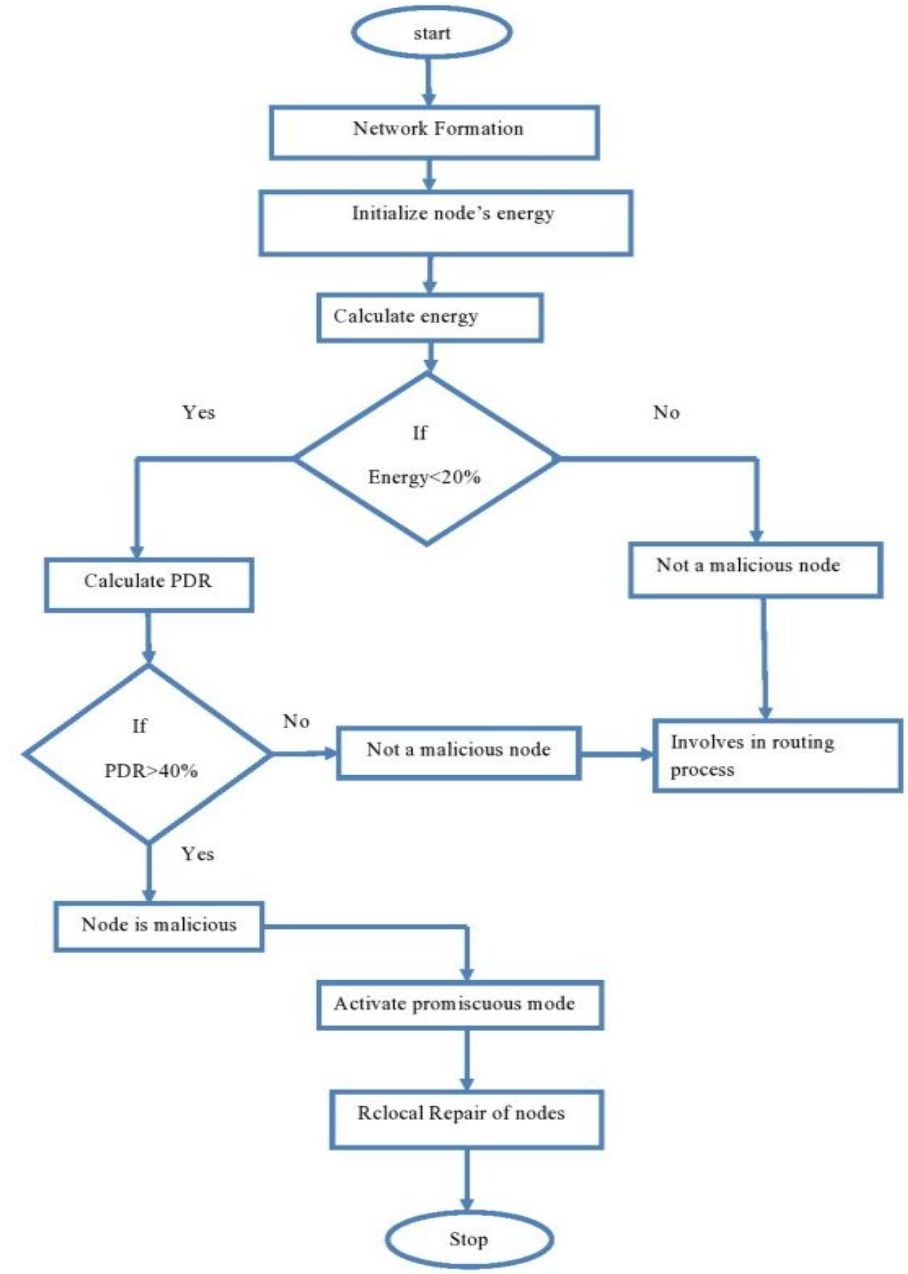

Fig. 6: Flow chart for promiscuous mode.

PDR Performance Analysis

To enhance the performance of the entire network, PDR and Throughput are considered to be the major parameters. The overall quality of service of the network is enhanced by the MDSR. PDR and Throughput are computed with the following formulas:

PDR= Nr/Nf

Where Nf= no of packets forwarded to the destination

Nr= no of packets received at the destination

The minimum PDR is less than 20%.

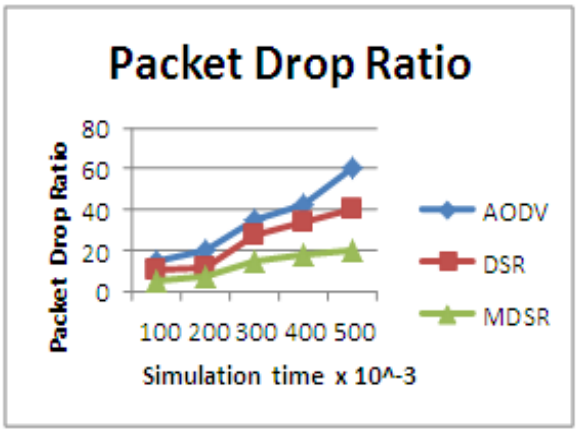

Fig. 7: Comparison of Packet Drop Ratio between DSR, AODV and MDSR.

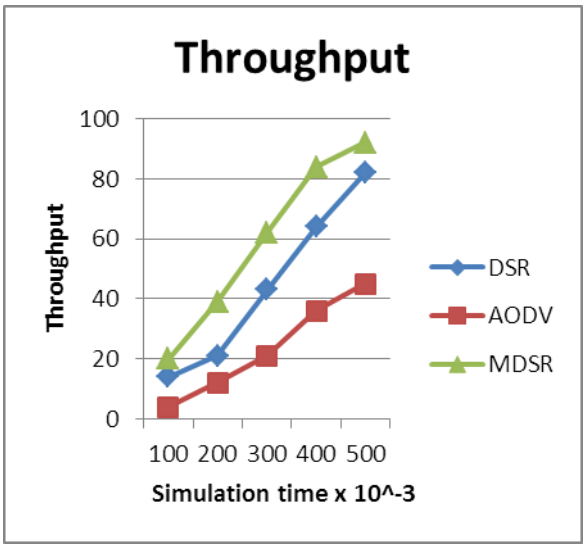

Fig. 8: Comparison of throughput between DSR, AODV and MDSR.

From the above graph, it is inferred that the PDR has been reduced drastically since there is no any malicious node participated in the routing process. Similarly, throughput is also maintained uptime throughout the routing process. This inference shows that the proposed method is far better that the existing methods to improve the efficiency of the network by eliminating the malicious nodes.

CONCLUSION

The reliability of the network is a major concern that should be concentrated to improve the efficiency and Quality of Service of the network. MANET, as it is more vulnerable to attack this paper proposes a mechanism called Promiscuous mode that converts the malicious node into a usual node. Promiscuous mode is activated only when the packet drop ratio and the energy level of a node falls below the threshold value since these nodes are assumed to be

inactive. So the promiscuous mode is initiated that monitors such inactive nodes and convert them into active one.

REFERENCES

1. Yi-an Huang and Wenke Lee "A Cooperative Intrusion Detection System for Ad Hoc Networks".
2. Bo Sun and Lawrence Osborne, Yang Xiao and Sghaierguizani "intrusion detection techniques in mobile ad hoc and wireless sensor networks", IEEE, October 2007.
3. Latha Tamilselvan and Dr. V Sankaranarayanan "Prevention of Co-operative Black Hole Attack in Manet", Journal of Networks, 2008; 3(5).
4. Dilpreet Kaur, Naresh Kumar "comparative analysis of aodv, olsr, tora, dsr and dsdv routing protocols in mobile ad-hoc networks" in: I. J. Computer Network and Information Security, 2013; 3: 39-46. Published Online March 2013 in MECS (http://www.mecs-press.org/) DOI: 10.5815/ijcnis.2013.03.05.
5. Parma Nand, Dr. S.C. Sharma "routing load analysis of broadcast based reactive routing protocols aodv, dsr and dymo for MANET", in: International Journal of Grid and Distributed Computing, March 2011.
6. Akshay Shankar, Lavanya Chelle "Performance Comparison of AODV, DSDV, OLSR and DSR Routing Protocols in Mobile Ad Hoc Networks", in**:** International Journal of Engineering Research & Technology, 2016; 5(10).
7. Nidal Nasser and Yunfeng Chen Enhanced Intrusion Detection System for Discovering Malicious Nodes in Mobile Ad hoc Networks", IEEE Communications Society subject matter experts for publication in the ICC proceedings, 2007.
8. Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, And Nei Kato, "A Survey Of Routing Attacks In Mobile Ad Hoc Networks".
9. M. Pushpalatha, Revathi Venkataraman, and T. Ramarao "Trust Based Energy Aware Reliable Reactive Protocol in Mobile Ad Hoc Networks".
10. Asad Amir Pirzada, "Secure Routing with the AODV Protocol", IEEE, 2005.