International Journal of Engineering Research and General Science Volume 3, Issue 1, January-February, 2015
ISSN 2091-2730

Examining the performance of AODV routing protocol under black hole attack with varied node densities and mobilities

B Satya Sravani[1], T Jagadeepak[2] , B A S Roopa Devi[3], B Prabhakara Rao[4]

[1]Dept. of ECE, Jawaharlal Nehru Technological University, Kakinada, Andhra Pradesh, India

satyasravani.buddana@gmail.com

[3]Dept. of CSE, Pragathi Engineering college, Surampalem, Andhra Pradesh, India

anasuyabhima@gmail.com

[2]Dept. of ECE, Jawaharlal Nehru Technological University, Kakinada, Andhra Pradesh, India

jagadeepak.tenali@gmail.com

[4]Dept. of ECE, Jawaharlal Nehru Technological University, Kakinada, Andhra Pradesh, India

drbpr@rediffmail.com

Abstract – In Mobile ad hoc network (MANET), nodes do not rely on any fixed infrastructure which enables users to communicate with each other without any pre-established physical link between them. Due to this high mobility nature and open distributed network characteristics, mobile ad hoc networks are threatened by lot of security attacks. Black hole attack is one such dangerous active attack in MANETs. In black hole attack, a malicious node falsely claims that it has the shortest part towards the destination inorder to transfer data packets even though it does not have one. Once the data packets broadcasted by the source node reaches this malicious node, it drops all those packets preventing from progressing further. This type of attacks seriously damages the performance of the network and should be strictly prevented. In this paper, the effect of black hole attack on the Ad-hoc On-demand Distance Vector (AODV) routing protocol is studied using Network Simulator (NS-2). The performance of the routing protocol AODV is evaluated with and without black hole attack in the network with varied node deployments

Keywords – Mobile ad hoc network, AODV, Black hole attack, Security attacks, Network Simulator, Packet delivery ratio, average end-to-end delay

1. INTRODUCTION

The remarkable technology of wireless networks started in late 1970s and the interest has been growing ever since. Earlier, information sharing between various communication devices is somewhat difficult, as the users need to set up static, bi-directional links between the devices to perform various administrative tasks. Inorder to prevent the difficulty in maintaining these infrastructure based networks, various techniques has been determined leading to ad hoc networks. In these type of networks, communication is entirely based on the construction of temporary networks with no basic infrastructure provided, no connecting wires and no administrative intervention required. Such interconnection between mobile nodes is called a Mobile Ad hoc Network (MANET).

Mobile ad hoc network is an autonomous and decentralized network in which any mobile node can freely move in and out of the network. These mobile nodes must act as both host and router in which both route discovery mechanism and data transmission between nodes is handled by the mobile nodes itself. These nodes have the ability to configure themselves and because of their self-configuring capability, they can form an arbitrary network when needed without the basis of any fixed infrastructure. Due to these characteristics, the network topology gets varied more frequently and hence a routing protocol must be efficient enough in delivering an ameliorated network performance. Traditional routing protocols used for wired networks cannot be employed for mobile ad hoc networks because the basic idea of such ad hoc networks is mobility with dynamic topology [14]. Routing protocols plays a major role

in such type of networks whose function is to transfer data packets between the mobile nodes efficiently tackling all the varying situations.

Due to their inherent characteristics and lack of any centralized administration, mobile ad hoc networks are vulnerable to different types of security attacks. These attacks include active interfering, passive eavesdropping, impersonation and denial of service [1]. Since the communication among the nodes is purely based on mutual trust between nodes, malicious nodes in the network must be identified carefully and must be restricted in their behaviour. Hence securing a mobile ad hoc network is necessary for basic functionality of the network. Black hole attack is one among these various attacks. In the black hole attack, a malicious node drops all the packets coming in its way without transferring them to its neighborhood node, thus degrading the network performance. Black hole attack may occur due to a malicious node which is deliberately misbehaving, as well as a damaged node interface. Such type of attacks must be prevented inorder to obtain better performance of the network. In this paper, the performance of the AODV routing protocol is examined under black hole attack.

2. ROUTING PROTOCOLS IN MANETS

In MANETs, nodes are not familiar with the network topology in priori. Routing protocols are responsible in establishing the paths between the mobile nodes inorder to transmit data between source and destination in that path. Hence a routing protocol must be efficient enough in handling various network phenomenon's and must tolerate against different security attacks. These routing protocols are broadly classified into three types based on the phenomenon in which they broadcast information.

1. Proactive or Table-Driven routing protocols

2. Reactive or On-Demand routing protocols

3. Hybrid routing protocols

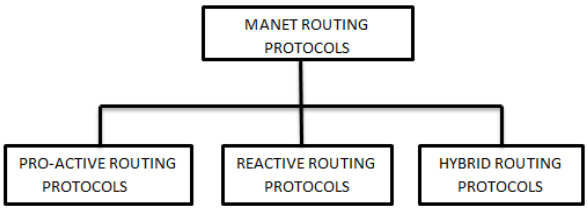

Figure 1: Routing Protocols in MANETs

2.1 Proactive routing protocols

Proactive routing protocols designed for MANETs are adopted from various traditional routing protocols available for wired networks. Proactive routing protocols attempt to maintain up-to-date routing information from each node to every other node in the network prior to the need of data transmission. The routing information is kept in a number of different routing tables and the routing information is updated regularly responding to the changes in the network topology. Primary advantage of proactive routing protocols is the availability of routes to concern nodes at any moment. Control overhead generated by these protocols is significantly more in large networks. Examples of such networks include DSDV, OLSR, WRP etc.

2.2 Reactive routing protocols

In this type of routing protocols, routes between the mobile nodes are not continuously maintained without any need such as in proactive routing protocols. Routes are established between the mobile nodes only when needed i.e., On-Demand. Here in reactive routing protocols, if a source node needs to send data packets to some destination, it checks whether it already has a route towards the destination to transmit data packets. If it does not find any route, then it initiates the route discovery phase to establish a new path towards the destination, through which the data packets are sent. The drawback of the reactive routing protocol is the introduction of route acquisition latency. The time taken by the data packets to reach the destination is more compared to proactive routing protocols. Reactive routing protocols include AODV, DSR, AOMDV etc.

2.3 Hybrid routing protocols

Hybrid routing protocols exploits the strengths of both proactive and reactive routing protocols inorder to deliver better performance. In hybrid routing, entire network is divided into zones so that, one protocol is used within a zone and another protocol is used between the zones. ZRP is an example of such routing protocol. Performance of the On-demand routing protocol, AODV is determined in this paper.

AD-HOC ON-DEMAND DISTANCE VECTOR (AODV) ROUTING PROTOCOL

AODV is an on-demand routing protocol. It does not maintain any routing information and participate in any periodic routing table exchanges prior to the necessity of communication. It finds the route between the mobile nodes only when needed (on-demand). AODV routing protocol adopts the concept of destination sequence numbers from DSDV to maintain the most recent information about the mobile nodes and the concept of on-demand route discovery and maintenance from DSR. Each entry in the routing table consists of the destination node, destination sequence number, number of hops, next hop, expiration table for the entry in the tables containing the routing information etc. AODV routing protocol makes use of various control messages such as Route Request (RREQ), and Route Reply (RREP) for establishing a path from source to destination. Header information of various control messages used in AODV is listed out in [10].

Whenever a source node needs to communicate with another node for which it has no route, the process of route discovery is initiated by the source which broadcasts a RREQ packet to its neighborhood nodes. Each neighboring node either responds to the RREQ by sending Route Reply (RREP) packet back to the source node or it further transfers the RREQ packets to its neighborhood nodes after incrementing the hop count. This route discovery process is carried on until the RREQ packet reaches the destination node or an intermediate node that has a fresh enough route entry for the destination in the routing table. Once the intermediate node has a valid route towards destination, it sends a RREP packet back to the source node in the reverse path. Making use of the reply from an intermediate node rather than the destination node reduces the route establishment time and also the control traffic in the network.

Sequence numbers are used in these control packets and they serve as time stamps which are used by the nodes to compare the freshness in the routing information [4]. When a node sends any type of routing control message, it increases its own sequence number in the message. Routing information with highest sequence number is considered to have more fresh or up-to-date information. If a node receives more than one RREP, it updates its routing information, and propagates the RREP with the highest sequence number discarding others.

The source starts the data transmission as soon as it receives the first RREP, and then it updates its routing information of better route to the destination node. If at all any of the nodes in the data path moves away causing the breakage of the link, the route discovery process is reinitiated to establish a new route to the destination node, Route Error (RERR) control packet is sent to all the nodes in the network which are using this broken link for communication. Routing protocol assumes that all the nodes are cooperative in nature in broadcasting information.

3. SECURITY ATTACKS IN MANETS

As in [12], security is a very important issue for the basic functioning of the network. MANETs are more susceptible to various attacks than wired networks due to its flexible environment. Due to its dynamic nature, the network can be accessed by both the legitimate users and malicious attackers. Since the routing protocol assumes that all the nodes in the network are cooperative in nature, malicious attackers can easily disrupt network operations by violating protocol specification. An attacker first analyses the network functioning and then launch attacks into the network which degrades the network performance. Hence these attacks must be strictly prohibited.

These attacks are basically classified into two categories – Passive attacks and Active attacks. These are further sub-classified into various kinds depending upon the type of the attack such as Denial of Service attack, Fabrication attack, Modification attack, Replay attack and Impersonation attack. Passive attacks just listen to the traffic of the network to obtain vital information. These types of attacks do not affect the functioning of the network. It is difficult to identify such type of attacks as the performance of the network does not vary. It is even not possible to detect the presence or the location of the attacker node in this case. The only way to prevent

such type of attacks is through encryption. Whereas, active attacks aim to modify the transmitted data by adding random packets or attempt to interrupt the data flow from source to destination. The main purpose is to pull all packets towards the attacker for analysis or to obstruct the network communication. Black hole attack is one such attack which comes into this category. Among these two types of attacks, only active attacks can be accepted out at routing level. They can either be inner or outer. In order to combat these attacks, a secure environment should provide confidentiality, availability, authenticity, integrity and non-repudiation [2].

BLACK HOLE ATTACK

A Black hole attack is a denial of service type of attack, where a malicious node attracts all the data packets by falsely claiming that it has the shortest and fresh enough route towards the destination [7]. Once the source node chooses that path to transfer data, the malicious node absorbs all the data without forwarding them to the destination. To be more elaborate, when a source nodes needs to communicate with some destination node, it initiates the route discovery process by sending route request (RREQ) packets. In black hole attack, a malicious node initially waits till the nodes broadcast RREQ packets. Once the RREQ packet is received by the malicious node, it immediately responds with a false route reply (RREP) packet with highest sequence number, indicating that it has the fresh route towards the destination. The source node believes that the destination node is behind the malicious node and ignores all the RREP packets received from other nodes, even if it is from actual destination. Then the source node transmits the data packets through the path containing the malicious node trusting that these packets will reach the destination.

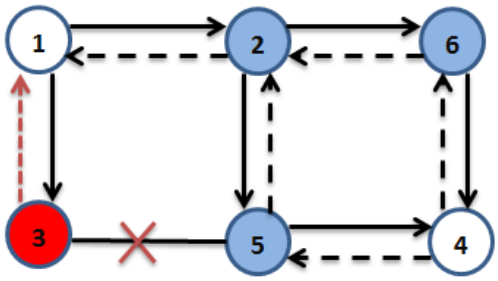

Figure 2: Black hole attack in MANET

Once the data packets reach the black hole node, it does not forward the data packets further and simply drops them. Thus, a black hole node pretends to have fresh routes to all the destinations in the network requested by all the nodes and absorbs the networks data traffic. This type of attack never forwards any data packets.

In figure 2, source node 1 wants to send data packets to the destination node 4 in the network. Here node 3 is a malicious node which acts as a black hole. When the source node initiates the route discovery process, the malicious node responds to the RREQ packet immediately with a false or malicious RREP having higher modified sequence number, though it do not have any route to the destination. Since the reply from the malicious node first reaches the source node, it updates its routing table accordingly. Then it starts broadcasting the data packets through node 3, which do not forward the data packets to its neighboring node.

4. SIMULATION SETUP

Inorder to analyze the performance of AODV under blackhole attack, network simulator NS-2 is used. NS-2 uses the collaborative environment for simulation making use of discrete event simulation [6]. Here various quantitative metrics like packet delivery ratio, average end-to-end delay, normalized routing load and jitter are estimated under blackhole attack. The performance of the network is determined with the following network parameters summarized in Table 1.

Table 1: Simulation Parameters

Parameters	Values
Simulator	NS – 2.35
Network Dimensions	1000m x 1000m
Simulation Time	200 sec
Node mobility model	Random waypoint
Routing protocols	AODV
Application type	UDP
Traffic type	Constant Bit Rate (CBR)
No. of nodes	20, 40, 60, 80, 100
Speed of node	5 – 30 m/s in steps of 5
Pause Time	0 sec
Physical Layer	IEEE 802.11b
MAC Protocol	IEEE 802.11
Transmission rate	100 kbps
Packet size	512 kb

5. PERFORMANCE EVALUATION

In this paper, the effect of black hole attack is determined by considering the quantitative metrics such as packet delivery ratio, average end-to-end delay, normalized routing load and jitter. However, the network performance is evaluated with and without attack. In both the cases, the following metrics are considered to evaluate the performance under varied node mobility and node density.

1) Packet Delivery Ratio: Packet Delivery Ratio (PDR) is the ratio between the number of packets transmitted by a traffic source and the number of packets received by a traffic sink. It measures the loss rate as seen by transport protocols and as such, it characterizes both the correctness and efficiency of ad hoc routing protocols. It represents the maximum throughput that the network can achieve. A high packet delivery ratio is desired in any network.

$$PDR = \frac{Total\ no.\ of\ received\ packets}{Total\ no.of\ packets\ sent}$$

2) Average End-to-End Delay: The packet end-to-end delay is considered as the average time a packet takes to traverse the network. This is the time from the generation of a packet by the source, till its reception at the destination's application layer and is expressed in seconds. It therefore includes all the delays in the network such as buffer queues, transmission time and delays induced by routing activities and MAC control exchanges. The end-to-end delay is therefore a measure of the how well reliability of a routing protocol adapts to the various constraints in the network and hence represents the reliability the routing protocol.

$$EED = \sum \frac{(Received\ time - sent\ time)}{Total\ data\ packets\ received}$$

3) Normalized Routing Load: Normalized Routing Load is the ratio between the total number of routing packets sent to the number of data packets delivered. This metric is used to evaluate the scalability of the network.

$$NRL = \frac{no.\ of\ routing\ packets\ sent}{no.of\ data\ packets\ received}$$

4) Jitter: Jitter is the variation in the time between packets arrival, caused by network congestion, timing drift, or route changes. A network with constant delay has no variation (or jitter). Hence jitter should be minimum for a routing protocol to perform better.

5.1 Impact of black hole attack with varied node densities

Inorder to determine the impact of the black hole attack on the AODV routing protocol, its performance is determined including an attacker node and by varying the total number of nodes. Various metric values are determined which are discussed in this section

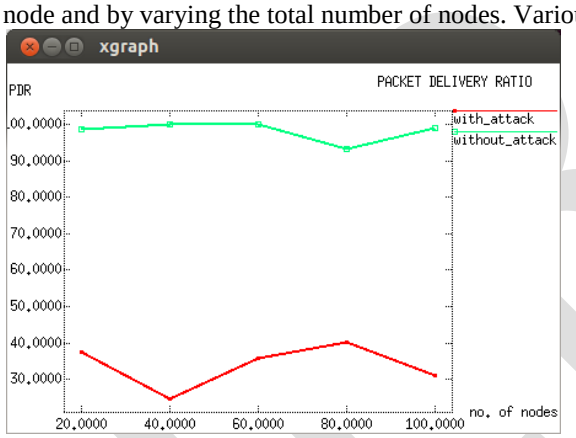

Figure 3: No. of nodes vs PDR

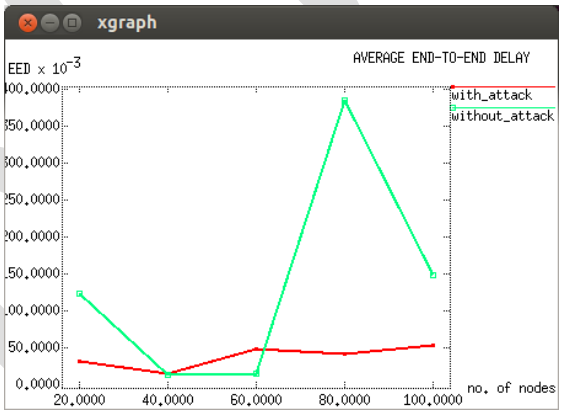

Figure 4: No. of nodes vs EED

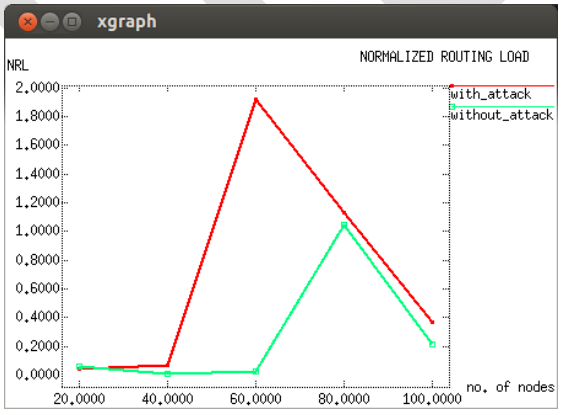

Figure 5: No. of nodes vs NRL

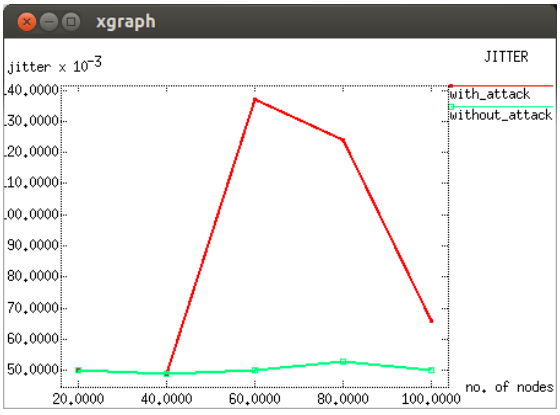

Figure 6: No. of nodes vs Jitter

From figure 3, a drastic change in the packet delivery ratio is observed, when the network is analyzed in the presence of blackhole attack. This happens because the number of packets delivered greatly reduces as all packets traversed in attacker's way, will be dropped. From figure 4, it is clear that the average end-to-end delay is somewhat consistent in the presence of the attacker than that of the normal case. Figure 5 depicts that normalized routing load is more in the presence of attack, as the routing packets generated in the network greatly increases because of the malicious nodes as it frequently broadcasts the packets to misinterpret the source node. From figure 6, it is evident that as the number of nodes increases over 40 nodes, jitter in the network increases indefinitely as the attacker nodes presence creates routing changes and congestion in the network when compared to no attack scenario.

5.2 Impact of black hole attack with varied node mobilities

In addition to analyzing the network performance with varying node densities, estimation of performance with changing node mobilities is also implemented. The node speeds are varied in the range of 5-30 m/sec. The following simulation results depict the impact of black hole attack on the AODV routing protocol

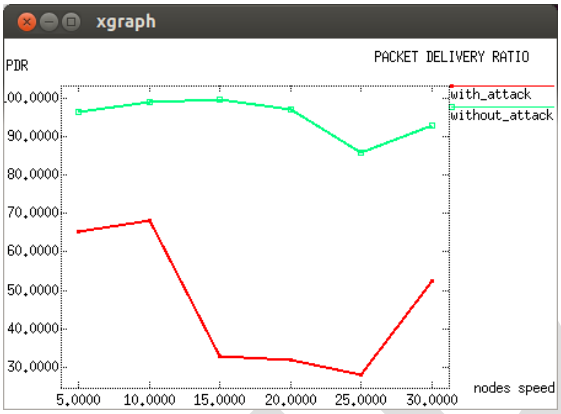

Figure 7: Node speed vs PDR

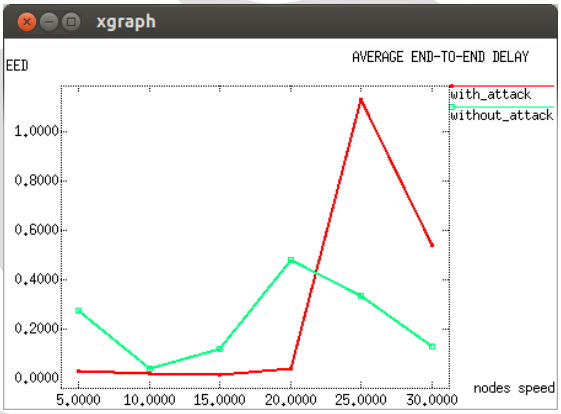

Figure 8: Node speed vs EED

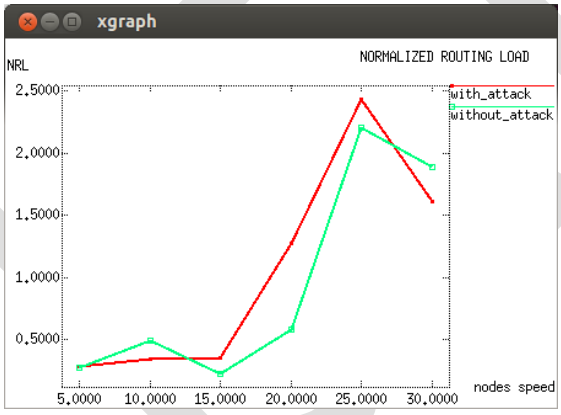

Figure 9: Node speed vs NRL

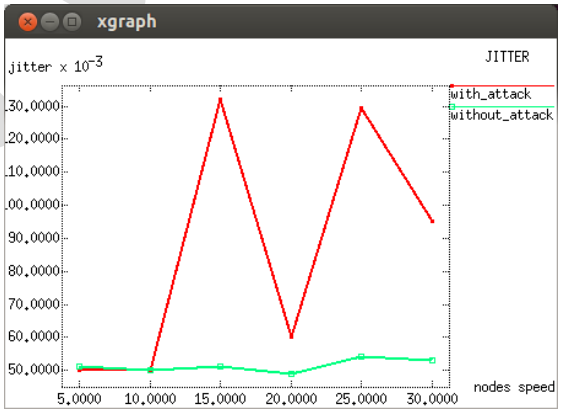

Figure 10: Node speed vs Jitter

Figure 7 shows that with increased node mobility, Packet delivery ratio declines drastically signifying the impact of blackhole attack. Figure 8 illustrates that when the speeds of the nodes is limited to 20m/s, in scenarios of with and without attack, end to end delay is low in the presence of the attacker because of its mischievous activity; however after 20 m/s, as mobility increases, delay increases predominantly. Figure 9 illustrates that the Normalized routing load remains almost same in instances of with and without blackhole attack with varying node mobilities. This shows that the impact of the attacker is slightly decreased in this case because of the frequent path changes with increased mobility. However, figure 10 shows the way in which the jitter gets fluctuated in the

presence of blackhole attack. This is because of the network congestion which greatly increases with varying node mobility. However, jitter is consistent in the network without any attacker.

6. CONCLUSION

In this paper, different mobile ad hoc network scenarios are analyzed with and without blackhole attack under AODV routing protocol, considering various simulation parameters listed above. The network is examined for different performance differentials like packet delivery ratio, average end-to-end delay, normalized routing load and jitter with varying node densities and mobilities in the deployed network. The simulation results signify that the performance of network in the presence of blackhole attack is predominantly decreasing in packet delivery ratio as the attacker nodes discards all the data packets traversing its path. Jitter increases as the attacker nodes increase congestion in the routes discovered. Average end-to-end delay decreases in the presence of attack, as the attacker nodes send RREP message immediately with minimum hop count and maximum sequence number. These changes in employed metrics conclude that network performance is degrading predominantly in the presence of blackhole attack.

REFERENCES:

[1] Ketan Sureshbhai Chavda, "A Performance analysis of AODV under Black hole attack in MANET", IJTCSE, Vol.1, No.2, pp. 82-87, June 2014.
[2] Jaspal Kumar, M. Kulkarni, Daya Gupta, "Effect of Black hole Attack on MANET routing protocols", IJCNIS, Issue 5, pp. 64-72, April 2013.
[3] Er. Punardeep Singh, Er. Harpal Kaur, Er. Satinder Ahuja, "Brief Description of Routing Protocols in MANETs and Performance and Analysis (AODV, AOMDV, TORA)", IJARCSSE, Vol. 2, Issue. 1, January 2012.
[4] Ranjeet Suryawanshi, Sunil Tamhankar, "Performance Analysis and Minimization of Black hole attack in MANET", IJERA, Vol. 2, Issue-4,pp. 1430-1437, July-August 2012.
[5] A. Bhattacharya, H. Nath Saha, "A Study of Secure Routing in MANET: various attacks and their Countermeasures", IEMCON 2011 organized by IEM., january 2011.
[6] The Network Simulator ns2,http://www.isi.edu/nsnam/ns, 2011.
[7] Ming-Yang Su, Kun-Lin Chiang and Wei-Cheng Liao , "Mitigation of Black Hole Nodes in Mobile Ad Hoc Networks", 2010 IEEE International Symposium on Parallel and Distributed Processing with Application.
[8] R. H Rashid Khokhar , Md. A. Nagdi, "A Review of Current Routing Attacks in Mobile Ad Hoc Networks", International Journal of Computer Science and Security, pages 18-29, 2009.
[9] K. Sanzgiri, D. LaFlamme, B. Dahill, B. N. Levine, C. Shields, and E. M. B. Royer, "Authenticated routing for ad hoc networks," IEEE Journal on Selected Areas in Communications, vol. 23, no. 3, pp. 598-610, Mar. 2005.
[10] C. E. Perkins, E. Beliding Royer, S. Das, "Ad hoc On-demand Distance Vector (AODV) routing", IETF Internet Draft, MANET working group, January 2004.
[11] M. A. Shurman, S. M. Yoo, and S. Park, "Black hole attack in wireless ad hoc networks." proceedings of the ACM 42nd Southeast Conference (ACMSE'04), pp 96-97, Apr. 2004.
[12] H. Deng, W. Li, and D. P. Agarwal, "Routing security in ad hoc networks", IEEE Communications Magazine, Vol. 40, No. 10, pp. 70-75, October 2002.
[13] C. E. Perkins and E. M. Royer, "Ad Hoc On-Demand Distance Vector Routing" Proc. 2nd IEEE Workshop. Mobile Computing System and Apps. New Orleans, LA, Feb. 1999, pp. 90–100.
[14] Janne Lundberg, Helsinki university of technology, "Routing Security in Ad hoc Networks", http://citeseer.nj.nec.com/400961.html