

## Prevention of Black Hole Attack in MANET

Pooja Jaiswal  
Computer Science & Engineering,  
Madan Mohan Malviya, Engineering College,  
Gorakhpur, Uttar Pradesh, India  
Email: [jaiswalpoo@gmail.com](mailto:jaiswalpoo@gmail.com)

Dr. Rakesh Kumar  
Computer Science & Engineering,  
Madan Mohan Malviya, Engineering College,  
Gorakhpur, Uttar Pradesh, India  
Email: [rkiitr@gmail.com](mailto:rkiitr@gmail.com)

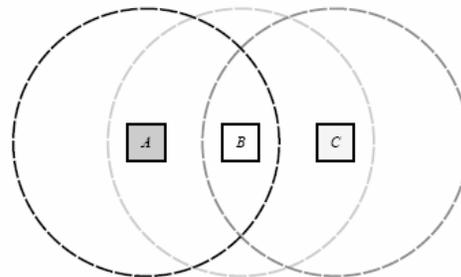
**Abstract:** An ad hoc network is a collection of mobile nodes that dynamically form a temporary network. It operates without the use of existing infrastructure. One of the principal routing protocols used in ad hoc networks is AODV (ad hoc on demand distance vector) protocol. This is anticipated to offer a range of flexible services to mobile and nomadic users by means of integrated homogeneous architecture. Energy constrained node, low channel bandwidth, node mobility, high channel error rates, channel variability and packet loss are some of the limitations of MANETs. The security of the AODV protocol is compromised by a particular type of attack called ‘Black Hole attack’. Black hole attack is one of the security threat in which the traffic is redirected to such a node that actually does not exist in the network. In this attack a malicious node advertises itself as having the shortest path to the node whose packets it wants to intercept. This paper shows simulation results, provides fast message verification, identifies black hole and discovers the safe routing and avoiding the black hole attack.

**Keywords-** MANET, Black Hole, Routing Protocols.

### 1. INTRODUCTION

An ad hoc network [1] is a wireless network without any fixed infrastructure. It is a group of mobile hosts without the required involvement of any offered infrastructure or centralized access point such as a base station. There are various challenges that are faced in the Ad hoc environment. AODV is an on demand routing network protocols which is specially design for Ad hoc network.

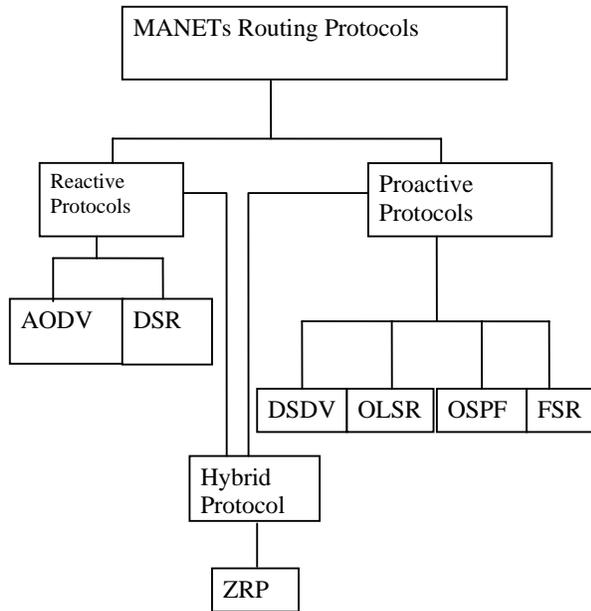
Ad hoc network offer great flexibility, higher throughput, lower operating cost and better coverage because of collection of independent nodes. Mobile ad hoc networks consist of mobile nodes, which can communicate with each other and nodes can enter and leave the network anytime due to the short transmission range of MANETs [2] [3], routes between nodes may consist of one or more hops. Thus each node may either work as a router or depend on some other node for routing. Figure 1.1 shows a simple ad hoc network with three mobile hosts using wireless interfaces. Host A and C are out of range from each other’s wireless transmitter. When exchanging packets, they may use the routing services of host B to forward packets since B is within the transmission range of both of them.



**Figure 1.1: Mobile Ad hoc network with 3 mobile nodes**

Routing protocols for Mobile Ad hoc networks can be broadly divided into two distinct categories, namely proactive (table-driven) routing protocols and reactive (on-demand) routing protocols. In Proactive routing protocols, each node maintains up-to-date routing information to every other in a number of routing tables & routes can quickly established without any delay. Reactive or on-demand routing

protocols are designed to overcome the increased overhead problem in proactive protocols. Unlike proactive protocols, reactive protocols create a route only when desired.



**Fig 1.2: MANETs Routing Protocol**

There are two kinds of possible attacks: Passive and Active. In passive attacks the attacker does not disturb the routing protocol. It only eavesdrops upon the routing. In active attacks, malicious nodes can disturb the correct functioning of a routing protocol by modifying routing information, by fabricating false routing information, and by impersonating other nodes launched on an ad hoc network. Some typical types of active attacks that can usually be easily performed against MANETs are listed as follows [4] [5] [6]:

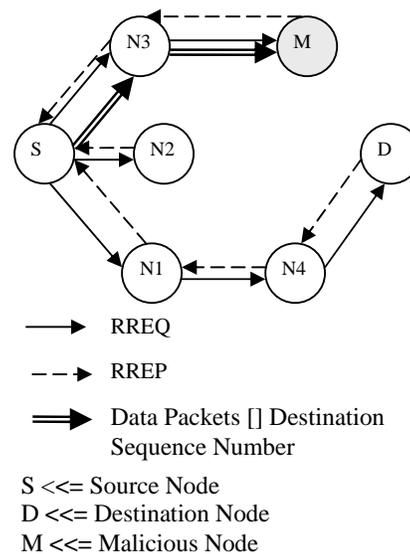
- **Black hole:** A malicious node may use the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. The detailed description is discussed below.
- **Denial of Service (DoS):** A malicious node may generate frequent unnecessary routing requests to make the network resources unavailable to other nodes. DoS attack results when the network bandwidth is hijacked by a malicious node [19].

- **Impersonation:** A malicious node may impersonate another node while sending the control packets to create an anomaly update in the Routing Table (RT).

The remaining part of this paper is organized as follows: Section 2 describes introduction of Black Hole Attack. Section 3 describes related works that prevent MANET from attack. Section 4 introduces the security issues of the MANET. Section 5 describes proposed solutions that explain in this paper. Section 6 describes simulation result using proposed solution and Section 7 describes conclusion and future work.

## 2. BLACK HOLE ATTACK

A black hole is a node that always responds positively with a RREP message to every RREQ, even through it does not really have a valid route to the destination node. Since a black hole node does not have to check its routing table, it is the first to respond to the RREQ in most cases. Then the source routes data through the black hole node, which will drop all the data packets it received rather than forwarding them to the destination. In this way the malicious node can easily misroute lot of network traffic to itself and could cause an attack to the network with very little effort on it. These black hole nodes may work as a group.



**Figure 2.1: Black Hole Attack**

In figure 2.1 Destination Sequence Number is a 32-bit integer associated with every route and is used to decide the freshness of a particular route. Node N3 will now send it to node. Since node N1 and node N2 do not have a route to node D, they would again broadcast the RREQ control message. RREQ control message broadcasted by node N3 is also expected to be received by node M (assumed to be a malicious node). Thus, node M would generate a false RREP control message and send it to node N3 with a very high destination sequence number subsequently sent to the node S. However, in simple AODV, as the destination sequence number is high, the route from node N3 will be considered to be fresher and hence node S would start sending data packets to node N3. But in our proposed AODV before sending data packets firstly source node will check the difference between sequence numbers. If it is too large, obviously the node will be a malicious one, and it will be isolated from the network. Otherwise it simply transfers the data packets to the destination node.

### **3. RELATED WORKS**

Researchers have proposed solutions to identify and eliminate black hole nodes. In [10], Deng et al. proposed a solution for individual black holes. According to their solution, information about the next hop to destination should be included in the RREP packet when any intermediate node replies for RREQ. Then the source node sends a further request (FREQ) to next hop of replied node and asks about the replied node and route to the destination. By using this method we can identify trustworthiness of the replied node only if the next hop is trusted. This solution detects only one black hole attack at a time. Ramaswamy et al. [11] studied multiple black hole attacks on mobile ad hoc networks. However, they only considered multiple black holes, in which there is no collaboration between these black holes. We also simulate AODV and the solution proposed by [10] and

compares them with [11]. An algorithm presented in [12] claims to detect the black hole attack in a MANET which is based on relationships of a certain trust level among the nodes. However, in the real network, it is very difficult to set an appropriate value for the trust level. In the method [17], every node has a function of learning the traffic flow in the network and evaluating the possibility criterion of black hole attack based on such learning results in order to detect the malicious node. If the value of the criterion is larger than a predetermined threshold, the node judges that there exists a black hole attacker. This method only provides detection of a single black hole attacker and cannot detect a chain of malicious nodes which cooperate with each other.

To defend against the black hole attack and to overcome the disadvantages of all the paper that studied above, this paper proposes a new detection method based on the destination sequence number. Furthermore, this proposed method can detect more than one attacker i.e. in a chain at the same time and have larger thresholds.

### **4. SECURITY ISSUES IN MANET**

Security in MANET is the most important concern for the basic functionality of network. Availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANET often suffer from security attacks because of the its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battle field situation for the MANET against the security threats.

MANETs are very flexible for the nodes i.e. nodes can freely join and leave the network. There is no main body that keeps watching on the nodes entering and leaving the network. All these weaknesses

of MANETs make it vulnerable to attacks and these are discussed below.

- **Non secure boundaries:** MANET is vulnerable to different kind of attacks due to no clear secure boundary. The nature of MANET, nodes have the freedom to join and leave inside the network. Node can join a network automatically if the network is in the radio range of the node, thus it can communicate with other nodes in the network. Due to no secure boundaries, MANET is more susceptible to attacks. The attacks may be passive or active, leakage of information, false message reply, denial of service or changing the data integrity. There is no protection against attacks like firewalls or access control, which may result the vulnerability of MANET to attacks [21].
- **Compromised Node:** Some of the attacks are to get access inside the network in order to get control over the node in the network using unfair means to carry out their malicious activities. Mobile nodes in MANET are free to move, join or leave the network in other words the mobile nodes are autonomous [22]. Due to this autonomous factor for mobile nodes it is very difficult for the nodes to prevent malicious activity it is communicating with. Ad-hoc network mobility makes it easier for a compromised node to change its position so frequently making it more difficult and troublesome to track the malicious activity.
- **No Central Management:** MANET is a self-configurable network, which consists of Mobile nodes where the communication among these mobile nodes is done without a central control. Each and every node act as router and can forward and receive packets [23]. MANET works without any preexisting infrastructure. This lack of centralized management leads MANET more vulnerable to attacks. Detecting attacks and monitoring the traffic in highly dynamic and for large scale ad hoc network is very difficult due to no central management.
- **Problem of Scalability:** In traditional networks, where the network is build and

each machine is connected to the other machine with help of wire. The network and the scale of the network, while designing it is defined and that do not change much during the use. In other words we can say that the scalability of the network is defined in the beginning phase of the designing of the network.

The case is quite opposite in MANETs because the nodes are mobile and due to their mobility in MANETs, the scale of the MANETs is changing. It is too hard to know and predict the numbers of nodes in the MANETs in the future. The nodes are free to move in and out of the ad hoc network which makes the ad hoc network very much scalable.

There are five major security goals that need to be addressed in order to maintain a reliable and secure ad-hoc network environment. These mechanisms prevent, detect, and respond to security attacks. They are mainly [9]:

- **Availability** ensures the survivability of network services despite denial of service attacks. It assures that the services of the system are available at all times and are not denied to authorize users. A denial of service attack could be launched at any layer of an ad hoc network.
- **Confidentiality** ensures that certain information is never disclosed to unauthorized entities. In MANETs, this is more difficult to achieve because intermediates nodes (that act as routers) receive the packets for other recipients, so they can easily eavesdrop the information being routed.
- **Integrity** guarantees that a message being transferred is never corrupted. And Message being transmitted is never altered. A message could be corrupted because of benign failures, such as radio propagation impairment, or because of malicious attacks on the network.
- **Authentication** Assure that an entity of concern or the origin of a communication is what it claims to be or from. It enables a node to ensure the identity of the peer node it is communicating with. Without authentication, an adversary could

masquerade a node, thus gaining unauthorized access to resource and sensitive information and interfering with the operation of other nodes.

- **Non-repudiation** ensures that sending and receiving parties can never deny ever sending or receiving the message. Non-repudiation is useful for detection and isolation of compromised nodes. When a node A receives an erroneous message from a node B, non-repudiation allows A to accuse B using this message and to convince other nodes that B is compromised.

## 5. PROPOSED SOLUTION

The Proposed method can be used to find the secure routes and prevent the black hole nodes in the MANET by checking whether there is large difference between the sequence number of source node or intermediate node who has sent back RREP or not. Generally the first route reply will be from the malicious node with high destination sequence number, which is stored as the first entry in the Route Request Table (RRT). Then compare the first destination sequence number with the source node sequence number, if there exists much more differences between them, surely that node is the malicious node, immediately remove that entry from the RRT.

**Algorithm: ReceiveReply (RREP) Method**

**Parameters:** DSN – Destination Sequence Number, NID – Node ID, MN-ID – Malicious Node ID, IN- Intermediate Node, RREP- Route Reply, NHN- Next Hop Node.

### Step 1: (Initialization Process)

In this if the source node (SN) does not have the route entry to the destination, it will broadcast a RREQ (Route Request) message to discover a secure route to the destination node.

### Step 2: (Storing Process)

Any node received this RREQ either replies for the request or again broadcasts

it to the network depending on the availability of fresh route to the destination. And store all the Route Replies DSN in RRT.

**Step 3:** When IN generates RREP and sends to NHN

```
{  
Table contains entry for each neighbor and  
check which data is sent and which data is  
received from neighbor.  
If reply comes back collects IP addresses  
of all nodes  
Updates route entry for destination and  
table is updated.  
}
```

### Step 4: (Identify and Remove Malicious Node)

```
Retrieve the first entry from RRT  
If DSN is much greater than SSN then  
discard entry from RRT as  
Select Dest_Seq_No from table  
If (DSN >>=Src_Seq_No)  
{  
MN=Node_Id  
Discard entry from table  
}
```

### Step 5: (Node Selection Process)

- \* Sort the contents of RRT entries according to the DSN
- \* Select the NID having highest DSN among RRT entries.

### Step 6: (Continue default process)

Call RREP method of default AODV Protocol.

This show malicious node is identified and removed.

(1) The malicious node is identified at the initial stage itself and immediately removed so that it cannot take part in further process.

(2) No delay = malicious node are easily identified

(3) No modification is made in other default operations of AODV Protocol.

(4) Better performance produced in little modification and

(5) Less memory overhead occurs because only few new things are added.

## 6. SIMULATION AND RESULTS

In this section, the simulation environment and the simulation results are discussed. Simulation is done using the network simulator NS-2 [24].

The numbers of nodes we have considered for simulation are 10 to 70 mobile nodes in the terrain area of 800m \* 800m. Around 10% of them to be attackers are assumed, which are performing data modification attack. We have also used some CBR (Constant Bit Rate) connections with packet length of 512 bytes to emulate traffic over the network. Each node independently repeats this behavior and mobility is varied by making each node stationary for a period of pause time.

**Table 1: Simulation Parameters**

Parameters	Values
Network size	800m * 800m
Number of nodes	30, 70
Max speed/mobility	50 m/s
Wait/Pause time	10 s
Traffic model	CBR
Routing protocol	AODV
Number of attackers	10%
Simulation time	1000s
Number of sources	5
Transmission range	250m

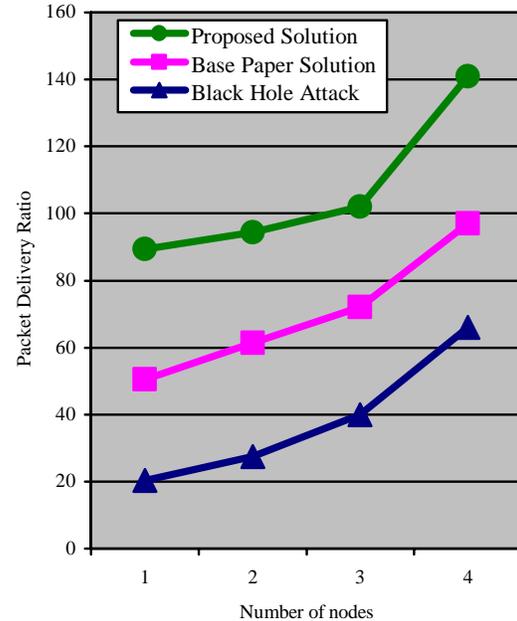
### 6.1 Performance Evaluation

The metrics used in evaluating the performance are:

- Packet Delivery Ratio:** It is the ratio of the number of data packets delivered to the destinations to the number of data packets generated by the sources. This evaluates the ability of the protocol to deliver data packets to the destination in the presence of malicious nodes [13]. It is clear from fig. 4 that PDR of AODV is heavily affected by the malicious nodes where as the PDR of Proposed AODV is immune to it. It is represented by P and calculated as:

$$P = \frac{\text{number of data packets received}}{\text{number of data packets sent}} * 100$$

The PDR decreases when there is malicious node (black hole) in AODV because some packets are dropped due to attack. This means the number of correctly received packet is very less than the number of transmitted packets.



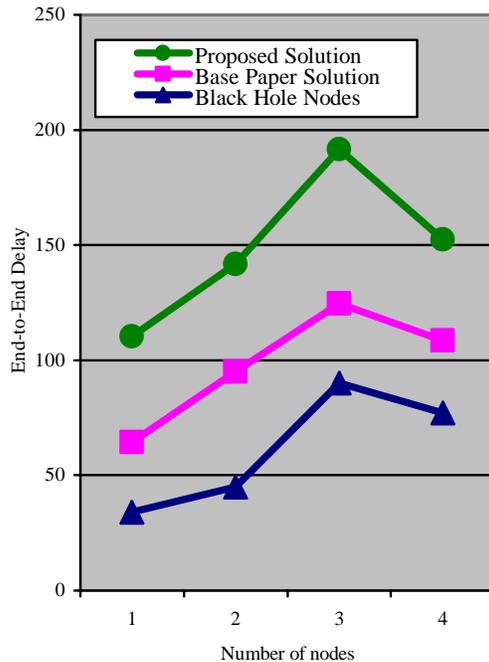
**Figure 6.1: PDR vs. number of nodes**

This figure 6.1 confirms that while proposed AODV is secure against black holes, AODV is not. This is mainly due to the fact that our protocol detects the attacker and allows the source nodes to avoid it.

- End-to-End Delay:** This is average delay between the sending of packets by the source and its receipt by the receiver. It means it is difference between the receiving time and sending time. This includes all possible delays caused by buffering during data acquisition, route discovery, queuing, processing at intermediate nodes, retransmission delays, propagation time, etc. It is denoted by D and calculated as:

$$D = \frac{\sum_{i=1}^n d_i}{n}$$

Where  $d_i$  is a time for end-to-end delay of data packets at  $i^{\text{th}}$  position.



**Figure 6.2: End-to-End delay vs. number of nodes**

The figure 6.2 shows the impact of the Black hole attack to the Networks end-to-end delay. The end-to-end delay of the network also decreases due to black hole effect as compared to without the effect of black hole attack. We vary the speed of the node and take the result to the different node speed.

## 7. CONCLUSION AND FUTURE SCOPE

MANET has the ability to deploy a network where a traditional network infrastructure environment cannot possibly be deployed. Security of MANET is one of the important features for its deployment. In our thesis we have analyzed the behavior and challenges of security threats in mobile ad hoc networks with solution finding technique. In this paper, we have studied the routing security issues of MANETs, described the black hole attack that can be mounted against a MANET, and proposed a feasible solution for it on the top of AODV protocol to avoid the black hole attack, and also prevented the

network from further malicious behavior. Proposed method can be used to find the secured routes and prevent the black hole nodes in the MANET by identifying the node with their sequence number; check is made for whether there is large difference between the sequence number of source node or intermediate node who has sent back RREP or not? Our solution presents good performance in terms of packet ratio and minimum packet end-to-end delay and throughput.

As future work, research work intend to develop simulations to analyze the performance of the proposed solution based on the various security parameters like mean delay time, packet overhead, memory usage, mobility, increasing number of malicious node, increasing number of nodes and scope of the black hole nodes and also focusing on resolving the problem of multiple attacks against AODV. The problem in proposed solution is that a malicious node can play a role of SN collector in order to get the SN of as many other nodes as possible by broadcasting RREQs with high frequency to different nodes in a MANET so that this collector always keeps the freshest SN of other nodes. Therefore, how to solve this problem is our next issue.

## 8. REFERENCES

- [1] Mohammad AL-Shurman, Seon-Moo Yoo and Seungjin Park, "Black Hole Attack in Mobile Ad Hoc Networks" ACMSE'04, April 2-3, 2004, Huntsville, AL, USA.
- [2] Y.-C. Hu, D. B. Johnson, and A. Perrig, "Sead: Secure efficient distance vector routing for mobile wireless ad-hoc networks," in *WMCSA '02: Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and Applications*. Washington, DC, USA: IEEE Computer Society, 2002, pp. 3–13.
- [3] X. Wang, T. liang Lin, and J. Wong, "Feature Selection in Intrusion Detection System over Mobile Ad-hoc Network", *Technical Report, Computer Science*, Iowa State University, 2005.

- [4] Y.-C. Hu, D. B. Johnson, and A. Perrig, "Sead: Secure efficient distance vector routing for mobile wireless ad-hoc networks," in *WMCSA '02: Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and Applications*. Washington, DC, USA: IEEE Computer Society, 2002, pp. 3–13.
- [5] S. Kurosawa, H. Nakayama, and N. Kato, "Detecting black hole attack on AODV based mobile ad-hoc networks by dynamic learning method," *International Journal of Network Security*, pp. 338–346, 2007.
- [6] Q. He, D. Wu, and P. Khosla, "Sori: A secure and objective reputationbased incentive scheme for ad-hoc networks," *Wireless Communications and Networking Conference, 2004. WCNC. 2004 IEEE*, vol. 2, pp. 825–830, 21-25 March 2004.
- [7] Y. F. Alem & Z. H. X. "Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection" by from Tainjin 300222, China 2010, IEEE
- [8] "An Adaptive Approach to Detecting Black Hole Attacks in Ad Hoc Network" 2010 24th IEEE International Conference.
- [9] S. Sreepathi, V. Venigalla, and A. Lal, A Survey Paper on "Security Issues Pertaining to Ad-Hoc Networks". [www4.ncsu.edu/~sssreepa/Adhoc-networks-Security-Survey.doc](http://www4.ncsu.edu/~sssreepa/Adhoc-networks-Security-Survey.doc).
- [10] H. Deng, Wei Li, and D. P. Agrawal, "Routing Security in Wireless Ad Hoc Network," *IEEE Communications Magazine*, vol. 40, no. 10, October 2002.
- [11] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard, "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks", 2003 International Conference on Wireless Networks (ICWN'03), Las Vegas, Nevada, USA.
- [12] L. Tamilselvan, V. Sankaranarayanan: "Prevention of Black Hole Attack in MANET", the 2nd international conference on wireless, Broadband and Ultra Wideband Communications (January 2007)
- [13] P. K. Sehgal & R. Nath, "A Encryption Based Dynamic and Secure Routing Protocol for Mobile Ad Hoc Network", *International Journal of Computer Science and Security (IJCSS)*, Volume (3) : Issue (1) 16
- [14] A.Patcha and A.Mishra, Collaborative security architecture for black hole attack prevention in mobile ad hoc networks, Radio and Wireless Conference, 2003. RAWCON '03, Proceedings, pp. 75-78, 10-13 Aug. 2003.
- [15] H. Weerasinghe. "Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation", IEEE Student Member
- [16] S. Dokurer, Y. M. Erten, Can Erkin Acar "Performance analysis of ad-hoc networks under black hole attacks", Turkey.
- [17] M. Al-Shurrnan et al: "Black Hole Attack in Mobile Ad Hoc Network", ACMSE' 04, (April 2004).
- [18] S. Lu, Longxuan Li, K. Yan, L. Jia "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack", 2009 International Conference.
- [19] Y. R. Tsai and S. J. Wang, "Two-tier authentication for cluster and individual sets in mobile ad-hoc networks," *Comput. Netw.*, vol. 51, no. 3, pp. 883–900, 2007.
- [20] M. Deb, "A Cooperative Black hole Node Detection Mechanism for ADHOC Networks", Proceedings of the World Congress on Engineering and Computer Science, 2008.
- [21] M.Parsons and P.Ebinger, "Performance Evaluation of the Impact of Attacks on mobile ad hoc networks".
- [22] D.B.Roy, R.Chaki and N.Chaki, "A New Cluster-Based Wormhole Intrusion Detection Algorithm for Mobile Ad Hoc Networks," *International Journal of Network Security and Its Application (IJNSA)*, Vol. 1, No.1, April, 2009.
- [23] N.Shanti, Lganesan and K.Ramar, "Study of Different Attacks On Multicast Mobile Ad Hoc Network".
- [24] The Network simulator ns-2 Project web page available at <http://www.isi.edu/nsnam/ns/>.