ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, Issue 4, April 2013

A STUDY OF DIFFERENT ATTACKS IN MANET AND DISCUSSION ABOUT SOLUTIONS OF BLACK HOLE ATTACK ON AODV PROTOCOL

Er.Kiran Narang, Sonal

***Abstract*— MANET are gaining popularity now days due to flexibility and communication without the infrastructure or centralized access point. The dynamic changing nature of network topology makes any node in MANET to leave and join the network at any point of time. From a security design perspective, MANETs have no clear line of defense; i.e. no in -bulit security. Thus MANET is accessible to both legitimate network users and malicious attackers. There are many routing attacks caused due to lack of security .The one of most suitable protocol is AODV for Ad-hoc networks and it is vulnerable to black hole attack by malicious nodes. It is similar to the black hole in the universe in which things disappear. The Black hole attack is that where a malicious node advertises itself as it is having the optimal route to the destination by sending RREP message with highest sequence number and minimum hop count.In this paper, a review of different types of attacks and existing solutions to detect black hole attack and their demerits.**

.

***IndexTerms*-Black hole attack, DRI, DPRAODV, IDAD**

I. INTRODUCTION

Mobile Ad hoc NETworks (MANET)[1] are the wireless networks of mobile computing devices without the required intervention of any existing infrastructure or centralized access point such as a base station. The mobile nodes in a MANET self organize together in some arbitrary fashion. A MANET is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. These networks can be applied between persons or between vehicles in areas which are depleted of fixed infrastructure. Two nodes can directly communicate with each other if they are within the radio range. If the nodes are not within the radio range they can communicate with each other using multihop routing. The

wireless link between the nodes in mobile networks is highly vulnerable. This is because nodes can continuously move causing the frequent breakage of the link. The power available for transmission is also strictly limited.. The topology of the network is highly dynamic due to the continuous breakage and establishment of wireless link. Nodes continuously move into and out of the radio range. This gives rise to the change in routing information. MANETS need energy - efficient operation because all the nodes depend on battery power which is highly limited. The network is decentralized, where all network activity including discovering the topology and delivering messages must be executed by the nodes themselves, i.e., routing functionality will be incorporated into mobile nodes. MANET has become popular in several application areas, including when a group of soldiers in enemy territory need to communicate through their available devices to receive a command or report their situations. Emergency operations like search and rescue, commando operations, security scenarios, and collaborative research group are other examples of applications using MANET. In most of these applications security is very important however each of them needs a different level of security.Advantages of MANET are it can be set up in any place and time .They provide access to sevices and information in any geographic areas. Disadvantages of MANET are limited resources leads to limited security and its time varying topology makes it hard to detect the malicious node.

The routing protocols are mainly categorized into proactive routing protocols an reactive routing protocols. Proactive routing protocol, every node maintains one or more tables representing the entire topology of the network. These tables are updated regularly in order to maintain a up-to-date routing information from each node to every other node and establish a route to the destination node. DSDV (Destination Sequence Distance Vector) and OLSR (Optimized Link State Routing Protocol) are two popular proactive routing protocols for MANETs.[2]

Reactive protocols[2] seek to set up routes on-demand. If a node wants to initiate communication with a node to which it has no route, the routing protocol will try to establish such a route. It is also called on demand routing protocol. hoc On-Demand DistanceVector(AODV) or Dynamic Source Routing(DSR).

Manuscript received April, 2013.
Kiran Narang, Department of Computer science, Hindu college of Engineering, Sonepat, India.
Sonal, Department of Computer science, Hindu college of Engineering, Sonepat, India.

II. AODV ROUTING PROTOCOL-OVERVIEW

The Ad-hoc On-Demand Distance Vector (AODV) is a reactive routing protocol designed for ad hoc mobile networks where nodes can enter and leave the network at will. AODV is capable of both unicast and multicast routing. It finds a route to a destination when a source node likes to transfer a packet to that destination. Routes are maintained by the source node as long as they needed. AODV uses several control packets like route request packet (RREQ) is broadcasted by a node requiring a route to another node, routing reply message (RREP) is unicasted back to the source of RREQ, and route error message (RERR) is sent to notify other nodes of the loss of the link. HELLO messages are used to find active neighbors. Sequence numbers are used to find the freshness of routes towards the destination. AODV builds routes using a route request / route reply query cycle. When a source node desires a route to a destination for which it does not already have a route, it broadcasts a route request (RREQ) packet across the network. Nodes receiving this packet update their information for the source node and set up backwards pointers to the source node in the route tables. In addition to the source node's IP address, current sequence number, and broadcast ID, the RREQ also contains the most recent sequence number for the destination of which the source node is aware. A node receiving the RREQ may send a route reply (RREP) if it is either the destination or if it has a route to the destination with corresponding sequence number greater than or equal to that contained in the RREQ. If this is the case, it unicasts a RREP back to the source. Otherwise, it rebroadcasts the RREQ. Nodes keep track of the RREQ's source IP address and broadcast ID. If they receive a RREQ which they have already processed, they discard the RREQ and do not forward it. As the RREP propagates back to the source, nodes set up forward pointers to the destination. Once the source node receives the RREP, it may begin to forward data packets to the destination. If the source later receives a RREP containing a greater sequence number or contains the same sequence number with a smaller hop count, it may update its routing information for that destination and begin using the better route. As long as the route remains active, it will continue to be maintained. A route is considered active as long as there are data packets periodically travelling from the source to the destination along that path. Once the source stops sending data packets, the links will time out and eventually be deleted from the intermediate node routing tables. If a link break occurs while the route is active, the node upstream of the break propagates a route error (RERR) message to the source node to inform it of the now unreachable destination(s). After receiving the RERR, if the source node still desires the route, it can reinitiate route discovery AODV protocol never produces routing loops by proving that a combination of sequence numbers and hop counts is monotonic along a route.

III. ATTACKS IN MANET

The security issues of MANETs[3] are more challenging in a multicasting environment with multiple senders and receivers. There are different kinds of attacks by malicious nodes that can harm a network and that make the communication unreliable.These attacks can be classified as active and passive attacks.. An active attack disrupts the normal operation of a network by modifying the packets in the network. Active attack can be further classified as internal and external attacks. External attacks are carried out by nodes that do not have part of the network. Internal attacks are formed by nodes that are in communication. A passive attack is one in which the information is intercepted by an attacker without disrupting the network activity. Attacks in manet are as follows:

A. Worm hole Attack

In wormhole attack,[6] the malicious nodes pretends to provide the shortest path between the two distant nodes. If the source node sends packet to destination node, a malicious node receives packets at one location in the network and tunnels them to another location in the network, the packets sent via this route are either dropped or keep on revolving but don't reach to their exact destination This tunnel between two colluding attackers is referred to as wormhole.

B. Byzantine Attack

A compromised intermediate node works alone,or a set of compromised intermediate nodes work in collusion and caary out attacks. These attacker node creates routing loops and forwarding packets through non- optimal paths or selectively dropping packets ,which results in distruption or degradation of routing services.

C. Black hole Attack

Black hole node[4] acts like black hole in the universe. In this attack black hole node absorbs all the traffic towards itself and doesn't forward to other nodes. Whenever, source node wants to send packet to the destination node. To attract all the packet towards it, this malicious node advertise that it has shortest path through it to the destination node.It will send minimum number of hops count and latest sequence number. Then all nodes send the data packet to this node and it wiil not forward to datapacket to any node .Drops the packets by sending false route reply messages to the route request.

D. Rushing Attack

Rushing attacks[5] are mainly against the on-demand routing protocols. These types of attacks change the route discovery process. On-demand routing protocols that use duplicate suppression during the route discovery process are vulnerable to this attack. When compromised node receives a route request packet from the source node, it floods the packet quickly throughout the network before other nodes, which also receive the same route request packet can react. Quickly forwards the control messages to gain access to the network.

E. Sinkhole Attack*:*

Sinkhole attack is one of the severe attacks in wireless Ad hoc network. In sinkhole Attack, a compromised node or malicious node advertises wrong routing information to produce itself as a specific node and receives whole network traffic. After receiving whole network traffic it modifies the secret information, such as changes made to data packet or drops them to make the network complicated. A malicious node tries to attract the secure data from all neighboring nodes.

F. Replay Attacks

In MANETs, the topology is not fixed; it changes frequently due to mobility of nodes. In this type of attack malicious node record control messages of other nodes and resends them later. This is carried out either by the originator or by an adversary who intercepts the data and retransmits it. These replay attacks [7] are later misused to disturb the routing operation in a MANETs.

G. Link Withholding & Link Spoofing Attacks

In link withholding attack, the malicious node does not broadcast any information about the links to specific nodes. It results in losing the links between nodes. In Link spoofing [7]attacks, a malicious node broadcasts or advertises the fake route information to disrupt the routing operation. It results in, malicious node manipulate the data or routing traffic.

H. Resource Consumption Attack

In this attack, an attacker node tries to consume or waste away resources like Battery power , Band width Computational power of the other nodes present in the network by requesting excessive route discovery, or by forwarding unnecessary packets to the victim. These types of attacks are also known as sleep deprivation attack and mainly occur against the devices that don't offer any services to the network.

I. Sybil Attack

In Sybil attack[5], Sybil attacker may generate false identities of number of additional nodes. In this, a malicious node produces itself as a large number of nodes instead of single node. The additional identities that the node acquires are called Sybil nodes. A Sybil node may fabricate a new identity for itself or it steals an identity of the legitimate node.

IV. BLACK HOLE ATTACK ON AODV PROTOCOL

To perform black hole attack, malicious node waits for RREQ messages from neighboring nodes. When the malicious node receives an RREQ message, immediately sends a fake RREP message with a latest sequence number and minimum hop count without checking its routing table to make an entry in the routing table of the source node, before other nodes replies to absorb transmitted data from source to that destination and drop them instead of forwarding. A blackhole has two properties. First, the node exploits the ad ho routing protocol, such as AODV, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting packets. Second, the node consumes the intercepted packets. Black hole attacks in AODV protocol routing level can be classified into two categories: RREQ Black hole attack and RREP Black hole attack.

A. Black hole attack caused by RREQ

An malicious node can send fake RREQ messages to form Black hole attack. In RREQ Blackhole attack, the malicious node pretends to broadcast a RREQ message with a non-existent node address. Other nodes will update their route to pass by the non-existent node to the destination node. As a result, the normal route will be broken down. The attacker can generate Blackhole attack by faked RREQ message as follows:

- Set the type field to RREQ (1)
- Set the originator IP address in RREQ to the originating node" s IP address.
- Set the destination IP address of IP header to broadcast address.
- Set the source IP address (in the IP header) to a non-existent IP address (Blackhole)..
- Set the source IP address of IP header to its own IP address .
- Increase the source sequence number by at least one, or decrease the hop count to 1 in RREQ field.

B. Blackhole attack caused by RREP

The malicious node unicasts the false RREP message to the originating node. When originating node receives the false RREP message, it will update its route to destination node through the non-existent node. Then RREP Blackhole is formed.

- Set the type field to RREP (2)
- Set the hop count field to 1
- Set the originator IP address in RREP to the originating nodes' IP address
- Set the destination IP address in RREP to the destination node's IP address.
- Set the source IP address (in the IP header) to a non-existent IP address (Blackhole).
- Increase the destination sequence number by at least One.

V. SOLUTIONS TO DETECT BLACK HOLE ATTACK IN MANET

1. DRI Table and Cross Checking Scheme

Hesiri Weerasinghe et al.[8][9] proposed an algorithm to identify Collaborative Black Hole Attack. He introduces the use of DRI (Data Routing Information) to keep information regarding past routing experience among mobile nodes in the network and crosschecking of RREP messages from intermediate nodes by source nodes.In this the AODV routing protocol is slightly modified by adding an additional table i.e. Data Routing Information (DRI) table and cross checking using Further Request (FREQ) and Further Reply (FREP). Data Routing Information (DRI) table contains two values 1 for true and 0 for false. The entry is composed of two bits, From and Through which stands for information on routing data packet from the node and through the node respectively.1 implies that when there is path between the source node and destination and 0 impiles that when there is no path between them. The procedure of proposed solution is simply described as below. The source node (SN) sends RREQ to each node, and sends packets to the node which replies the RREP packet. The intermediate node (IN) transmits next hop node (NHN) and DRI table to the SN, then the SN cross

checks its own table and the received DRI table to determine the INs honesty. After that, SN sends the further request to INs NHN for asking its routing information, including the current NHN, the NHNs DRI table and its own DRI table. Finally, the SN compares the above information by cross checking to judge the malicious nodes in the routing path.The procedure of proposed solution is simply described as below 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 same as in the AODV. 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. If the destination replies, all intermediate nodes update or insert routing entry for that destination since we always trust destination. The intermediate node (IN) transmits next hop node (NHN) and DRI table to the SN, then the SN cross checks its own table and the received DRI table to determine the INs honesty. After that, SN sends the further request to INs NHN for asking its routing information, including the current NHN, the NHNs DRI table and its own DRI table. Finally, the SN compares the above information by cross checking to judge the malicious nodes in the routing path. Disadvantages of this method is an additional table is needed for every node and crosschecking process is time consuming.

2. Detection, Prevention and Reactive AODV (DPRAODV) Scheme

In DPRAODV a new control packet called ALARM is used in DPRAODV, while other main concepts are the dynamic threshold value .An extra check is done to find whether the RREP_seq_no value is higher than the threshold value as compared to normal AODV. If the RREP_seq_no value is higher than the threshold value, the node is considered to be malicious and that node is added to the black list. As the node detects a malicious node, it sends an ALARM packet to its neighbors. This ALARM packet has black listed node as a parameter. Later, if any other node receives the RREP packet it checks the black list. If that node is black listed, it simply ignores it and does not receive reply from that node again. . According to this scheme, the black hole attacks not only be detected but also prevented by updating threshold which responses the realistic network environment. Advantages of this method is simplicity. Disadvantages of DPRAODV simply detects multiple black holes rather than cooperative black hole attack. This method may also make mistake when a node is not malicious, but according to its higher sequence number may be entered into blocked list. • This process takes a considerable amount of time to notify all nodes for a large network in addition to the network overhead that can be caused by ALARM broadcast[10].

.

3. Sequence Number Comparison

Lalit Himral et al [16] have proposed method to find the secured routes and prevent the black hole nodes (malicious node) in the MANET by checking whether there is large difference between the sequence number of source node or intermediate node who has sent back first 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 RR-Table. Then compare the first destination sequence number with the source node sequence number, if there exists much more differences between them, surely it is from the malicious node, immediately remove that entry from the RR-Table. Destination Sequence Number is a 32-bit integer associated with every route and is used to decide the freshness of a particular route. The larger the sequence number, the fresher is the route. This solution may be used to maintain the identity of the malicious node as MN-Id, so that in future, it can discard any control messages coming from that node.This method cannot find multiple black hole nodes.

4. Trust Table Method

Yaser khamayseh et.al.[11] proposed protocol and modifies the behavior of the original AODV by introducing a data structure referred as trust table at every node. This table is responsible for holding the addresses of the reliable nodes. The RREP is extended with an extra field called trust field. In order for a node to be added to the trust table of another node, it needs firstly to pass the behavioral analysis filter. Once the behavior of the broadcasting node is normal, it is added to the trust table of the receiving node. RREP is overloaded with an extra field to indicate the reliability of the replying node. The value of the trust field is initialized to zero by the replying node and might be modified by its previous hop during the trip of the RREP. The value of the trust field could be modified either to 2 if the replying node is the destination itself or to 1 if the replying node is not the destination but still exist in the trust table. Upon the RREP is received by the source node, it decides whether to send the data or to wait for further route. In case the trust field value equals to 1 or 2, the source node sends, otherwise the source node waits for further route. Although the proposed method gives reliable routes but it consumes high network delay

5. Redundant Route Method and Sequence Number Solution

Al-Shurman et.al. [12] have proposed two solutions designed to target on black hole attacks on AODV protocol. The first proposed solution is to find more than one route to the destination. Source node unicasts a RREQ (ping) packet to the destination node. The receiver and the malicious in addition to intermediate node will reply RREP message to this RREQ packet. The source node receives an acknowledgement RREP message from different routes and it will check to find the safe routes transmit the buffered packets. It represents that there are at least two routing paths

existing at the same time. After that, the source node identifies the safe route by counting the number of hops or nodes and thus prevents black hole attacks. In the second solution,unique sequence number is used. The sequence value is aggregated; hence it's ever higher than the current sequence number. In this technique, two values are recorded in two additional tables.To find the malicious node, each node needs to maintain two tables to store sequence numbers of last packet sent to every node and last packet received from every sender respectively and compare the last sequence number which is extracted from RREP at source node. Whenever a packet are transmitted or received, these two table values are updated automatically. Using these two table values, the sender can analyze whether there is malicious nodes in network or not.if it matches, data will be forwarded to that route otherwise an alarm message is broadcasted to isolate the malicious node in the network. . Second technique is considered to be good compared to first technique because of the sequence number which is included to every packet contained in the original routing protocol. If it However, the two solutions has time delay as the drawback and both the solution is not for cooperative black hole attacks.

6. Time-based Threshold Detection Scheme
Tamilselvan L et al. [13]proposed a solution based on an enhancement of the original AODV routing protocol. The source node has to wait for other replies with next hop information without sending the data packets to the destination. The major concept is setting timer for collecting the other request from other nodes after receiving the first request. It sets timer in the "TimerExpiredTable" , to collect the further RREP" s from different nodes are stored in "Collect Route Reply Table" (CRRT) with the "sequence number" , and the time at which the packet arrives.The route validity is checked based on the arrival time of the first request and the threshold value.

7. Fidelity Table Concept
Latha Tamilselvan, Dr. V Sankaranarayanan in their.paper about Prevention of Co-operative Black Hole Attack in MANET gave a approach to combat the Black hole attack. In MANET, the absence of a fixed infrastructure, thus nodes have to cooperate in order to provide the necessary network functionality. One of the principal routing protocols used in Ad-hoc networks is AODV (Ad hoc on demand Distance vec--tor) protocol. The security of the AODV protocol is compromised by a particular type of attack called 'Black Hole' attack .In this attack a malicious node advertises itself as having the shortest path to the node whose packets it wants to intercept. To reduce the probability it is proposed to wait and check the replies from all the neighboring nodes to find a safe route. Their approach to combat the Black hole attack is to make use of a 'Fidelity Table' wherein every participating node will be assigned a fidelity level that acts as a measure of reliability of that node. In case the level of any node drops to 0, it is considered to be amalicious node,termed as a 'Black hole' and is eliminated .The percentage of packets received through our system is better than that in AODV in presence of cooperative black hole attack.[14]

8 . Intrusion Detection using Anomaly Detection (IDAD)
In authors Alem, Y.F et al [15]. proposed a solution based on Intrusion Detection using Anomaly Detection (IDAD) to prevent attacks by the both single and multiple black hole nodes. IDAD assumes every activity of a user can be monitored and anomaly activities of an attacker can be identified from normal activities. To find a black hole node IDAD needs to be provided with a precollected set of anomaly activities, called audit data. Once audit data collected and it is given to the IDAD system, which is able to compare every activity with audit data. If any activity of a node is out of the activity listed in the audit data, the IDAD system isolates the particular node from the network. Advantage is reduction of the number of routing packets in turn minimizes network overhead and facilitates a faster communication. Another advantage is to avoid false positive alarms of intrusion detection, this technique checks multiple anomaly conditions. Disadvantages of IDAD is that Neighbour nodes may give false information

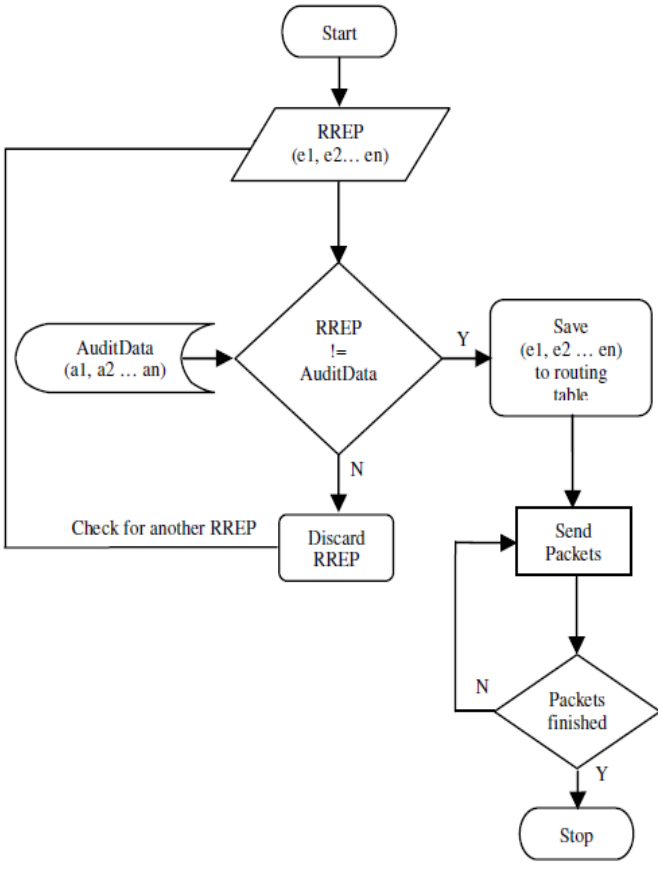

Figure1" Flowchart of Intrusion Detection by IDAD"

VI. CONCLUSION

In this paper an overview of MANET is been presented first. After it we define AODV protocol and different types of attack in MANET.This paper has amalgamated various solutions to detect Black hole attack in AODV-based MANETs and their disadvantages . For future work, to find an effective solution to the black hole attack on AODV protocol.

ACKNOWLEDGMENT

I would like to give my sincere gratitude to my guide Kiran Narang who guided me throughout, to complete this topic.

.

REFERENCES

[1] RFC 2501, http://www.faqs.org/rfcs/rfc2501.html.
[2] M.Saravana karthikeyan, K.Angayarkanni , and Dr.S.Sujatha,“ Throughput Enhancement in Scalable MANETs using Proactive And Reactive Routing Protocols”, Proceedings of International Multiconference of engineers and computer scientists, Vol2, Hong Kong, March17-19, 2010.
[3] Rashid Sheikhl Mahakal Singh Chande,” Security Issues in MANET: A Review” 978-1-4244-7202-4/10/$26.00 ©2010 IEEE
[4] Govind Sharma, Manish Gupta” Black Hole Detection in MANET Using AODV Routing Protocol”, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volu me-1, Issue-6, January 2012 297
[5] Mangesh M Ghonge, Pradeep M Jawandhiya,” Countermeasures of Network Layer Attacks in MANETs” IJCA Special Issue on “Network Security and Cryptography” NSC, 2011
[6] Yih-Chun Hu, *Member, IEEE* Adrian Perrig, *Member, IEEE*, and David B. Johnson “Wormhole Attacks in Wireless Networks”, IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 24, NO. 2, FEBRUARY 2006
[7] Abhay Kumar Rai, Rajiv Ranjan Tewari & Saurabh Kant Upadhyay, “Different Types of Attacks on Integrated MANET-Internet Communication”, International Journal of Computer Science and Security (IJCSS) Volume (4): Issue (3) 265
[8] Hesiri Weerasinghe and Huirong Fu, “Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation”, Intenation Journal of Software Engineering and its Application, Vol.2, Issue 3, July 2008.
[9] Ramaswamy S, Fu H, Sreekantaradhya M, Dixon J, Nygard K, “ Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks”, Paper presented at the International Conference on Wireless Networks, Las Vegas, Nevada, USA, 23-26 June 2003
[10] Payal N. Raj1 and Prashant B. Swadas2, “DPRAODV: A Dynamic Learning System against Blackhole Attack in AODV based MANET”, IJCSI International Journal of Computer Science Issues, Vol. 2, 2009
[11] Yaser khamayseh, Abdulraheem Bader, Wail Mardini, and Muneer BaniYasein, “A New Protocol for Detecting Black Hole Nodes in Ad Hoc Networks”, International Journal of Communication Networks and Information Security (IJCNIS) Vol. 3, No. 1, April 2011.
[12] Al-Shurman, M., Yoo, S. and Park, S, "Black hole Attack in Mobile Ad Hoc Networks", ACM Southeast Regional Conference, pp. 96-97, 2004.
[13] Tamilselvan, L.; Sankaranarayanan, V., "Prevention of Blackhole Attack in MANET," Wireless Broadband and Ultra Wideband Communications, 2007. Aus Wireless 2007. The 2nd International Conference on, vol., no., pp.21, 27-30 Aug. 2007
[14] Latha Tamilselvan “Prevention of Co-operative Black Hole Attack in MANET” JOURNAL OF NETWORKS, VOL. 3, NO. 5, MAY 2008.
[15] Alem, Y.F.; Zhao Cheng Xuan; , "Preventing black hole attack in mobile ad-hoc networks using Anomaly Detection," Future Computer and Communication (ICFCC), 2010 2nd International Conference, vol.3, no., pp.V3-672-V3-676, 21-24 May 2010
[16] Lalit Himral, Vishal Vig, Nagesh Chand, “Preventing AODV Routing Protocol from Black Hole Attack” International Journal of Engineering Science and Technology (IJEST) Vol. 3 No. 5 May. 2011

Er.Kiran Narang is presently working as Assistant Professor in Hindu College of Engineering,Sonepat. She posses qualifications of B.Tech, M.Tech. she has been published many papers in National/ International journals and holds a teaching experience of approximate 10 years. Her research areas are in Wireless Networks, Computer Architecture and Data Structure.

Ms.Sonal has completed her B.Tech degree in Computer Science from Maharishi Dayanand University, Rohtak in year 2011. She is pursuing Hindu College of Engineering ,Sonepat from 2011. Her research interests are in Mobile ad hoc networks and computer networks.