Comparative study of Attacks on AODV-based Mobile Ad Hoc Networks

Ipsa De
Calcutta Institute of Engineering and Management
India

Debdutta Barman Roy
Calcutta Institute of Engineering and Management
India

Abstract: ***In recent years, the use of mobile ad hoc networks (MANETs) has been widespread in many applications, The lack of infrastructures in MANETs makes the detection and control of security hazards all the more difficult. The security issue is becoming a major concern and bottle neck in the application of MANET. In this paper, an attempt has been made to thoroughly study the blackhole attack which is one of the possible attacks in ad hoc networks in routing protocol AODV with possible solution to blackhole attack detection.***

Keywords: MANET, black hole, security, AODV

I INTRODUCTION

A mobile ad hoc network (MANET) is a self-configuring network that is formed automatically by a collection of mobile nodes without the help of a fixed infrastructure or centralized management. Each node is equipped with a wireless transmitter and receiver, which allow it to communicate with other nodes in its radio communication range. In order for a node to forward a packet to a node that is out of its radio range, the cooperation of other nodes in the network is needed; this is known as multi-hop communication. Therefore, each node
must act as both a host and a router at the same time. The network topology frequently changes due to the mobility of mobile nodes as they move within, move into, or move out of the network.

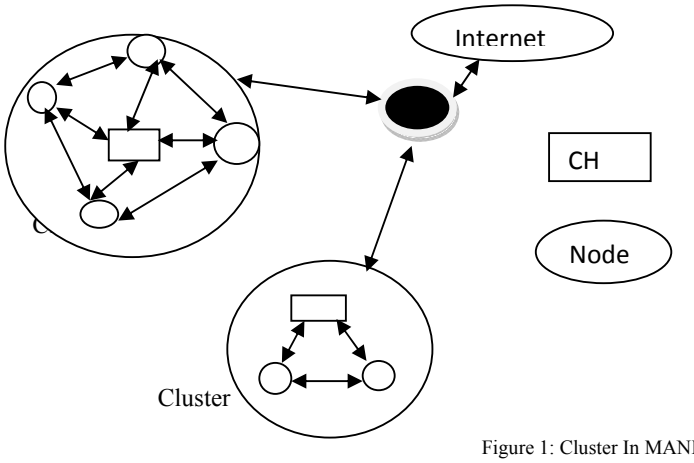


Figure 1: Cluster In MANET

A MANET with the characteristics described above was originally developed for military purposes, as nodes are scattered across a battlefield and there is no infrastructure to help them form a network. In recent years, MANETs have been developing rapidly and are increasingly being used in many applications, ranging from military to civilian and commercial uses, since setting up such networks can be done without the help of any infrastructure or interaction with a human. Some examples are: search-and-rescue missions, data collection, and virtual classrooms and conferences where laptops, PDA or other mobile devices share wireless medium and communicate to each other.

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

II RELATED WORK

The security problems in MANETS may raise the possibility of multiple security attacks. The possible security attacks in MANETs can be divided into two categories:

• *Route Logic Compromise:* Incorrect routing control messages are injected into the network to damage routing logic. The following may be the techniques:

- *Cache poisoning:* - Information in routing table is either modified, deleted or injection with false information.
- *Routing Table Overflow*: This is done by sending unnecessary and fake route advertisements.

• *Traffic Distortion Attack:* All attacks that prohibit data packets to transfer from the source to the destination, either selectively or collectively comes under the category of Traffic Distortion Attack. It can be done by packet modification, including fake routing message (RREQ, RREP) etc.

A. The common attacks in MANETs are discussed as under

Jamming: If attacker has a powerful transmitter, he/she can generate a radio signal strong enough to overwhelm weaker signals, disrupting communications. This condition is called jamming.

Snooping: Due to broadcast nature of radio signals from transmitter, it is possible to eavesdrop the packets. Due to inherent trust between mobile nodes, they are allowed to look at the whole packet data. Two types of information can be obtained from snooping:

• *Packet Payload data:* The actual data that the packets are carrying can be revealed if proper encryptions are not used.

• *Routing information:* The source and destination information from the packets may reveal the nature of communication & relationship between them.

Flood Storm Attack: Malicious node deliberately floods the whole network with meaningless Route Request (RREQ) and Route Reply (RREP) messages. So it can paralyze the network by destroying its routing logic.

Packet Modifications (Tampering): It is possible for intermediate nodes to modify the packet content, if proper integrity checks are not maintained. Also it is possible to change the header information including source and destination address.

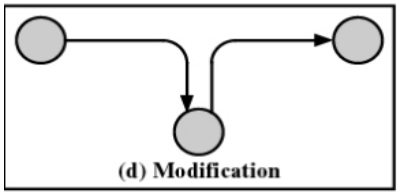


Figure 2: Packet Modification

Packet Dropping (Denial of service): A node is prevented from receiving and sending data packets to its Destination

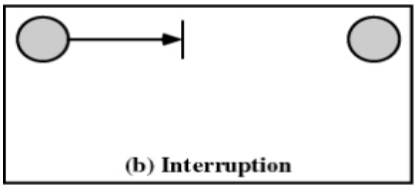


Figure 3: Packet Dropping

Repeater attack In this attack, a malicious node simply replays packets of one of its neighbor A. This will result in other side neighbor (say one of them is B) assuming that the A is its neighbor, in fact it is not. Two nodes are

said to be neighbor if they are in transmission range of each other. Now the malicious node I can selectively replay packets between A and B, while dropping other packets. This would cause a Denial of Service for the nodes A and B.

Blackhole Attack: All traffic is forward to a specific node which may not forward any traffic at all. Such malicious node also advertises itself as having shortest path to requested node and blackhole drops all data packet.

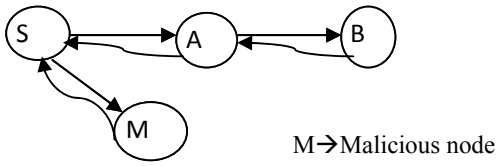


Figure 4: BlackHole Attack

Grey hole: Similar to the above case but only data packets are dropped and not all.

Routing loop: A loop is introduced in route path.

Network partition: A connection network is subdivided into k (k>=2) sub-network where no link present between them.

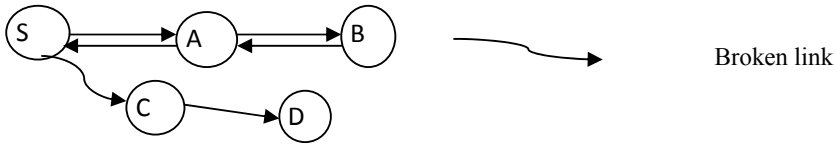


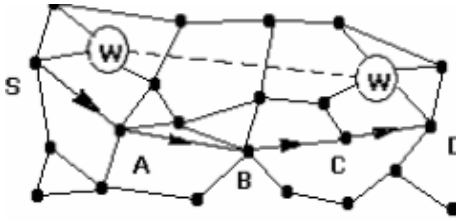
Figure 5: Network Partitioning Attack

Selfishness: A node is not serving as a relay to other nodes.
Sleep Deprivation: A node is forced to exhaust its battery power.
Location Disclosure: Topology of the network or geographical location of a node is disclosed along with its neighbors.
Detour Attack: Delaying in packet forwarding so that a packet may not be able to meet end-to-end delay or jitter requirement in packet transmission. As a result such a node will not be chosen to forward packets.
Back-off Attack: Packets are sent in such a way that packet transmission is hampered by collision.

Figure 6: Back off Attack

Time-out Attack: A node maliciously forces the forwarding operation to fail in order to either disrupt the route discovery process or cause damage to the existing flows routed through it.

Wormhole attack: - A tunnel is created between two nodes that can be utilized to secretly transmit packets.



W----W indicates Wormhole tunnel

Figure 7: Wormhole Attack

Rushing attack: In rushing attack, a malicious node wants a route to be established through it. [2][3]

III. ROUTING PROTOCOLS

A. TYPES OF ROUTING PROTOCOL

There are different types Routing algorithms. One common classification is as follows

1. Proactive (table driven) routing
2. Reactive (on demand) routing

Proactive (table driven) routing: This type of protocols maintains fresh lists of destinations and their routes by periodically distributing routing tables throughout the network. As here router knows all nodes of the network so, here response is quick. But it has *large routing overhead*. E.g. Destination Sequenced Distance Vector (DSDV), Topology broadcast based on reverse path forwarding (TBRPF) and Optimized link state routing (OLSR).

Reactive (on demand) routing: This type of protocols finds a route on demand by flooding the network with Route Request packet. Here a node only knows its neighbors, so other routes are determined on demand. Routing overhead is smaller. E.g.: Ad hoc On-demand Distance Vector (AODV), Dynamic source routing (DSR) [7]

B. BREIF OVERVIEW ON ROUTING PROTOCOL AODV

Adhoc On-demand Distance Vector (AODV). is a routing protocol for (MANETs) and other wireless ad-hoc networks. It establishes a route to a destination only on demand. AODV is, as the name indicates, a distance vector routing protocol. AODV avoids the *counting-to-infinity* problem of other distance-vector protocols by using sequence numbers on route updates.

Each node has its own sequence number and this number increases when links change. Each node judges whether the channel information is new according to sequence numbers. Node S is trying to establish a connection to destination D. First, the source node S refers to the route map at the start of communication. In case where there is no route to destination node D, it sends a Route Request (RREQ) message using broadcasting. RREQ ID increases one every time node S sends a RREQ. Node A and B which have received RREQ generate and renew the route to its previous hop. They also judge if this is a repeated RREQ. If such RREQ is received, it will be discarded. If A and B has a valid route to the destination D, they send a Route Reply (RREP) message to node S. By contrast, in case where the node has no valid route, they send a RREQ using broadcasting. The exchange of route information will be repeated until a RREQ reaches at node D. When node D receives the RREQ, it sends a RREP to node S. When node S receives the RREP, then a route is established. In case a node receives multiple RREPs, it will select a RREP whose the destination sequence number (Dst Seq) is the largest amongst all previously received RREPs. But if Dst Seq were same, it will select the RREP whose hop count is the smallest.

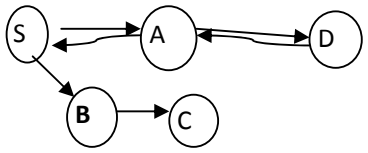


Figure 8: Route discovery process

If there is any disconnection in the route then a Route Error (RERR) message is generated and this information is sent to source. [5]

IV BLACK HOLE ATTACK

In networking, black holes refer to places in the network where incoming traffic is silently discarded (or "dropped"), without informing the source that the data did not reach its destination. These black hole nodes are invisible and can only be detected by monitoring the lost traffic. So, it is named as black hole.

A black hole attack or packet drop attack is a type of denial of service attack accomplished by dropping packets. The attack can be accomplished either selectively (e.g. by dropping packets for a particular network destination, a packet every *n* packets or every *t* seconds, or a randomly selected portion of the packets, which is called "Gray hole attack") or in bulk (by dropping all packets). [5]

Two properties of Black Hole Attack:
1. The node exploits the ad hoc routing protocol to advertise itself as having a shortest valid route to a destination node, even though the route is spurious.
2. The node consumes the intercepted packets. [4]

A. Why AODV Is Prone To Black Hole Attack.
In table driven or proactive routing protocol the total routing table is shared. So, there is no chance of on-demand request or reply messages i.e. no chance of blackhole attack. Probability of black hole attack is more in reactive algorithm. AODV and DSR are the most recognized reactive (on-demand) protocol. Here black hole attack can occur. But DSR uses source routing and in AODV, the source node and the intermediate nodes store the next-hop information corresponding to each flow for data packet transmission. So, AODV is much more prone to black hole attack as a black hole always responds positively with a RREP message to every RREQ, even though it does not really have a valid route to the destination node.
Comparative study can reveal that AODV is much more prone to black hole attack than other relevant attacks (like flooding attack or rushing attack). In fact the packet loss in blackhole attack is higher than any other attack under AODV protocol. The throughput of received packets in blackhole AODV decreases with the increase of number of Blackhole Nodes. Also the average End-to-end Delay without blackhole attack is increased as compared to the effect of blackhole attack. This is due to the immediate reply from the blackhole node owing to AODV protocol without checking its routing table. In blackhole attack, the attackers also have the option of manipulating only a fraction of RREP messages to reduce probability of detection.

B. Black Hole Attack in AODV
In AODV, Dst Seq is used to determine the freshness of routing information contained in the message from originating node. When generating a RREP message, a destination node compares its current sequence number and Dst Seq in the RREQ packet plus one, and then selects the larger one as RREP's Dst Seq. Upon receiving a number of RREP, a source node selects the one with greatest Dst Seq in order to construct a route. To succeed in the blackhole attack the attacker must generate its RREP with Dst Seq greater than the Dst Seq of the destination node. It is possible for the attacker to find out Dst Seq of the destination node from the RREQ packet. In general, the attacker can set the value of its RREP's Dst Seq base on the received RREQ's Dst Seq. However, this RREQ's Dst Seq may not present the current Dst Seq of the destination node. Figure shows an example of the blackhole attack. The value of RREQ and RREP using in the attack are shown in Table 1.

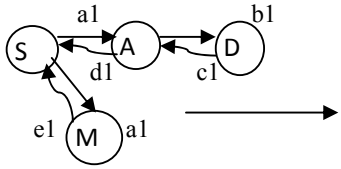


Figure 9: BlackHole Attack

Table1: Values of RREQ and RREP

	RREQ		RREP		
	a1	b1	c1	d1	e1
IP.Src	S	A	D	A	D (MD)
AODV.Dst	D		D		D (MD)
Dst Seq	60		61		65
AODV.Src	S		-		-

In Table1 IP.Src indicates the node which generates or forwards a RREQ or RREP, AODV.Dst indicates the destination node and AODV.Src indicates the source node. Here, we assume that the destination node D has no connections with other nodes. The source node S constructs a route in order to communicate with destination node D. Let the destination node D's Dst Seq that the source node S has is 60. Hence, source node S sets its RREQ (a1) and broadcasts as shown in Table. Upon receiving RREQ (a1), node A forwards RREQ (b1) since it is not the destination node. To impersonate the destination node, the attacker M sends spoofed RREP(e1) shown

in Table with IP.Src, AODV.Dst the same with D and increased Dst Seq (in this case 65 as) to source node S. At the same time, the destination node D which received RREQ (b1) sends RREP (c1) with Dst Seq incremented by one to node S. Although, the source node S receive two RREP, base on Dst Seq the RREP(e1) from the attacker M is judged to be the most recent routing information and the route to node M is established. As a result, the traffic from the source node to the destination node is deprived by node M. So, blackhole node enters into the network. [5]

V PROPOSED WORK

My objective is to find out the malicious node that performs the blackhole attack in network. We have assumed that the MANET consists of clusters of nodes. The assumptions regarding the organization of the MANET are listed in section 5.1.

In a computer system, a cluster is a group of servers and other resources that act like a single system and enable high availability and, in some cases, load balancing and parallel processing.

In computers, clustering is the use of multiple computers, typically PCs or UNIX workstations, multiple storage devices, and redundant interconnections, to form what appears to users as a single highly available system. [1]

Advantages of Clustering: The advantage of clustering computers for high availability is seen if one of these computers fails; another computer in the cluster can then assume the workload of the failed computer. Users of the system see no interruption of access.
The advantages of clustering computers for scalability include increased application performance and the support of a greater number of users.

There is a myth that to provide high availability, all that is required is to cluster one or more computer hardware solutions. To date, no hardware only solution has been able to deliver trouble-free fail-over. Providing trouble-free solutions requires extensive and complex software to be written to cope with the myriad of failure modes that are possible with two or more sets of hardware.

Disadvantages of Clustering: The disadvantage of clustering is that it takes longer to update records if only when the fields in the clustering index are changed. Another disadvantage is to recover from database corruption. Again if Cluster head becomes intruder then it is difficult to recover. [2, 4]
So, we can see that there are various advantages of forming cluster. Before moving into further details of clustering I have assumed certain assumptions. They are as follows:

A. Assumptions

The following assumptions are taken in order to design the proposed algorithm.

1. A node interacts with its 1-hop neighbors directly and with other nodes via intermediate nodes using multi-hop packet forwarding.
2. Every node has a unique id in the network, which is assigned to a new node collaboratively by existing nodes.
3. The network is considered to be layered.
4. Cluster head is not the intruder.
5. A cluster head at the inner layer is represented as CH (1,i), where 1 signifies inner Layer, and i stands for the cluster number
6. Each cluster is monitored by only one cluster head (monitoring node).
7. There is a guard node in the outer layer who monitors some cluster heads.

B Cluster Formation

In this paper, we have proposed an algorithm where intrusion detection has been done in a cluster based manner to take care of the black hole attacks. The AODV routing protocol is used as the underlying network topology. A two layer approach is used for detecting whether a node is participating in a blackhole attack. The layered approach is introduced to reduce the load of processing on each cluster heads. From security point of view, this will also reduce the risk of a cluster head being compromised.
The entire network is divided in clusters as in figure 10. The clusters may be overlapped or disjoint. Each cluster has its own cluster head and a number of nodes designated as member nodes. Member nodes pass on the information only to the cluster head. The cluster-head (CH) is responsible for passing on the aggregate information to all its members. The cluster head is elected dynamically and maintains the routing information.

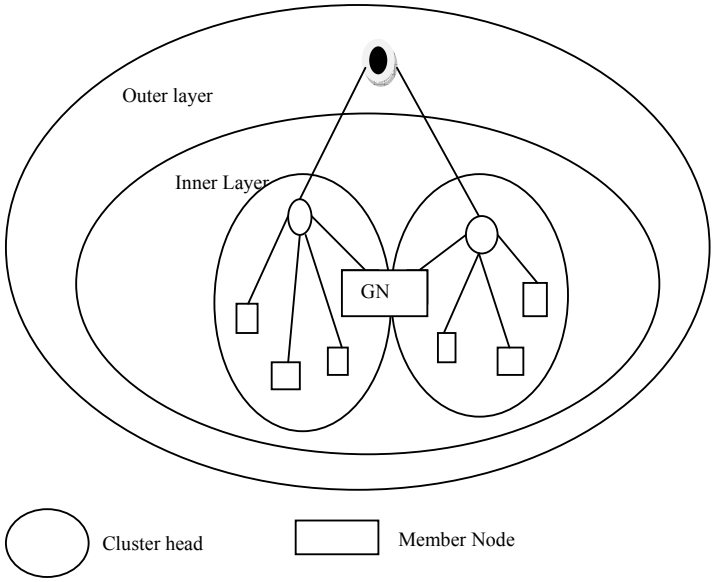


Figure 10 - The Layered structure

GN is the guard node, used for monitoring the malicious activity. The main purpose of the guard node is to guard the cluster from possible attacks. The guard node has the power to monitor the activity of any node within the cluster (cluster head also). The guard node is reported by the cluster head of the respective layer in case a malicious activity is detected. A cluster head in the inner layer (CH1, i) detects a malicious activity and informs the cluster head CH_2 of the outer layer to take appropriate action. It's the duty of (CH1, i) to check the number of false routes generated by any node. The cluster head CH_2 of outer layer takes upon itself the responsibility of informing all nodes of the inner layer about the malicious node [4]

Again if we form a cluster then it is necessary to choose a cluster head for the cluster. Cluster head can be selected in two different ways:
1. Selection method
2. Election method

C Selection Method
Here a cluster head or group leader is selected based on selection method. In selection method a single node takes initiation to form a cluster. This initiator node of the cluster makes itself cluster head. It is done by exchanging a number of requests and reply message among the selected cluster head and other node belong to that cluster. So, all nodes in a cluster should be in a transmission range. Here group leader is selected based on the transmission of confirmation message from the cluster head who initiates to make a logical cluster group. So, here cluster head is selected by itself.

D Algorithm for Cluster Head election
This algorithm is highly adaptive leader election algorithm based on finding an extreme and uses diffusing computations for this purpose. The algorithm is "Weakly Stabilizing" and "terminating". After a finite number of topological changes, every connected component will eventually select a unique leader, which is the "most valued" node from among the nodes in that component. When an election is triggered due to disconnection from its leader or value of the leader falling below some application defend threshold at a node. Several nodes start diffusing computation terminates the nodes to identify leader. In context of leader election, we observe that the choice of signaling used in the protocol accounting for broad cast nature of wireless medium. Ad hoc network is modeled as undirected graph that changes over time as mobile node moves. The graph becomes disconnected if network is partitioned. Five messages are involved in this algorithm, a) Election: It is used for "grow" spanning tree. b) ACKNOWLEDGE: It is readily sent to the neighbor node which is not the parent of a node. When the node gets "ACKNOWLEDGE" from its entire child then it sends "ACKNOWLEDGE" to parent contain leader election information. c) Leader: Once a source node for computation has received ACKNOWLEDGE from all children then sends "Leader" message to all nodes. d) Probe: this message is sent periodically by each node to its entire neighbor for knowing ex9istance of node, e) Reply: A node that get "Probe" reply with this message. The node which disconnect, does not reply. This cluster head election algorithm based on large number of

message passing which increases network traffic. For each node the ID & Value are maintained independently which makes it complex. Each variable set should be updated each time.

E Cluster Based Detection Technique of Blackhole Attack in MANET:

The terms used for blackhole detection has been described below

1. Round trip time (Tv): When the source node send packet it starts a timer. On receipt of an acknowledgement, the timer is stopped. The total time elapsed is recorded as Tr.

2. Expected time of delivery (T_e): The expected time of delivery of a packet to a destination node is calculated as the time taken when the source node send HELLO packet to the destination node and get back an acknowledgement for that.

3. Threshold tolerance (n): This refers to the threshold value defined by the monitoring node. It is the tolerance value for lost packets.

4. Neighbor table ($Neighbor_i$):Neighbor table for i^{th} node consists of {neighbor_id} for all its neighbors.

5. Number of packets sent to a destination node D from source node S.

6. Number of packets received by node D from a specific source node S. [4]

F Procedure for BlackHole Detection:

Begin
- Step 1: Initiate the network with two cluster and each cluster have some nodes.
- Step 2: The cluster head is selected based on cluster election algorithm.
- Step 3: Each node stores the information of its immediate neighbors in its neighbor table.
- Step 4: Source node S sends a HELLO packet to the intermediate node with destination node ID and cluster ID
- Step 5: S starts timer, initializes T_1
- Step 6: When S get acknowledgement from destination node stop timer, T_2
- Step 7: The expected round trip time is computed as $T_e = T_2 - T_1$
- Step 8: Source provides a unique sequence number to each packet and this number is known to Source, destination and cluster head only.
- Step 9: Source node S sends a packet to destination node
- Step 10: S starts timer TP_1
- Step 11: When S get acknowledgement from destination node stop timer, TP_2
- Step 12: The round trip time is calculated as $Tv = TP_2 - TP_1$
- Step 13: If $T_r << T_e$
  - Step 13.1: Inform cluster head
  - Step 13.2: The cluster head checks number of packet send by source node and number of packet receive by

destination node .
Step 13.3: x =no of sent packet – no of received packet
Step 13.4: If x >n then inform the source node to stop packet transfer.
Step 13.5: The source node stop packet transfer and inform the CH of outer layer to inform other clusters
Step 13.6: CH discards that path and establishes a new path.
Step 14:Else
Step 14.1: The cluster head calculates x.
Step 14.2: If x is not zero then goto Step 13.1

End. [4, 7]

VI CONCLUSION AND FUTURE WORK

In this paper the routing security issues of MANETs and different attacks in a MANET network have been studied with detail analysis of blackhole attack (prone to AODV) which is one of the most important security problems in MANET. It is an attack that a malicious node impersonates a destination node by sending forged RREP to a source node that initiates route discovery, and consequently deprives data traffic from the source node. So, all data packets move to the malicious node. The proposed solution can be applied to 1.) Identify black hole nodes in a MANET; and 2.) Discover secure paths from source to destination by avoiding black hole nodes.

As future work, it is intended to implement those possible solutions using neighborhood-based method or feature analysis of a node or any other method. The performance of the solution should also be observed in a dynamic environment.

VII .ACKNOWLEDGMENT

My Sincere thanks to my guide Ms Debdutta Pal, for providing me an opportunity to do my project work. I express my thanks to my Institution namely Calcutta Institute of Engineering & Management (CIEM) for providing me with a good environment and facilities like Internet, books, computers and all that as my source to complete this project. . My heart-felt thanks to my family, friends and colleagues who have helped me for the completion of this work.

VIII. REFERENCES

[1] A Survey on Intrusion Detection in Mobile Ad Hoc Networks, by Tiranuch Anantvalee, Department of Computer Science and Engineering Florida Atlantic University, Boca Raton, Jie Wu, Department of Computer Science and Engineering Florida Atlantic University, Boca Raton, Wireless/Mobile Network Security Y. Xiao, X. Shen, and D.-Z. Du (Eds.) pp. 170 - 196 2006 Springer

[2] Yi-an-Huang, Wenke Lee, A Cooperative Intrusion Detection System for Ad Hoc Networks 2003, ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '03) October 31, 2003, George W. Johnson Center at George Mason University, Fairfax, VA, USA

[3] State-of-the-Art Analysis of Intrusion Detection in Mobile Ad-hoc Networks Based on Feature Selection and Clustering, Debdutta Barman Roy, West Bengal University of Technology, Kolkata, West Bengal, India., and Rituparna Chaki, West Bengal University of Technology Kolkata, West Bengal, India,2007

[4] A New Cluster-Based Wormhole Intrusion Detection Algorithm for Mobile Ad-Hoc Networks by Debdutta Barman Roy(1Calcutta Institute of Engineering and Management, Kolkata, India,), Rituparna Chaki(West Bengal University of Technology, Kolkata 700064, India), Nabendu Chaki (University of Calcutta, 92 A.P.C. Road, Kolkata 700009, India), International Journal of Network Security & Its Applications (IJNSA), Vol 1, No 1, April 2009

[5] Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard, Department of Computer Science, IACC 258 North Dakota State University, Fargo, ND 58105,2010

[6] Detecting Blackhole Attack on AODV-based MANET by Dynamic Learning Method, Satoshi Kurosawa1, Hidehisa Nakayama1, Nei Kato1, Abbas Jamalipour2, and Yoshiaki Nemoto1, Graduate School of Information Sciences, Tohoku University1 Aoba 6–3–09, Aramaki, Aoba-ku, Sendai, Miyagi 980–8579, Japan. School of Electrical and Information Engineering, The University of Sydney, Sydney NSW 2006 , Australia2

[7] A Highly Secured Approach against Attacks in MANETS by G.S. Mamatha and Dr. S. C. Sharma, International Journal of Computer Theory and Engineering, Vol. 2, No. 5, October, 2010, 1793-8201 815

[8] M. Al- Shurman, S.-M. Yoo, and S. Park, "Black Hole Attack in Mobile Ad Hoc Networks," in Proceedings of the 42nd Annual ACM Southeast Regional Conference. Huntsville, AL, USA: ACM Press, Apr. 2004

[9] Performance Analysis of Flooding Attack Prevention Algorithm in MANETs by Revathi Venkataraman, M. Pushpalatha, and T. Rama Rao , World Academy of Science, Engineering and Technology 56 2009

Authors Profile:

Ipsa De is an under graduate student of Calcutta Institute of Engineering and Management, Kolkata, West Bengal. Her research interests include the field of Computer Networking, and Wireless Mobile Ad hoc Network.

Debdutta Barman Roy received her M. Tech. Degree in Software Engineering from the West Bengal University of Technology in 2007. She is at present working as a Lecturer at Calcutta Institute of Engineering and Management, Kolkata, West Bengal. Her research interests include the field of Computer Networking, and Wireless Mobile Ad hoc Network.