International Journal of Modern Engineering Research (IJMER)

www.ijmer.com Vol.2, Issue.3, May-June 2012 pp-1017-1021 ISSN: 2249-6645

# Prevention of Black Hole Attack in Mobile Ad-hoc Networks using MN-ID Broadcasting

Antony Devassy[1], K. Jayanthi[2]

*(PG scholar, ME communication Systems, SNS College of Technology, Coimbatore, India)

** (Associate professor, Department of ECE, SNS College of Technology, Coimbatore, India)

## ABSTRACT

**Black hole is a malicious node that always gives the false replay for any route request without having specified route to the destination and drops all the received packets. This can be easily employed by exploiting vulnerability of on demand routing protocol AODV. In mobile Ad hoc networks black hole attack is a severe threat which can be prevented by broadcasting the MN-ID (malicious node id) to the whole nodes in the network. The existing method identified the attacked node, retransmit the packets and again find a new route from source to destination.**

**Here the proposed method broadcast the MN-ID to the whole nodes in the network. This method prevents the black hole attack imposed by both single and multiple black hole nodes. The tool used to implement the proposed algorithm is NS2, which is an object oriented event drive software package. The result of the simulation study expected to get good network performance by minimizing the packet losses as well as effectively prevent the black hole attack against mobile Ad hoc networks.**

***Keywords*- Ad-hoc, AODV, Blackhole, MN-ID**

## 1. INTRODUCTION

A mobile ad hoc network (MANET)[5] is a collection of wireless mobile nodes which have the ability to communicate with each other without having fixed network infrastructure or any central base station. It is one of the recent active fields and has received spectacular consideration because of their self-configuration and self-maintenance. Early research assumed a friendly and cooperative environment of wireless network. As a result they focused on problems such as wireless channel access and multihop routing. Since mobile nodes are not controlled by any other controlling entity, they have unrestricted mobility and connectivity to others. Routing and network management are done cooperatively by each other nodes. Due to limited transmission power, multi hop architecture is needed for one node to communicate with another through network. In this multi hop architecture, each node works as a host and as well as a router that forwards packets for other nodes that may not be within a direct communication range. Each node participates in an ad hoc route discovery protocol which finds out multi hop routes through the mobile network between any two nodes. These infrastructure-less mobile nodes in ad hoc networks dynamically create routes among themselves to form own wireless network on the fly.

Wireless ad-hoc networks are composed of autonomous nodes that are self- managed without any infrastructure. In this way, ad-hoc networks have a dynamic topology such that nodes can easily join or leave the network at any time. Ad hoc network have many potential applications, especially, in military and rescue areas such as connecting soldiers on the battlefield or establishing a new network in place of a network which collapsed after a disaster like an earth quake. Ad-hoc networks are suitable for areas where fixed infrastructure is not possible. Since the nodes communicate with each other without an infrastructure, they provide the connectivity by forwarding packets over themselves. To support this connectivity, nodes use some routing protocols such as AODV (Ad-hoc On-Demand Distance Vector), DSR (Dynamic Source Routing) and DSDV (Destination-Sequenced Distance-Vector). Besides acting as a host, each node also acts as a router to discover a path and forward packets to the correct node in the network..In wireless ad-hoc networks lack an infrastructure and such networks are exposed to a lot of attacks. One of these attacks is the Black Hole attack.

In the Black Hole attack [2][4][7], a malicious node absorbs all data packets in itself, similar to a hole which sucks in everything in. In this way, all packets in the network are dropped. A malicious node dropping all the traffic in the network makes use of the vulnerabilities of the route discovery packets of the on demand protocols, such as AODV. Which is used for identifying a fresh route from the source to destination?

## 2. AD-HOC ROUTING PROTOCOLS AND BLACK HOLE ATTACK

An ad-hoc routing protocol[8] is a convention, or standard, that controls how nodes decide which way to route packets between computing devices in a mobile ad hoc network. Being one of the category of ad-hoc routing protocols, on-demand protocols such as AODV [4] (Ad-hoc On demand Distance Vector) and DSR (Dynamic Source Routing) establish routes between nodes only when they are required to route data packets. AODV is one of the most common ad-hoc routing protocols used for mobile ad-hoc networks. As its name indicates AODV is an on-demand routing protocol that discovers a route only when there is a demand from mobile nodes in the network.

In an ad-hoc network that uses AODV[4][6] as a routing protocol, a mobile node that wishes to communicate with other node first broadcasts an RREQ (Route Request) message to find a fresh route to a desired destination node. This process is called route discovery.

www.ijmer.com Vol.2, Issue.3, May-June 2012 pp-1017-1021 ISSN: 2249-6645

Every neighboring node that receives RREQ broadcast first saves the path the RREQ was transmitted along to its routing table. It subsequently checks its routing table to see if it has a fresh enough route to the destination node provided in the RREQ message. The freshness of a route is indicated by a destination sequence number that is attached to it. If a node finds a fresh enough route, it unicast an RREP (Route Reply) message back along the saved path to the source node or it re-broadcasts the RREQ message otherwise.

Route discovery is a vulnerability of on-demand ad-hoc routing protocols, especially AODV, which an adversary can exploit to perform a black hole attack on mobile ad-hoc networks. A malicious node in the network receiving an RREQ message replies to source nodes by sending a fake RREP message that contains desirable parameters to be chosen for packet delivery to destination nodes. After promising (by sending a fake RREP to confirm it has a path to a destination node) to source nodes that it will forward data, a malicious node starts to drop all the network traffic it receives from source nodes. This deliberate dropping of packets by a malicious node is what we call a black hole attack. The RREQ messages and RREP messages are shown in the figure2 and figure3.

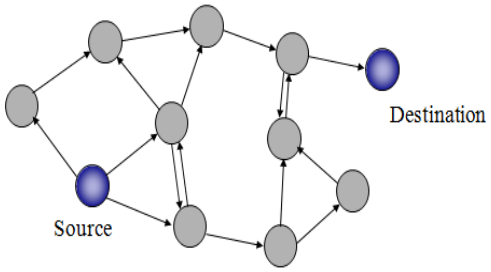


Fig 1: RREQ messages

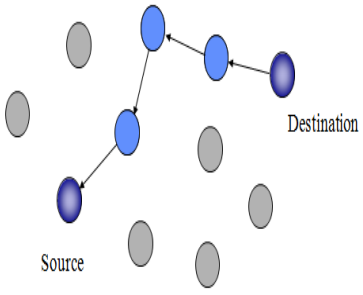


**Fig 2:RREP messages**

Back hole is a malicious node that falsely replies for any route requests without having active route to specified destination and drops all the receiving packets. If these malicious nodes work together as a group then the damage will be very serious. This type of attack is called cooperative black hole attack[5][9]shown in figure3.

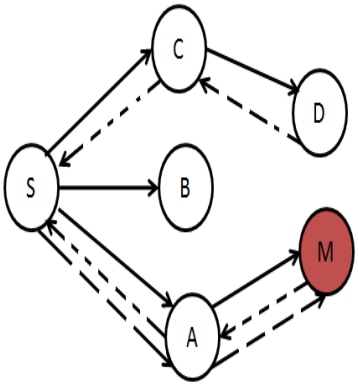


**Fig 3: Blackhole**

In black hole attack all network traffics are redirected to a specific node which does not exist at all. Because traffics disappear into the special node as the matter disappears into Blackhole in universe. So the specific node is named as a Blackhole. A Blackhole has two properties[5]. First, the node exploits the ad hoc 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. Blackhole attacks in AODV protocol routing level can be classified into two categories: RREQ Blackhole attack and RREP Blackhole attack.

2.1 Black Hole Attack Caused By RREQ

An attacker can send fake RREQ messages to form Black hole attack [2]. In RREQ node address. Other nodes will update their route to pass by the non-existent node to the destination node

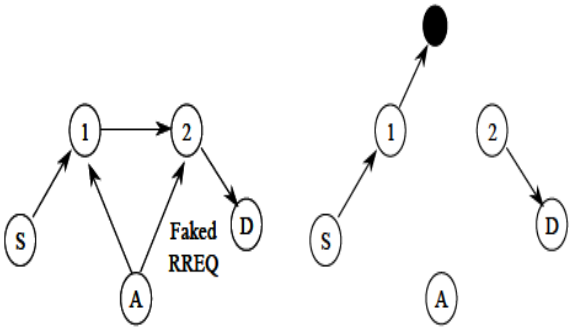


Fig 4: Blackhole Formed By Faked RREQ

As a result, the normal route will be broken down. The attacker can generate Blackhole attack by faked RREQ. The attacker forms a Blackhole attack between the source node and the destination node by faked RREQ message as it is shown in Figure 4

2.2. Blackhole Attack Caused By RREP

The attacker unicasts the faked RREP[1] message to the originating node. When originating node receives the faked RREP message

www.ijmer.com Vol.2, Issue.3, May-June 2012 pp-1017-1021 ISSN: 2249-6645

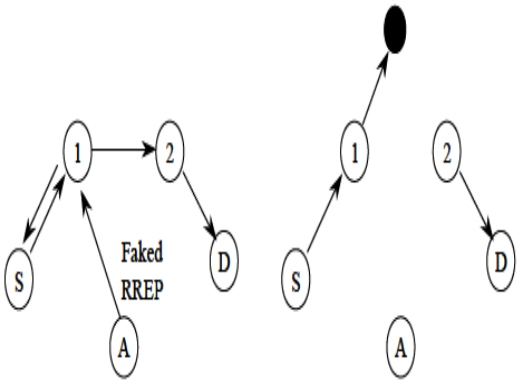


Fig 5: Blackhole Caused By Faked RREP

it will update its route to destination node through the non-existent node. Then RREP Blackhole[2] is formed as it is shown in Figure 5

## 3. PROTOCOL IMPLEMENTATION

Ad-hoc On-Demand Distance Vector (AODV) Routing Protocol[4] is used for finding a path to the destination in an ad-hoc network. To find the path to the destination all mobile nodes work in cooperation using the routing control messages. Thanks to these control messages, AODV Routing Protocol offers quick adaptation to dynamic network conditions, low processing and memory overhead, low network bandwidth utilization with small size control messages. The most distinguishing feature of AODV compared to the other routing protocols is that it uses a destination sequence number for each route entry. The destination sequence number is generated by the destination when a connection is requested from it. Using the destination sequence number ensures loop freedom. AODV makes sure the route to the destination does not contain a loop and is the shortest path. Here the AODV introduce data routing information table and cross checking the RREQ and RREP messages

### 3.1 Data Routing Information Table

Each node maintains a data routing information (DRI) table[1][2]. This table keeps track of whether or not the node did data transfers with its neighbors. This table contains one entry for each neighbor and indicates whether the node has sent data through this neighbor and whether the node has received data from this neighbor. Table entry contains *node id*, *from* and *through* as shown in Table 1. The field *from* stands for information on routing data packets from the node (in the node id field) whiles the field *through* stands for information on routing data packets through the node (in the node id field). Values of *from* and *through* fields will be 0 or 1 to represent false and true respectively. Table 1 shows the sample DRI table for a node. The entry 1,0 for node 3 implies that this node has routed data packets from node 3 but has not routed any data packet through node 3. The entry 1,1 for node 6 implies that this node has successfully routed data packets from and through node 6. The entry 0,0 for node 2 implies that node has not routed any data packets from or through node 2.

This DRI table is updated when any node received data packet from one of its neighbors or any node that sent data packets through one of its neighbors. In addition, if any node finds out the reliable path to destination which it needs to send the data, DRI table is updated with entries for all intermediate nodes through the path.

Table 1. Example of DRI table

| Node Id | Data Routing Information | |
|---|---|---|
| | From | Through |
| 3 | 1 | 0 |
| 6 | 1 | 1 |
| 2 | 0 | 0 |

In this protocol, if the source node (SN) does not have the route entry to the destination, and 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 the destination will be trusted. Source node also trusts on destination node and will start to send data along the path that reply comes back. Also source node will update the DRI table with all intermediate nodes between source and the destination.

If the intermediate node (IN) generates the Route Reply (RREP), it has to provide its next hop node (NHN) and its DRI entry for the next hop node. When the reply comes back, it collects the IP addresses of all nodes between source and the intermediate node but no intermediate node updates the route entry for the destination. Upon receiving RREP message from IN, the source node will check its own DRI table to see whether IN is a reliable node or not. If the source node has used IN before to route data, then IN is a reliable node and source will first send a route establishment message to IN node along the path that RREP comes according to the information contains in the RREP message. Upon receiving this message all nodes between the source and the intermediate node will update or insert route entry for the destination. Then source node starts sending data through the IN and updates the DRI table with nodes between source and IN node. If the source has not routed data through IN before, IN is not a reliable node. Then source first stores the information about IN and the nodes between the source and IN, and sends Further Request (FREQ) message to NHN of the IN to verify the reliability of the IN and ask NHN:

If the current NHN is the destination, then the next hop entry and the DRI entry for the next hop fields of FREP contain zeros and all intermediate nodes will either update or insert route entry for the destination. When the source receives FREP from destination, it starts routing data and updates its DRI table with all nodes

www.ijmer.com Vol.2, Issue.3, May-June 2012 pp-1017-1021 ISSN: 2249-6645

between the source and the destination. If NHN is not the destination, based on the FREP message from NHN, the source node checks whether NHN is a reliable node or not. If the source node has routed data through NHN before, NHN is reliable; otherwise NHN is unreliable.

## 4. PERFORMANCE METRICS

### 4.1 Throughput Ratio

The throughput is the number of bytes transmitted or received per second. The *throughput ratio*, denoted by *T*, is calculated as follows:

$$T = \frac{\sum_{i=1}^{n} T_i^r}{\sum_{i=1}^{n} T_i^s} \times 100\% \qquad (1)$$

4.2 Average End To End Delay

Average end-to-end delay of the application data packets, denoted by D, is calculated as follows;

$$D = \frac{\sum_{i=1}^{n} d_i}{n} \qquad (2)$$

Where *di* is the average end-to-end delay of data packets of *i*th application and *n* is the number of CBR applications.

## 5. COMPARISON WITH EXISTED METHOD

Researchers have proposed various techniques to prevent black hole attack in mobile ad-hoc networks. H. Weerasinghe and H. Fu[1] introduces the use of DRI (Data Routing Information) to keep track of past routing experience among mobile nodes in the network and crosschecking of RREP messages from intermediate nodes by source nodes. The main drawback of this technique is that whenever the black hole node take part in two or more transmission path, each path there is a huge packet losses due to the black hole. Therefore the delay performance is high.

### 5.1 MN-Id Broadcasting Method

In the proposed system, MN-ID broadcasting method is used. In this method once the malicious node is identified, the particular node id(only for simulation, real time ip address is used) is transmitted to the entire network therefore whether the malicious node take part in two or more path packets does not move towards the malicious node because whole nodes in the network should know about the malicious node. Therefore the packets transamitted through an alternative path from source to destination.

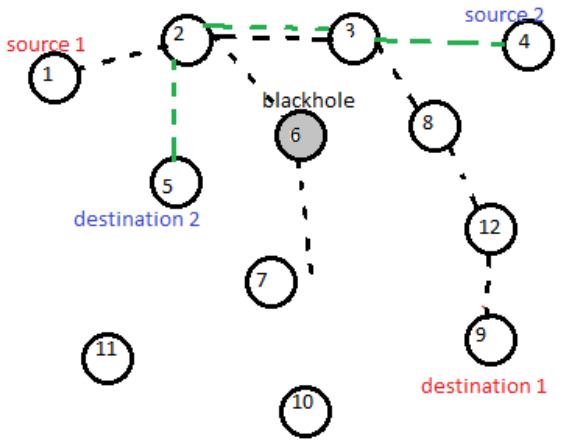


Fig.6 MN-ID broadcasting method

Figure6 shows the MN-ID broadcasting method. Here node 1 represented as source 1 and node 9 represented as destination 1and node 6 is assigned as black hole node. When the packet transmission takes place source 1 transmitted packets to destination node 9. When packet reaches on the node 6 it will drop all the received packets. Then the protocol identify an alternative path to destination and broadcasting the corresponding malicious node ID (that is node 6)to the entire nodes in the network. The actual shortest from node 4 to node 5 is 4-3-6-5. Whenever the packet transmitted from node 4, the packets are not transmitted through the correct shortest path because node 6 is a black hole and that particular node ID is broadcasted to the entire network. Hence the packet transmission takes place through the path 4-3-2-5 and reach the proper destination.

## 6. SIMULATION PARAMETERS AND RESULTS

The various parameters which are considered for network simulation is specified in the table2

Table 2. simulation parameters

| | |
|---|---|
| Number of nodes | 50 |
| Packet size | 512bytes |
| Data rate | 512b/s |
| No. of BH nodes | 2 |

The existing method (H. Weerasinghe and H. Fu method) simulation results throughput vs time and packet delivery ratio vs time is given below. These results are improved by MN-ID broadcasting method.

www.ijmer.com Vol.2, Issue.3, May-June 2012 pp-1017-1021 ISSN: 2249-6645

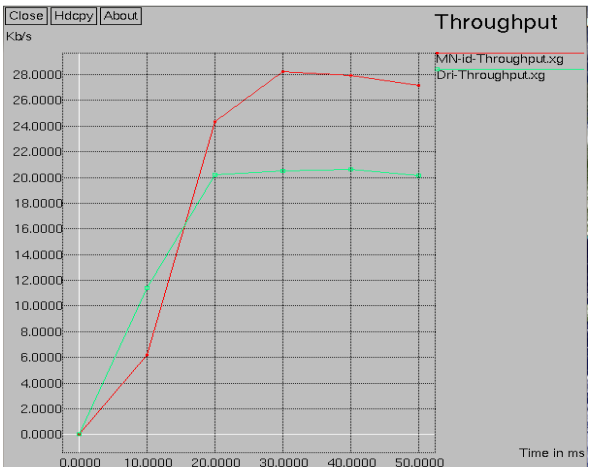


Fig6: Throughput vs time MN-ID broadcasting and DRI method(existing method**)**

The comparison of packet delivery ratio vs time and packet drop vs time in the MN-id method and DRI method is given in the fig7 and fig8. The graph shows that better results in MN-id method

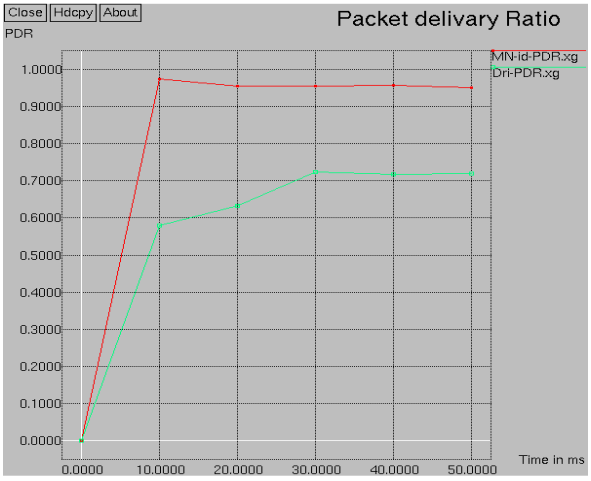


Fig7: pdr vs time in MN-ID broadcasting method and DRI(existing method) method

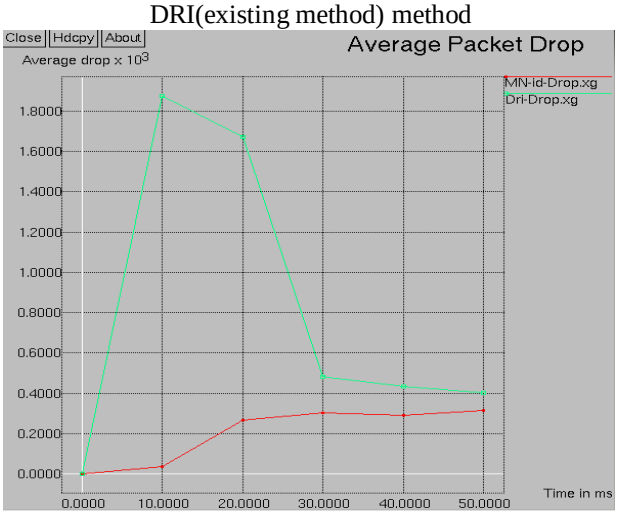


Fig 8: packet drop vs time in MN-ID broadcasting method and DRI(existing method) method

## 7. CONCLUSION

In this paper, we studied the problem of cooperative black hole attacks in MANET routing. The MN-ID broadcasting method provides improved performance of throughput packet delivery ratio and reduced packet loss comparing with H.Weerasinge and H.Fu method. Therefore MN-ID broadcasting method provide improved network performance and minimum packet loss in the packet transmission.

## REFERENCES

[1] H.Weerasinge and H.Fu(2008) "Preventing Black Hole Attack in Mobile Ad hoc Networks: simulation, implimentation and evaluation"*international journal of software engg. and its applications,vol2,no3*

[2] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon, and Kendall Nygard, "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks", 2003 *International Conference on Wireless Networks (ICWN'03), Las Vegas, Nevada, USA*

[3] Hongmei Deng, Wei Li, and Dharma P. Agarwal, (2002) "Routing Security in Wireless Ad Hoc Networks", University of Cincinnati, *IEEE Communications magazine, Vol.40,* No.10

[4] Charles E. Perkins, and Elizabeth M. Royer, "Ad-hoc On-Demand Distance Vector (AODV) Routing," *InternetDraft*, November 2002.

[5] S. Sharma and R. Gupta, (2009) "Simulation study of black hole attack in the mobile ad-hoc networks," *journal of engineering science and technology, vol. 4, no. 2* pp. 243-250.

[6] LathaTamilselvan,Dr.VSankaranarayanan "Prevention of Co-operative Black Hole Attack in MANET", *Journal Of Networks, Vol. 3,* NO. 5,2008

[7] Jian Yin, Sanjay Madria, "A Hierarchical Secure Routing Protocol against Black Hole", *IEEE SUTC 2006 Taiwan, 5-7* June 2006

[8] Dokurer, S.; Ert, Y.M.; and Acar, C.E. (2007). Performance analysis of ad hoc networks under black hole attacks. SoutheastCon, 2007, *Proceedings IEEE*, 148 – 153.

[9] Dr. Karim Konate and Abdourahime Gaye(2011)'a proposal mechanism against the attacks: cooperative black hole, blackmail, overflow and selfish in routing protocol of mobile ad hoc network',*internationaljournal of future generation communication and networking Vol. 4*, No. 2