A Novel Technique to Detect and Isolate Multiple Black Hole Attack using Fake Destination ID

Manisha Raj
M.Tech. Scholar,
Computer Science Arya College of Engg. & IT Jaipur, India
E-mail: manisha.raj@gmail.com

Prof. Vishal Shrivastav
Professor, CS Dept.
Arya College of Engg. & IT
Jaipur, India
E-mail: vishal500371@yahoo.co.in

***Abstract*—**MANET is autonomous, decentralized, infrastructure less, cooperative & self-configurable network. It composed of continuously moving mobile nodes which deploy dynamic topologies. The mobile nodes in MANET can act as host as well as router. There are various protocols available for managing these mobile nodes which are formally categorized in proactive & reactive and hybrid protocols. As the network employs dynamic topology and no infrastructure, it is prone to so many security attacks viz. flooding, DoS, wormhole, grey hole, black hole, eavesdropping, jamming, man-in-the-middle, Sybil attacks etc. Among them black hole attack is most popular attack in which the attacker behave as black node and fool the source node that it has the shortest path available to the destination and thus prevents the packet reaching the destination. In this paper a new technique is proposed to detect and isolate black hole attack using fake route request packets. The simulation results show that the scheme is better than the previously described schemes in the terms of packet delay and throughput.

Keywords: *autonomous, self-configurable, hybrid, flooding, black hole.*

*****

I. INTRODUCTION

A mobile ad hoc network incorporate mobile devices such as cell phones, PDA's, laptops etc., that communicate with each other via intermediate nodes. There is no central control present to manage the communication and data transfer between mobile nodes.[1] MANET sets up a network whenever a transfer has to take place. The transmission range of the nodes is limited so it uses multi hops to transfer data packets between the nodes which are out of range. The nodes in manet operates as host, when it wants to transit or receive data or router, when it is used just to forward packets to other nodes.[2] Manets are having the freedom to govern itself and act independently. There is no centralised system or node to manage the network scenario. Manet does not pursue a fixed infrastructure as the nodes can anytime join or leave the network. They do not have to ask any node in the network to do this. The network manages the transfer of data in a cooperative way i.e. the intermediate nodes work in cooperative manner to forward the data packet to the destination. It is a self-configurable network i.e. nodes can work as host as well as router according to the circumstances. It has a constrained capability and less hardware resources. Due to the dynamic nature of MANET, routing of the data packets is more complex task.

There are several routing protocols available for MANET which are classified into three categories namely proactive, reactive and hybrid. Hybrid is the combination of proactive and reactive protocol. Manet is useful where all the networks are out of reach like battlefields, disaster management, rescue missions & military applications.[3] Security is still the complex issue in MANETs as it is infrastructure less, involves mobile nodes and deploys dynamic topology. Routing protocols are used to set up an optimal & effective route between participating entities. Each routing protocol has security issues for which so many solutions are available but still there are some problems which are still unable to prevent completely.

One of the major attacks is black hole attack which is the well-known security threat in wireless ad-hoc networks. This paper focuses on various types of black hole attack, their detection and solutions.[2] Black hole attack can be broadly classified into ordinary and cooperative black hole attack.[4] These are mainly evaluated on the basis of performance matrices including Packet Delivery Ratio (PDR), Packet Loss, Routing Overhead and Average delay. In this paper we first discuss different types of attacks and we a new method is described to detect and isolate multiple black hole attack.[5,6]

II. SECURITY ATTACKS IN MANET

Manet suffers from many attacks that breach the security of network. Some of them are discussed in this section.

A. Wormhole Attack

Wormhole attack is another severe attack in which two colluding nodes that are apart from each other linked

through a tunnel and gives an impression that they are neighbours. Each node receives route request message and other control messages and forwards them to other colluding nodes through tunnel, which in turn replay them to other nodes in the network. It is a network layer attack.[7] The two colluding attacker's tunnel between them is referred as wormhole.

B. Black hole Attack

In this type of attack the requests is listened by an attacker for the routers in a flooding based protocol. When a request is received by the attacker to the destination node for a route, it creates a reply by showing that it has the shortest route and enters into the passageway to do something with the packets passing between them [2]. In this way the black hole node fools the source and grabs access to all the packets that belong to the destination.

C. Denial of Service Attack

The aim of attack is to hit the accessibility of a node and all the nodes in the entire network. The services will not be accessible if the attack is successful [8]. The attacker generally uses battery exhaustion method and radio signal jamming. It has further sub categories:

1. Smurf Attack
2. Distributed denial of services
3. SYN flood attack

D. Byzantine Attack

In this attack, an intermediate compromised node carries out attacks such as creating collision, forwarding packets on non-optimal paths, routing loops, and dropping packets selectively which result in interruption or dreadful conditions of the routing services.[6]

E. Man- in- the- middle attack

In this attack, an attacker sits between the sender and receiver and any information being sent between two nodes sniffs by him. In some cases, attacker may masquerade as the sender to communicate with receiver or masquerade as the receiver to reply to the sender. It starts when first attacker sniffs and eve dropped the packets [5].

F. Eavesdropping

Eavesdropping is the passive form of attack. The malicious nodes in the network can sniff the network traffic.[9] The secret information like passwords, private keys can be fetched by the attacker out of the sniffed data. The passive attacks may leads to the perpetuation of active attacks.

G. Jamming Attack

The jamming attack is the active type of attack. In this a malicious nodes can send unlimited number of packets to selective node due to which the node will be unable to handle such large number of packets. In lieu of this, network blockage kind of situation has been cropped up.

III. BACKGROUND OF BLACK HOLE ATTACK

Previously many of the researchers have worked on the security issues in MANET. One of the major security attacks is Black Hole attack which is studied under the AODV routing protocol and its effects are particularized by specifying how this attack disturb the performance of MANET.[4,10] AODV protocol is written in RFC 3561. AODV is an important on-demand routing protocol that creates routes only when desired by the source node. When node requires a route to a destination, it starts a route discovery process within the network. It broadcasts a route request (RREQ) packet to its neighbours, which send the request to their neighbours, and the process is repeated, until either the destination or an intermediate node with a "fresh enough" route to the destination is identified. In this process the intermediate node can reply to the RREQ packet only if it has a fresh enough route to the destination.[11] When the RREQ reaches the destination or an intermediate node with a fresh enough route to the destination, it responds by unicasting a route reply (RREP) packet back to the neighbour from which it first received the RREQ. After selecting and establishing a route, it is kept by a route maintenance method until either the destination becomes inaccessible along every path from the source or the route is no longer desired. A RERR (Route Errors) message is used to notify other nodes that the loss of that link has occurred.

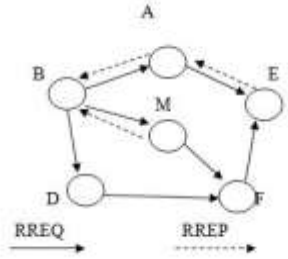

Fig. 1. Route Discovery Process in AODV Protocol

A black hole problem means that a malicious node utilize the routing protocol to claim itself of being the shortest path to the destination node, but drops the routing

packets and does not forward packets to its neighbours.[8] Imagine a malicious node 'M'. When node 'A' broadcasts a RREQ packet, nodes 'B' 'D' and 'M' receive it. Node 'M', being a malicious node, does not check its routing table for the requested route to node 'E'.

Hence, it immediately sends back a RREP packet, which tells that it has a route to the destination.

Node 'A' receives the RREP from 'M' ahead of the RREP from 'B' and 'D'. Node 'A' assumes that the route through 'M' is the shortest route and sends any packet to the destination through it. When the node 'A' sends data to 'M', it absorbs all the data and thus behaves like a 'Black hole'.

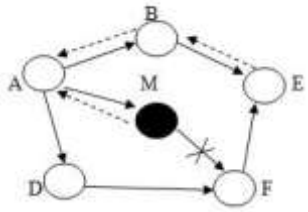

Fig. 2. Black Hole problem in MANET

In AODV, the sequence number is used to determine the freshness of routing information contained in the message from the initiating node i.e source node.[4] When the destination generates RREP message, it compares its current sequence number with the RRQ packet's sequence number, adds one in it and then selects the larger one as RREPs sequence number. Upon receiving many RREPs, the source node picks the one with greatest sequence number in order to establish a route. But, in presence of black hole when a source node broadcasts the RREQ message for any destination weather it present in the network or not, the black hole node immediately responds with an RREP message that includes the highest sequence number and this message is perceived as if it is coming from the destination or from a node which has a fresh enough route to the destination. The source thinks that the destination is behind the black hole and discards the other RREP packets coming from the other nodes.[4] The source then starts the communication by sending packets to the black hole believing that these packets will reach the destination. Thus the black hole will invite all the packets from the source and instead of forwarding those packets to the destination (black hole) it will simply discard them. Thus the packets attracted by the black hole node will not reach the destination.

IV. PROPOSED TECHNIQUE

In MANET internal and external attacks are possible, which cut down the performance of the network. In Internal attacks a node within the network become malicious node and it launched attacks on network. In external attacks a malicious node which is outside the network, it become the member of the networks and then launched the attack on network.

Among all the attacks discussed previously black hole attack is the most common attack. It is the denial of service attack which is triggered by the malicious nodes in the network. Many techniques have been proposed to isolate it from the network. When black hole attack is triggered in the network, throughput of the network decreases and delay increases. The black hole attack is even inferior if the multiple black hole nodes exist in the network. When this happens, all the malicious nodes are responsible for triggering the black hole attack. This is called multiple black hole attack. In our work, we work on to detect and isolate multiple black hole attack in mobile Ad hoc network.[1] The whole scenario will be implemented on NS2 simulator.

V. RESEARCH METHODOLOGY

The mobile ad-hoc network is the self-configuring type of networks in which the mobile nodes can join or leave the network when they want. It is a decentralized network in which source node can communicate to the destination node. The path between source and destination is required to be the shortest and reliable. AODV routing protocol is required to select the shortest and reliable path. To start the communication the source node floods the network with route request packets (RREQ). The nodes which have direct path to the destination, reply to the source by using route reply packets (RREP). After receiving RREP message the source node select best path on the basis of hop count and sequence number. Some malicious nodes exist in the network which do not have path to destination but revert back with route reply packets. The source node may select the best path through that malicious nodes and that node may drop all the packets, which reduce the network throughput. These malicious nodes are known as black hole and this type of attack is called black hole attack.

To isolate black hole attack from the network a new method is introduces in which source node floods the route request packets in the network with fake destination ID. As the malicious node does not know about any destination, it reverts back with route reply packet and all legitimate (genuine) nodes will not revert back. The source node maintain table in which the information about the malicious nodes are stored. The source node identifies the malicious nodes and to isolate them from the network, it floods the network with ALARM message and the table which contain the information of malicious nodes.[7] After receiving the ALARM message the intermediate nodes stop the

communication with these malicious nodes. Now the source node again floods the network with RREQ message having genuine destination ID and select a reliable path to the destination. To verify the reliability of selected path diffie-hellman key establishment algorithm is used. In the Diffie-Hellman algorithm if two parties, say, Master and Slave desires to interchange data, both agree on a symmetric key.[9] A symmetric key is used to encrypt and decrypt the messages. Both the parties choose their own random number. On the basis of the selected random numbers, a secure channel is established.[12]

VI. SIMULATION ENVIRONMENT

A. Simulation Parameters

We use NS-2 to form the simulation environment. The AODV protocol is used to detect black hole.
The operating system used here is Ubantu. The parameters that are considered to show the simulation are given in Table 1.

Table 1. Simulation Parameters

The nodes are numbered from 0 to 14. The source and destination are marked as 0 and 7 and the black hole nodes are 5 and 11.

S. No.	Parameter	Value
1.	Terrain Area	800m x 800m
2.	Simulation Time	50 s
3.	MAC Type	802.11
4.	Application Traffic	CBR(Constant Bit Rate)
5.	Routing Protocol	AODV
6.	Data Payload	512 Bytes/Packet
7.	Pause Time	2s
8.	Number of Mobile Nodes	15
9.	Number of Sources	1
10.	No. of Adversaries	1 to 3

B. Performance Metrics

Following metrics are used to evaluate the technique:

i. Throughput

It is the rate of packets delivered successfully from source node to the destination, in a communication network. It is measured in bits/seconds.

Throughput= (no. of packet delivered*packet size)/ total duration of simulation.

ii. Packet Delay

A packet can be delayed to reach the destination due to many reasons like processing delay, propagation delay, route discovery latency and retransmission by intermediate node. It is the ratio of the time interval between sending and receiving packet and total data packets received.

Packet delay=∑ (Time received - Time sent)/Total Data packets received

VII. SIMULATION RESULT AND DISCUSSIONS

First, we investigate the Packet delay.

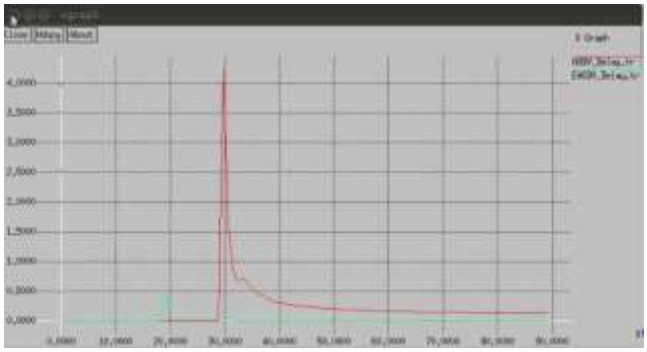

Fig. 3. Packet Delay Comparison

In above figure red line shows the delay in previous scheme and green line show delay in proposed scheme. X-axis show time and y axis shows packets. It is observed that the proposed scheme has less delay as compare to previous technique.

Then we examine the throughput of the network and observed that the throughput of the proposed technique is better than the previous scheme.

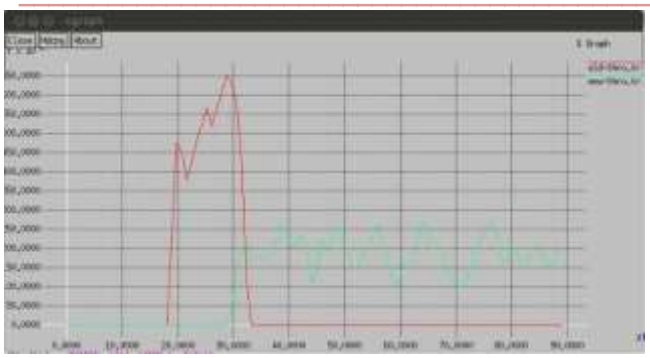

Fig. 4. Throughput Comparison

Parameters	Previous Scheme	Proposed Scheme
Throughput	18%	60%
Delay	25%	4%

Table 2. Comparison of previous scheme and proposed scheme

Table 2 presents the comparison between the previously described scheme and the proposed scheme. It is seen that the throughput of previous scheme is 18%, which is increased to 60% in the new technique proposed here. The packet delay is reduced to 4%, which was 25% in old scheme.

VIII. CONCLUSION

One of the most important security problems in MANET is Black hole attack. It is an active attack in which intruder or malicious node can impersonate as a genuine node and reply to the source node saying that it has the best route to the destination, as a result the packets are dropped by the malicious node and the performance of network degrades.

In this paper we have analysed the effect of black hole attack. The simulation result shows that the proposed method is better than the previous methods in terms of throughput and packet delay.

REFERENCES

[1] JeroenHoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester, "An Overview of Mobile Ad Hoc Networks: Applications and Challenges", Journal of The Communication Network 2004, Volume 3, ISSN 1477-4739, pp. 60-66

[2] Bo Sun Yong, "Detecting Black-hole Attack in Mobile Ad Hoc Networks", 5th European Personal Mobile Communications Conference 2003, pp. 490-495

[3] PriyankaGoyal, VintraParmar and Rahul Rishi "MANET: Vulnerabilities, Challenges, Attacks, Application", IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011 ISSN (Online): 2230-7893 2011, pp. 32-37

[4] Giovanni VignaSumitGwalaniKavitha Srinivasan Elizabeth M. Belding-Royer Richard A. Kemmerer, "An Intrusion Detection Tool for AODV-based Ad hoc Wireless Networks", Computer Security Applications Conference,IEEE 2004, ISSN- 1063-9527, pp. 16-27

[5] Sun B, Guan Y, Chen J, Pooch UW , " Detecting Black-hole Attack in Mobile Ad Hoc Networks". 5th European Personal Mobile Communications Conference, Glasgow, United Kingdom, 22-25 April 2003, ISSN- 0537-9989

[6] DurgeshWadbude, VineetRichariya, "An Efficient Secure AODV Routing Protocol in MANET"International Journal of Engineering and Innovative Technology (IJEIT) ISSN: 2277-3754 Volume 1, Issue 4, April 2012, pp. 274-279

[7] Jacek Cicho, Rafał Kapelko, Jakub Lemiesz, and Marcin Zawada "On Alarm Protocol in Wireless Sensor Networks", 9th International Conference ADHOC-NOW 2010, Edmonton, AB, Canada, August pp.20-22, 2010

[8] Satoshi Kurosawa1, Hidehisa Nakayama1, Nei Kato1, Abbas Jamalipour2, and Yoshiaki Nemoto1 "Detecting Black hole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method" International Journal of Network Security, Vol.5, No.3, Nov. 2007 pp: 338-346

[9] Seung Yi, Robin Kravets, "Key Management for Heterogeneous Ad Hoc Wireless Networks",10th IEEE International Conference on Network Protocols (ICNP'02), 2002, ISSN :1092-1648, pp. 202-203Cooperative and Multiple Black Hole Attack in Mobile ADHOC Networks" International Conference on Computer and Software Modeling IPCSIT vol.14 (2011), pp. 66-70

[10] Mehdi Medadian , Proposing a Method to Remove Gray Hole Attack in AODV Protocol in MANET

[11] Nitesh A. Funde, P. R. Pardhi, " Detection & Prevention Techniques to Black & Gray Hole Attacks In MANET", International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 10, October 2013, ISSN (Print) : 2319-5940, pp. 4132-4136

[12] Suparna Biswas, Tanumoy Nag, Sarmistha Neogy, "Trust Based Energy Efficient Detection and Avoidance of Black Hole Attack to Ensure Secure Routing in MANET", Applications and innovations in mobile computing, 2014, (AIMoC), pp.157-164