Blackhole detection and prevention in manet

[1]Ms. Twincle G. Vyas, [2]Ms. Divya M. Patel, [3]Ms. Ekta P. Soni

Department of Computer Engineering
Faculty of Engineering Technology & Research
Gujarat Technological University (GTU)
Gujarat, India

***Abstract*— mobile ad hoc network(MANET) is self-arranged network made up of sensor mobile nodes formed anytime and anywhere without the any centralized management due to the dynamic network topology, autonomous terminal, lack of centralized monitoring and lack of manage point mobile ad-hoc network are highly vulnerable to security threats compared to wired network and infrastructure network. In black hole attack, a malicious node gives wrong information of having shortest path to reach the destination node so as to get all data packets and drop it. In this paper, we have discussed different detection and prevention techniques for the black hole attack in MANAET.**

***Index Terms*— AODV, Black hole attack, MANET, Routing protocols, malicious node.**

I. INTRODUCTION

MANET consists of a collection of wireless mobile nodes that have capability to communicate with each other without use of network infrastructure or any centralized administration. Also security is important to provide protection over communicating nodes in an environment. Although security has long been a most demanding research topic in wire line networks, the unique characteristics of MANETs present a new set of challenges to security design. Routing protocol in MANET is divided into two main categories, proactive and reactive. In proactive routing protocols, routing information of nodes is exchanged, periodically, such as DSDV. In on-demand routing protocols, route is established and nodes exchange routing information when needed such as AODV [9]. Furthermore, some ad-hoc routing protocols are a combination of above categories. AODV protocol is preferred as compare to other protocols because it minimizes the routing overhead [10].AODV provides loop free routes and repair broken links [10]. AODV is an on demand routing protocol, this means that routes are only established when needed. The black hole attack is the most severe security attacks which can significantly disrupt the communications across the network. AODV protocol use control messages to find a route from source to the destination node in the network. There are three types of control messages in AODV; these are

1. Route Request Message (RREQ)
2. Route Reply Message (RREP)
3. Route Error Message (RERR).

II. WHAT IS BLACK HOLE ATTACK?

A Black Hole attack [11] is a kind of denial of service attack where a malicious node gives false information of having shortest route to the destination in order to get all the data packets and drop it In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept. This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it[12].In protocol based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from actual node; hence a malicious and forged route is created. When this route is establish, now it's up to the node whether to drop all the packets or forward it to other unknown address..The method how malicious node fits in the data routes varies.

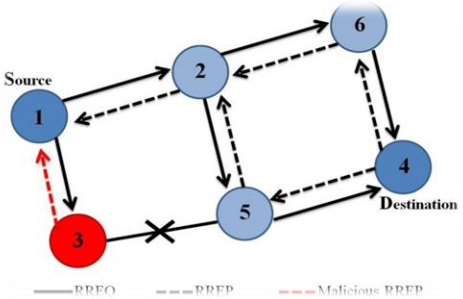

Fig 1: Black Hole attack in MANET

Fig shows how black hole problem arises, here node "A" want to send data packets to node "D" and initiate the route discovery process. So if node "C" is a malicious node then it will claim that it has active route to the specified destination as soon as it receives RREQ packets. It will then send the response to node "A" before any other node.
In this way Node "A" will think that this is the active route and thus active route Discovery is complete. Node "A" will ignore all other replies and will starts siding data packets to node "C". In this way all the data packet will be lost consumed or lost.

III. BLACK HOLE ATTACK DETECTION METHOD

Watchdog Scheme- Patcha et al [5] proposed a method for black hole attack network to tackle collusion amongst nodes. In this algorithm, nodes in the network are classified into trusted, watchdog, and ordinary nodes. Every watchdog that is elected should observe the neighboring node and decide whether it is a trusted node or a malicious node.

In this scheme, when the source node forwards a packet, it waits for an acknowledgement packet from destination node. When the destination node receives a packet it sends back an acknowledgement back to source node through each node along the reverse route. The packet transmission is successful if source node receives an acknowledgement packet. Otherwise an alarm message is generated.

IV. BLACK HOLE ATTACK PREVENTION METHOD

Retrieve the first entry from RRT
If DSN is much greater than SSN then
discard entry from RRT as
Select Dest_Seq_No from table
If (DSN >>=Src_Seq_No)
{
MN=Node_Id
Discard entry from table
}
(Node Selection Process)
* Sort the contents of RRT entries according to the DSN
* Select the NID having highest DSN among RRT entries.
(Continue default process)
Call RREP method of default AODV Protocol.
This show malicious node is identified and removed.
(1) The malicious node is identified at the initial stage itself and immediately removed so that it cannot take part in further process.
(2) No delay = malicious node are easily identified
(3) No modification is made in other default operations of AODV Protocol.
(4) Better performance produced in little modification and
(5) Less memory overhead occurs because only few new things are added.

V. SIMULATION PARAMETERS AND TERMINOLOGIES

The following table shows the simulation parameters which we are using to implement the detection technique.

Table 1 Simulation Parameters

Parameter	Value
Simulator	NS-2.35
Area	750mx750m
Routing Protocol	AODV
Simulation time	300s
Application Traffic	CBR
Number of Nodes	20
Malicious Node	1-5
Packet Size	512 bytes
Transmission rate	2 packets/s

To evaluate the black hole attack we consider the following three metrics:

Packet Delivery Ratio

- It is the ratio of the packets that are successfully delivered to the destination.
- Packet Delivery Ratio=Number of packets received / Number of packets send

End-to-End Delay

- It is the average time taken by the packets to pass through the network.
- End-to-End Delay=received time – sent time

Throughput

- It is the amount of data transferred over the period of expressed in bits per second.
- Throughput (bits per second)= (No. of delivered packets*Packet size*8)/(Simulation time)
-

VI. SIMULATION RESULTS

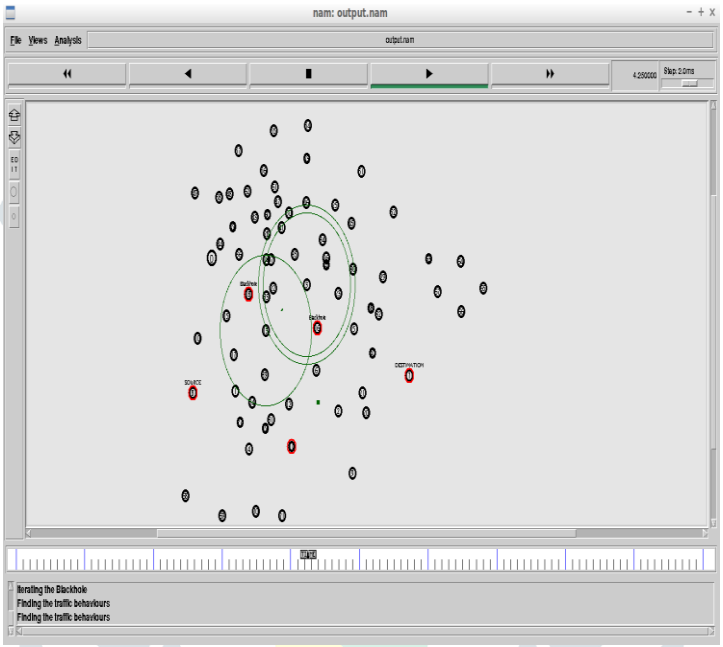

Fig 2: Traffic Behaviors

In this scenario iterating the blackhole and finding the traffic behavior.

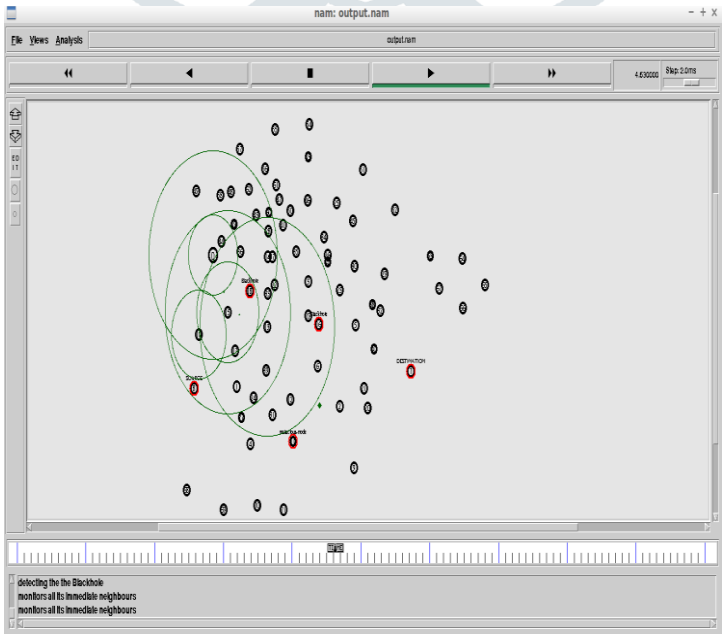

Fig 3: Monitor immediate neighboring node

In this scenario detecting the blackhole and also monitor its all immediate neighbors.

Fig 4: Xgraph for Performance before attack

Fig 5: Xgraph for Performance when attack happen

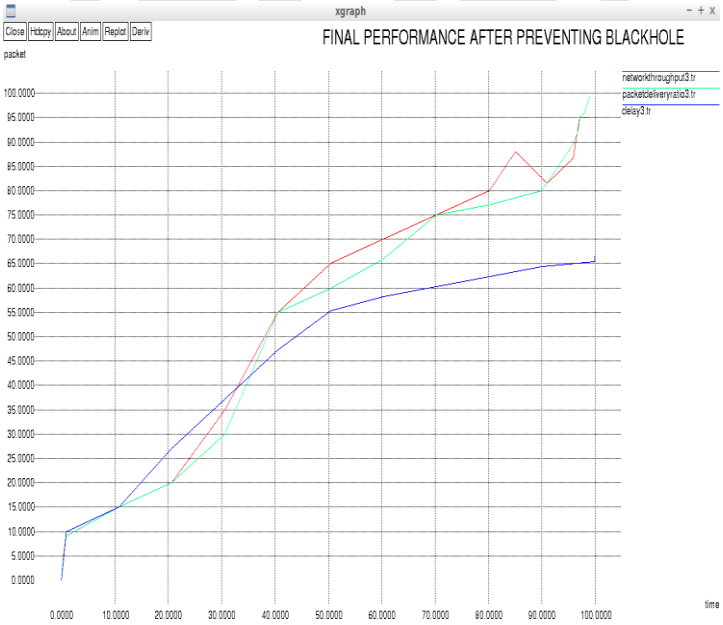

Fig 6: XGraph for Performance after preventing black hole

VII. CONCLUSION

Black Hole Attack is a main security attack that degrades the performance of the routing protocol in Mobile Ad-hoc Network. Its detection and prevention is the main matter of concern to improve network quality. In this paper, we have analyzed and describe various techniques for detection and prevention of black hole attack in the Mobile Ad-hoc Network. Methods that we have discussed to detect and prevent black hole attack in MANET give better results thanoth er security mechanism.

VIII. ACKNOWLWDGEMENT

In this paper, we are implimented detection and prevention technique of BlackHole Attack.

REFERENCES

[1]"survey of black hole attack detection in mobile adhoc networks"shashi gurung, aditya kumar, krishan kumar saluja july 2013
[2]"Black hole attack in AODV routing protocol: A Review by ijarcsse "april-13
[3]"Detection and Prevention of Blackhole Attack in MANET Using ACO by IJCSNS" Sowmya K.S, Rakesh T.and Deepthi P Hu dedagaddi.
[4]Luca Maria Gambardella IDSIA, Lugano, "Ant Colony Optimization for ad-hoc networks", The First MICS Workshop on Routing for Mobile Ad-Hoc Networks
[5]Patcha; A. Mishra; Collaborative security architecturefor black hole attack prevention in mobile ad hocnetworks; Radio and Wireless Conference, 2003, 75-78
[6] Sun; Y. Guan; J. Chen; U.W. Pooch, Detecting Black-hole Attack in Mobile Ad Hoc Networks
[7] X.P. Gao; W. Chen; A Novel Gray Hole Attack Detection Scheme for Mobile Ad-Hoc Networks; IFIPInternational Conference on Network and ParallelComputing Workshops, 2007
[8] Tamilselvan L, Sankaranarayanan V (2007) Preventionof Blackhole Attack in MANET. Wireless Broadband and Ultra Wideband Communications, Sydney,Australia
[9] Su M-Y (2011) Prevention of Selective Black HoleAttacks on Mobile Ad Hoc Networks Through IntrusionDetection Systems. IEEE Computer Communications
[10] Kozma W, Lazos L (2009) REAct: Resource-EfficientAccountability for Node Misbehavior in Ad Hoc Networks based on Random Audits.
[11] Wang W, Bhargava B, Linderman M (2009) Defendingagainst Collaborative Packet Drop Attacks on MANET
[12] Tsou P-C, Chang J-M, Lin Y-H, Chao H-C, Chen J-L(2011) Developing a BDSR Scheme to Avoid Black Hole Attack Based on Proactive and ReactiveArchitecture in MANETs.
[13] Dokurer, S.; Erten Y.M., Acar. C.E., SoutheastCon Journal, "Performance analysis of ad-hoc networks under black hole attacks". Proceedings IEEE Volume, Issue, 22-25 March 2007 Page(s):148 – 153.
[14] A. Shevtekar, K. Anantharam, and N. Ansari, "Low Rate TCP Denial-of-Service Attack Detection at Edge Routers," IEEE Commun. Lett., vol. 9, no. 4, Apr. 2005, pp. 363–65.
[15] Mohammad Al-Shurman and Seong-Moo Yoo, Seungjin Park, "Black hole Attack in Mobile Ad Hoc Networks" Proceedings of the 42nd annual Southeast regional conference ACM-SE 42, APRIL 2004, pp. 96-97.
[16]Y-C Hu and A. Perrig, "A Survey of Secure Wireless Ad Hoc Routing," IEEE Sec. and Privacy, May–June 2004.
[17]K. Sanzgiri et al., "A Secure Routing Protocol for Ad Hoc Networks," Proc. 2002 IEEE Int'l. Conf. Network Protocols, Nov. 2002
[18] Payal N. Raj, Prashant B. Swadas" DPRAODV: A Dyanamic Learning System Against Blackhole Attack In AODV Based Manet." arXiv:0909.2371,2009.
[19] Ming-Yang Su," Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems", Elsevier, Computer Communications 34 (2011) 107–117