ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

Preventing Black Hole Attack in MANETs

E. Shanthi, A.Rama

Department of MCA, Bharath University, Chennai, India

Department of IT, Bharath Institute of Science and Technology, Chennai, India

ABSTRACT: A mobile ad hoc network (MANET) is a system of wireless mobile nodes that can generously and dynamically self organize into arbitrary and temporary topologies without the need of any preexisting communication infrastructure. While many challenges need to be resolved before the large scale use of MANET, one particular area of concern is the routing, where one important role is security. A black hole is a malicious node that incorrectly 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. The key concept of the existing solution is that, to use modified AODV routing protocol by introducing data routing information table (DRI) where as watchdog method detects misbehaving nodes by maintaining a buffer that contains recently sent packets.

I.INTRODUCTION

The recent wireless research indicates that the wireless MANET presents a larger security problem than conventional wired and wireless networks. While most of the underlying features make MANETs useful and popular. In general, the wireless MANET is particularly vulnerable due to its fundamental characteristics of open medium, active topology, and lack of central establishment, distributed cooperation, and constrained capability. The accessible security solution for wired networks cannot be applied directly in wireless MANETs. In this paper we study the security issues when routing is performed in a MANET, analyze in detail one type of attack —the ―black hole problem —that can easily be deployed against MANETs, and use the proposed solution given by Sanjay Ramaswamy [1] and we also analyze a feasible solution by introducing concepts such as ―Watchdog‖ for ad hoc on-demand distance vector (AODV) routing protocol. The rest of the paper is

organized as follows. We discuss the routing security issues in a MANET and give an overview of black hole attack in MANETs in literature as well as by simulation [1]. We describe the co-operative black hole problem in AODV protocol in detail. Then, we compare the both DRI and watchdog solution in terms of throughput and packet losses. Finally, we provide conclusions and directions for our future research.

II. ROUTING SECURITY IN MANETS

The nodes in an ad hoc network also purpose as routers that discover and maintain routes to other nodes in the network. The primary goal of a MANET routing protocol is to establish a correct and efficient route between a pair of nodes so that messages may be delivered in a appropriate manner. If routing can be misdirected, the entire network can be paralyzed. Thus, routing security plays an important role in the security of the whole network.

A. Black hole attack in MANETS.

In this attack, a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to catch. In a flooding based protocol, the attacker listens to requests for routes [1]. When the attacker receives a request for a route to the target node, the attacker creates a reply consisting of an tremendously short route. If the malicious reply reaches the requesting node before the reply from the actual node does, a forged route has been created. Once the malicious device has been able to insert itself between the correspond nodes, it is able to do anything with the packets passing between them. It can choose to fall the packets to achieve a denial- of- service attack or alternatively use its place on the route as the first step in a man-in-the-middle attack. When two or more malicious node works together, the it is called as ―Cooperative Black Hole Attack‖

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

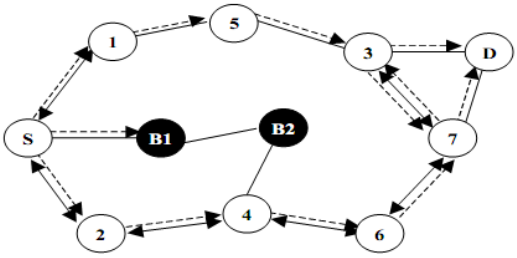
Vol. 2, Issue 10, October 2014

B. Military Attacks.
Since MANETs are extensively used in Military Applications, the attacks which can be carried out in these cases are:

Strategic routing attacks:
These are only intelligence gathering, Passive attacks are best put use in this case.
Tactical routing attacks:
These attacks are used most effectively in battle zones in order to gain information about the enemy's network topology; Active attacks are best used in this case [2].
One of the most widely deployed attack is the Black Hole Attack. Even though the AODV is most widely tuned for its better performance it still lacks secured communication, although the introduction of Message Authentication (MAC) and other Intrusion Detection Methods in MANETs has improved the routing security, AODV protocol still lacks proper secured communication and is still vulnerable to Black hole attack. In this paper, we evaluate the proposed method by Sanjay Ramaswamy et al [1], and
compare it with our modified IDS by Sergio Marti et al [3], by introduction of Watchdog in AODV than the currently used DSR protocol. We then simulate our results by using Network Simulator 2, and show that our modified IDS have better throughput and security in AODV as well.

III. COOPERATIVE BLACK HOLE PROBLEMIN AODV PROTOCOL

AODV is an important on-demand routing protocol that creates routes only when desired by the source node. When a node requires a route to a destination, it initiates a route discovery process within the network. It broadcasts a route request (RREQ) packet (Fig. 1) to its neighbors, which then forward the request to their neighbors, and so on, until either the destination or an intermediate node with a ―fresh enough‖ route to the destination is located [4]. In this procedure the intermediate node can reply to the RREQ packet only if it has a fresh enough route to the destination. Once the RREQ reaches the destination or an intermediate node with a new sufficient route, the purpose or transitional node responds by unicasting a route reply (RREP) packet (Fig. 2) back to the neighbor from which it first received the RREQ. After selecting and establishing a route, it is maintained by a way preservation process until either the destination becomes complicated to get to along every path from the source or the route is no longer desired.



Network flooding of RREQ

i and j are reliable to each other.

There exists route between two packets.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

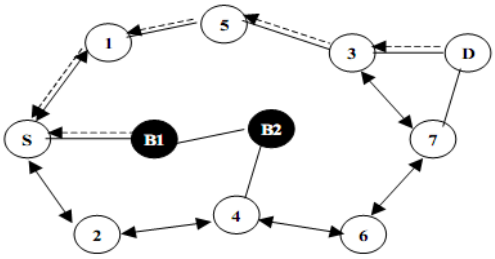
Vol. 2, Issue 10, October 2014

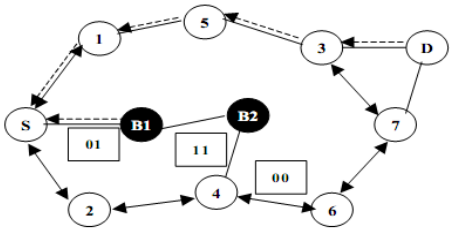
Researchers have proposed solutions to identify and eliminate a single black hole node as well as the multiple black hole attack [1, 4]. However, in the case of multiple black hole nodes acting in coordination even though researchers have come up with different ideas, it gets affected in terms of throughput and efficiency [3].

A. Cross Checking Solution for the Black Hole problem.

1. DRI Table:

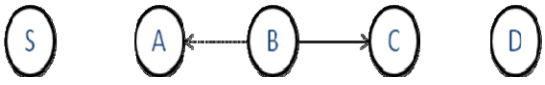
The solution to identify multiple black hole nodes acting in cooperation involves two bits of additional information from the nodes responding to the RREQ of source node S. Each node maintains an additional Data Routing Information (DRI) table. In the DRI table, 1 stands for _true' and 0 for _false'. The first bit —From‖ stands for information on routing data packet from the node (in the Node field) while the second bit —Through‖ stands for information on routing data packet through the node (in the Node field). In reference to the example of Figure 5, a sample of the database maintained by node 4 is shown in Table 1. The entry 1 0 for node 3 implies that node 4 has routed data packets from 3, but has
not routed any data packets through 3 (before node 3 moved away from 4). The entry 1 1 for node 6 implies that, node 4 has successfully routed data
packets from and through node 6. The entry 0 0 for node B2 implies that, node 4 has NOT routed any data packets from or through B2.





Solution for cooperative black hole

o



Watchdog Technique

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

II. CROSS CHECKING

In cross checking, the source node floods the RREQ message to entire network (broadcast), the intermediate node (IN) which first replies or send
RREP message, has to send the information about the
next hop node (NHN) and the DRI table of the Next Hop Node. If the IN node is unreliable the source node contacts the NHN based on the information
provided by IN and checks its DRI Table as well as the DRI table of the NHN, if the node is secure then the packets are transmitted through the secure node.
This is the working of Cross Checking. A pictorial representation of Cross Checking is given below in Fig.5.

B. Watchdog method in terms of better throughput

Our solution uses concepts provided by Sergio Marti et al [3], i.e., Watchdog and Pathrater that significantly improves the throughput in MANET by identifying misbehaving nodes, this concepts is mainly used in DSR (Destination Sequence routing) protocol. Since the DSR doesn‘t support multicast and has a higher memory overhead it is not very efficient when compared to AODV [5]. Hence, we use the Watchdog and Pathrater concept in AODV where the throughput is significantly higher.

Watchdog is used to identify misbehaving nodes. In general, malicious nodes are recognized by eavesdropping on the next hop through Watchdog technique. In AODV protocol, routing data is defined in the source node. This data is passed to the Intermediate nodes in the form of a message until it reaches its intended destination [6]. Therefore each Intermediate node in the path must recognize the node in the next hop. In addition, due to the special features of wireless networks, it is possible to hear messages in the next hop. For example, if node A is in the vicinity of node B, then node A can hear node B's communications. Fig.6. shows how the Watchdog technique operates.
Assume that node S wishes to send a packet to node D. There exists a route form S to D via A, B and C. Imagine now that node A had previously received a packet on route from S to D. The packet contains a message plus routing data. When A sends this packet to B, it keeps a copy of it in its buffer [7]. It then eavesdrops on node B ensuring that B forwards the packet to C. If the packet is heard by B (shown by dotted lines) and it is also identical to what it has in its buffer, this indicates that B has forwarded the packet to C (shown by solid lines). The packet is then removed from the source node buffer. If, on the other hand, the packet is not compared with the packet in the source node buffer in a specific time, the Watchdog adds one to the node B's failure counter. If this counter exceeds the threshold, node A oncludes that node B is malicious and reports this to the source node S. Simulation results show that systems using these two techniques to find their routes are very effective in detecting misbehaving nodes and also increases throughput efficiently [9].

IV. SIMULATION AND RESULTS

The simulation parameters are set up as given in the

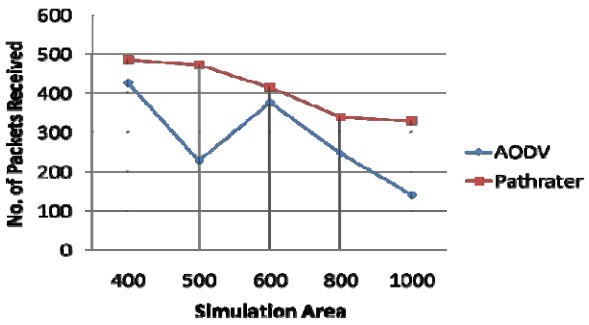


Table.2. Simulation Parameters

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

A. Impact in Number of Nodes.

The node number was set from 10 to 50 and simulated; the throughput in number of packets received was considerably higher in our modified method rather than the proposed one. The throughput was 99.17% in our concept. Fig.7. represents the impact of number of nodes in AODV in presence of Cooperative black hole attack.

B. Impact in Terrain Area.

Here, for the different terrain area the protocol was simulated. The maximum area used was
1000m * 1000m, even in this the Path rater had
highest throughput when compared to the solution provided by Sanjay Ramaswamy [1].

The maximum throughput was around 100% for 400m * 400m area.
Fig.8. represents the Impact of terrain area on black hole.

C. Impact of Speed.

The protocol was simulated for different speed values; the node speed determined its movement in milliseconds, the highest speed set up was around 50ms. The results show that our proposed method had higher throughput when the speed was around 20-30ms, but the solution provided by Sanjay et al [8], had better throughput when kept around

V. CONCLUSION AND FUTURE WORK

In this paper, we studied the problem of Co- operative black hole attack and used the solution provided by Sanjay et al [1] as well as Watchdog method in AODV. The simulation shows that watchdog method had better throughput than the solution provided.
As future work, we intend to develop the performance of the watchdog solution in terms of Speed and Packet loss.

REFERENCES

1. Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks by SanjayRamaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard.
2. Khanaa, V., Mohanta, K., Saravanan, T.,"Comparative study of uwb communications over fiber using direct and external modulations", Indian Journal of Science and Technology, ISSN : 0974-6846, 6(S6) (2013) pp.4845-4847.
3. Security in Wireless Ad Hoc Networks by Amitabh Mishra(Virginia Polytechnic Institute and State University) and KetanM. Nadkarni (Virginia Polytechnic Institute and State University)
4. Kumar Giri, R., Saikia, M., "Multipath routing for admission control and load balancing in wireless mesh networks", International Review on Computers and Software, ISSN : 1828-6003, 8(3) (2013) pp. 779-785.
5. S. Marti et al., ―Mitigating Routing Misbehavior in Mobile Ad Hoc Networks,‖6th Int'l. Conf. Mobile Comp. Net., Aug.2000, pp. 255–65
6. Kumarave A., Udayakumar R., "Web portal visits patterns predicted by intuitionistic fuzzy approach", Indian Journal of Science and Technology, ISSN : 0974-6846, 6(S6) (2013) pp. 4549-4553.
7. Hongmei Deng, Wei Li, and Dharma P. Agrawal, ―Routing Security in Wireless Ad Hoc Network,‖ IEEE Communications Magzine, vol. 40, no. 10, October 2002.
8. Body, Personal, and Local Ad Hoc WirelessNetworks by Marco Conti (Consiglio Nazionale delle Ricerche)
9. Y. Zhang, W. Lee, ―Intrusion Detection in Wireless Ad Hoc Networks,‖ 6th Int'l. Conference Mobile Comp. Net., Mobicom 2000, pp. 275-283, August 2000.