DETECT AND REMOVE CO-OPERATIVE BLACK HOLE ATTACK BY RELYING ON RELIABLE NODE IN MENENT

Sunita Kumari#1, Preeti #2, Neelam #3
# PG (M.Tech) student in RPSGOI Mohindergarh
# Asst. Prof. In yaduwanshi Engineering college Narnul
# Asst. Prof. In DPG engineering college gurgoan
1 sonu.swami6@gmail.com
2 priti16rao@gmail.com
3 neelamlochab2006@gmail.com

Abstract— Now days Wireless networking is an emerging technology that allows users to access information and services electronically, regardless of their geographic position. The use of wireless communication between mobile users has become increasingly popular due to recent performance advancements in computer and wireless technologies. The approach which is the focus of this research is to form a wireless ad hoc network among users wanting to communicate with each other with no pre-established infrastructure. In this paper we discuss Security agents in MANET’s have presented an algorithm for the prevention of cooperative black hole attack in MANET.

Keywords— Menent, black hole, communication, wireless network

I. INTRODUCTION : MOBILE AD HOC NETWORKS
A Mobile Ad Hoc Network (MANET) consists of a set of mobile hosts that carry out basic networking functions like packet forwarding, routing, and service discovery without the help of an established infrastructure. Nodes of an ad hoc network rely on one another in forwarding a packet to its destination, due to the limited range of each mobile host’s wireless transmissions. An ad hoc network uses no centralized administration. This ensures that the network will not cease functioning just because one of the mobile nodes moves out of the range of the others. Nodes should be able to enter and leave the network as they wish. Because of the limited transmitter range of the nodes, multiple hops are generally needed to reach other nodes. Every node in an ad hoc network must be willing to forward packets for other nodes. Thus, every node acts both as a host and as a router. The topology of ad hoc networks varies with time as nodes move, join or leave the network. This topological instability requires a routing protocol to run on each node to create and maintain routes among the nodes.

2. BLACK HOLE ATTACK
Two types of black hole attack can be described in order to distinguish the kind of black hole attack.

2.1 Internal Black hole attack
This type of black hole attack has an internal malicious node which fits in between the routes of given source and destination. As soon as it gets the chance this malicious node make itself an active data route element. At this stage it is now capable of conducting attack with the start of data transmission. This is an internal attack because node itself belongs to the data route. Internal attack is more vulnerable to defend against because of difficulty in detecting the internal misbehaving node.

2.2 External Black hole attack
External attacks physically stay outside of the network and deny access to network traffic or creating congestion in network or by disrupting the entire network. External attack can become a kind of internal attack when it take control of internal malicious node and control it to attack other nodes in MANET. External black hole attack can be summarized in following points:-

1. Malicious node detects the active route and notes the destination address.
2. Malicious node sends a route reply packet (RREP) including the destination address field spoofed to an unknown destination address. Hop count value is set to lowest values and the sequence number is set to the highest value.
3. Malicious node send RREP to the nearest available node which belongs to the active route. This can also
be send directly to the data source node if route is available.
4. The RREP received by the nearest available node to the malicious node will relayed via the established inverse route to the data of source node.
5. The new information received in the route reply will allow the source node to update its routing table.
6. New route selected by source node for selecting data.
7. The malicious node will drop now all the data to which it belong in the route.

As figure 2.2 Blackhole attack specification specifies that in AODV black hole attack the malicious node “A” first detect the active route in between the sender “E” and destination node “D”. The malicious node “A” then send the RREP which contains the spoofed destination address including small hop count and large sequence number than normal to node “C”. This node “C” forwards this RREP to the sender node “E”. Now this route is used by the sender to send the data and in this way data will arrive at the malicious node. These data will then be dropped. In this way sender and destination node will be in no position any more to communicate in state of black hole attack.

A Black hole node also operates by replying for a RREQ message come from any source in the network as the node itself is a nearest node to the destination and receive all the packet of data meant for some other node.

3 Co-Operative Black hole attack problem
working strategy

This work is about to detect the cooperative blackhole nodes in a mobile network and to generate a secure and reliable path. In this work, a nearest neighbor analysis will be performed to identify an active blackhole node in the active path. As the particular nodes sends a ROUTE REQ message to the neighboring nodes and if any node does not return the reply message [REPLY] in the specified time interval then it assumes that the node is a blackhole node. To ensure the status of node, all neighbors to that node send the request to that suspected node. If maximum nodes not get the reply, then that particular node is declared as the blackhole node and its status is set to be disable by including a status bit. Once the blackhole node is detected, next neighbor is detected as the compromising node and the transmission is performed through that compromising node.

In this section, we prepare a methodology for identifying multiple black hole nodes co-operating each other as a group with slightly modified AODV protocol by introducing Data Routing Information (DRI) Table and Cross Checking.

3.1 Data Routing Information 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 3.3, 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.
Table 3.1 table of data routed from, and routed to nodes maintained by node 4.

<table>
<thead>
<tr>
<th>Node #</th>
<th>Data Routing Information</th>
<th>From Node</th>
<th>Through Node</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td></td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td></td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>B2</td>
<td></td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Figure 3.1: Solution to avoid cooperative black hole attack

Figure 3.2: Solution to identify multiple black hole nodes in one-time check

CONCLUSIONS

In this paper, we designed and implemented a new modified algorithm against a well-known insider active attack cooperative black hole attack. An analysis on the nearest neighbour node within the network where the multiple black hole attacker nodes are present, prevents the formation of the black hole and identifies the safe and secure route towards destination.

The results of this thesis show that in the presence of 10% misbehaving nodes in the scenario of 26 nodes throughput increases 43% and packet delivery ratio increases approximately 60% to 65% in the presence of modified algorithm. On the basis of results, it is concluded that modified algorithm is able to counter the cooperative black hole attack in MANET.

REFERENCES


Umair Sadiq, "CRISP: Collusion–Resistant Incentive–Compatible Routing and Forwarding in Opportunistic Networks", MSWiM’12, October 21–25, 2012, Paphos, Cyprus. ACM 978-1-4503-1628-6/12/10


Garima Gupta, "Reference based approach to Mitigate Blackhole Attacks in Delay Tolerant Networks”, Q2SWinet’12, October 24–25, 2012, Paphos, Cyprus. ACM 978-1-4503-1619-4/12/10


Enrique Hernández-Orallo, "Evaluation of Collaborative Selfish Node Detection in MANETs and DTNs”, MSWiM’12, October 21–25, 2012, Paphos, Cyprus. ACM 978-1-4503-1628-6/12/10