Detection/Removal of Black Hole Attack in Mobile Ad-Hoc Networks

Sandeep Lalasaheb Dhende1, Prof. Mrs. D. M. Bhalerao2
Department of E&TC, Sinhgad College of Engg., Pune, India.

Abstract- The inherent features (such as-open medium, dynamically changing network topology, lack of centralized monitoring and management point, and lack of a clear line of defense) of the MANET make it vulnerable to a wide range of attacks. There is no guarantee that a communication path is free from malicious or compromised nodes which deliberately wish to disrupt the network communication. So protecting the mobile ad-hoc network from malicious attacks is very important and challenging issue. In this paper we address the problem of packet forwarding misbehavior and propose a mechanism to detect and remove the black attack.

Keywords: ad hoc networks, black hole, security, routing, AODV

I. INTRODUCTION

Ad hoc network is a wireless network without having any fixed infrastructure. Each mobile node in an ad hoc network moves arbitrarily and acts as both a router and a host [1]. A wireless ad-hoc network consists of a collection of "peer" mobile nodes that are capable of communicating with each other without help from a fixed infrastructure. The interconnections between nodes are capable of changing on a continual and arbitrary basis. Nodes within each other's radio range communicate directly via wireless links, while those that are far apart use other nodes as relays. Nodes usually share the same physical media; they transmit and acquire signals at the same frequency band. However, due to their inherent characteristics of dynamic topology and lack of centralized management security, MANET is vulnerable to various kinds of attacks [2]. Black hole attack is one of many possible attacks in MANET. Black hole attack can occur when the malicious node on the path directly attacks the data traffic and intentionally drops, delay or alter the data traffic passing through it [3] [4]. There is lots of detection and defense mechanisms to eliminate the intruder that carry out the black hole attack. We present a technique to identify black attack and a solution to discover a safe route avoiding black hole attack.

II. BLACK HOLE ATTACK PROBLEM

In an ad hoc network that uses the DSR/AODV protocol, a black hole node pretends to have a fresh enough routes to all destinations requested by all the nodes and absorb the network traffic.

When source node broadcasts the RREQ message for any destination, the black hole node immediately responds with the RREP message and with next hop details. 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 node assume that the destination is behind the black hole node and next hop node and perceives the other RREP packets with next hop node coming from other nodes [5].

![Figure 1. Propagation of RREQ and RREP from A to E](image)

The source node then start to send out its data packets to the black hole node and after small time interval to the other node, trusting that these packets will reach to the destination either by one link [6].

In the following illustrated Figure 2, imagine a malicious node ‘M’. When node ‘A’ broadcast a
RREQ packets, nodes ‘B’ ‘D’ and node ‘M’ receives it. Node ‘M’ being a malicious node does not check up with its routing table for the requested route to node ‘E’.

Hence, it immediately sends back a RREP packet, claiming 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’. However in that solution next hope also behaves as a malicious node they cannot identify it.

III. SOLUTION

We proposed a solution that is an enhancement of the basic AODV routing protocol, which will be able to avoid and detect black holes. To reduce the probability it is proposed to wait and check the replies from all the neighboring nodes to find a safe route.

According to this proposed solution the requesting node without sending the DATA packets to the reply node at once, it has to wait till other replies. After receiving the first request it sets timer in the ‘Timer Expired Table’, for collecting the further requests from different nodes. It will store the ‘Sequence number, and the time at which the packet arrives, in a first ‘Collect Route Reply Table’ (CRRT).

After the timeout value, we considered another destination node D1 in same network to repeat route establishment process to collect route replies from same nodes in second ‘Collect Route Reply Table’ (CRRT). Here we can obtain two different ‘Collect Route Reply Table’ (CRRT) because of two route establishment process as shown below.

<table>
<thead>
<tr>
<th>Source</th>
<th>Reply</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>s</td>
<td>M</td>
<td>D</td>
</tr>
<tr>
<td>s</td>
<td>1</td>
<td>D</td>
</tr>
<tr>
<td>s</td>
<td>2</td>
<td>D</td>
</tr>
</tbody>
</table>
Table 2. Routing details

<table>
<thead>
<tr>
<th>Source</th>
<th>Reply</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>s</td>
<td>M</td>
<td>D1</td>
</tr>
<tr>
<td>s</td>
<td>2</td>
<td>D1</td>
</tr>
<tr>
<td>s</td>
<td>1</td>
<td>D1</td>
</tr>
</tbody>
</table>

Now compare first route reply from both the ‘Collect Route Reply Table’ (CRRT), if we found the same node replying very firstly in two different route establishment processes then such node can be malicious node. Then we can choose second route reply from first routing table for further communication as shown below.

According to this proposed solution we considered another destination node D1 in same network, to repeat route establishment process to collect route replies from same nodes in second ‘Collect Route Reply Table’ (CRRT). Which shows, if S wants to transmit to D1. So it first transmits the route request to all the neighboring nodes. Here node 1, node M and node 2 receive this request. The malicious node has no intention to transmit the DATA packets to the destination node D but it wants to intercept/collect the DATA from the source node S. So it immediately replies to the request as M. Instead of transmitting the DATA packets immediately through M, S has to wait for further reply from the other nodes. After some time it will receives the reply from node 1 as 1 and node 2 as 2 as shown in table.

Figure 4. Solution to Black hole

Thus Black hole attacks can greatly be detected and reduced and DATA packets can be transmitted along with chosen path.

IV. WORKING PRINCIPLE of AODV

In the above figure 3, S wants to transmit to D. So it first transmits the route request to all the neighboring nodes. Here node 1, node M and node 2 receive this request. The malicious node has no intention to transmit the DATA packets to the destination node D but it wants to intercept/collect the DATA from the source node S. So it immediately replies to the request as M. Instead of transmitting the DATA packets immediately through M, S has to wait for further reply from the other nodes. After some time it will receives the reply from node 1 as 1 and node 2 as 2.

Now compare first route reply from both the ‘Collect Route Reply Table’ (CRRT), if we found the same node replying very firstly in two different route establishment processes then such node can be malicious node. Then we can select second route reply from first routing table for further communication as shown below.
V. CONCLUSION AND FUTURE WORK

According to the proposed solution the required security in MANET can be achieved with minimum delay and control overhead and simultaneously we can detect the Black hole attack and transmit DATA packets to the destination.

As future work, we intend to develop simulations to analyze the performance of the proposed solution.

REFERENCES


