An Efficient Algorithm for Detecting and Removing Black hole Attack for Secure Routing in Mobile Ad-hoc Network

Viswa Jhananie K.R,
Assistant Professor, Seshaderipuram Academy of Business Studies, Bangalore, Karnataka-560076, India.

Abstract
Securing Mobile Ad-hoc Network (MANET) is challenging because they do not have any fixed infrastructure. In MANET, all the networking functions are performed by the nodes themselves in a self-organizing manner. Since, the mobile nodes do not require any pre-installed infrastructure, they can be utilized in places such as battle field, disaster recovery and where ever there is a need for wireless network. Ad-hoc networks are highly susceptible to security attacks. Black hole attack is one of the serious attacks in MANET. In this paper, we propose two different solutions for detecting and removing black hole attack, which will enable a secured routing in MANET.

1)Algorithm using watchdog and 2) Two way routing protocol method.

Keywords: MANET, black hole attack, watchdog, routing protocol, mobility model.

Introduction
Mobile ad-hoc network is an autonomous, multihop network. The advantage of this network is that, it can be used for communication purpose throughout the world while in mobile. In MANET, each node acts as a router and also once the route is found, nodes will start forwarding packets to the correct correct node in the network [1]. These networks do not have any fixed or static topology. Since the routers are free to move randomly, deployment of these networks is very easy [2]. MANETs are vulnerable to routing attacks like wormhole attack, Sybil attack, grayhole attack, black hole attack and many more attacks due to its dynamic nature[3]. Black hole attack is one of the serious attacks in MANET.

In this paper, we present two solutions to prevent MANET from black hole attack. In the first solution, black hole nodes are detected and removed from the routing path. In the second solution, black hole nodes are detected and that route is avoided for communication among the nodes. Section-2 discusses the review of the related work. Section-3 is dedicated for routing protocols. Section-4 describes about black hole attack in MANET. Section-5 will focus on the methodology. Section-6 is dedicated to simulation parameters, performance metrics and simulation results. We close our work in section-7 with conclusion and suggestions for future work.

Literature Review
Shalini et al [4] have proposed a mechanism for detecting and removing black and gray hole attacks. In this, instead of sending the entire data, data is sent in small sized blocks. The flow of message is monitored at its neighborhood both by its source and destination independently. Thus, the malicious node is detected and removed in between the transmission of two such blocks with a constant check at both the ends.

Kamatchi et al [5] have proposed a solution for the prevention of black hole attack by using receive route reply method (RRR) and Shamir’s secret sharing method. The node with the largest sequence number is considered as a black hole and that route towards destination is discarded when using RRR method. In Shamir’s secret sharing method, the original packet is divided in to some bytes of shares and the copy of shares are taken and forwarded towards multiple random routes. All the packets will be reconstructed under reconstruction phase.

Vipan et al [6] have proposed a solution by modifying the working of the source node. Initially, waiting time is set to the source node till it receives RREQ from other neighboring nodes. After that, the current time is added with waiting time. The destination sequence number is stored along with its node ID. The destination sequence number is compared with the source node sequence number and if there are more differences, then the node is identified as malicious. The entry of the node is removed from route request table.

Murtuza et al [7] have proposed three different algorithms namely polynomial algorithm and two heuristic based algorithms to improve the quality of localization and to secure distance based localization in the presence of cheating beacon nodes. The accuracy of localization algorithm is also verified.

Sanjay et al [8] have presented a technique to identify multiple black holes acting in group and proposed a solution to discover a safe route avoiding co-operative black hole attack. Modified AODV routing protocol with DRI – Data Routing Information.

Routing Protocols
In MANET, routing protocols are needed to handle dynamic communication and also find route so as to deliver data packets to the correct destination [9]. Effective and accurate routing protocols are required to handle mobility of nodes. Several routing protocols and security extensions have been proposed to specifically address the area of Mobile Ad-hoc Networks. The protocols that are used for routing purpose can be broadly classified into three types. They are proactive or table driven protocols, reactive or on demand protocol and hybrid protocol.
Proactive or Table Driven Protocol

Each mobile node in this network maintains routing table for destination node. To maintain consistency, the routing table is updated periodically for each change in the network [10]. This results in frequent route updates. Eg: Destination Sequence Distance Vector (DSDV). They maintain consistent, up to date routing information of the whole network. The delay in communication is minimized. It also determines quickly which nodes are present or reachable in the network.

Reactive or on Demand Protocol

These protocols discover the routes when needed. They decrease the control traffic messages overhead at the cost of increased latency while discovering the new routes. Eg: Ad-hoc On Demand Distance Vector Protocol (AODV). To find the path to the destination, all mobile nodes work in cooperation using routing control messages such as route request (RREQ), route error (RERR) and route reply (RREP). Thus, AODV offers quick adaptation to dynamic network conditions.

Hybrid Protocols

This combines the characteristics of both proactive and reactive routing protocols. In this method, communication takes place when nodes are close to each other. It was designed to reduce the latency during the discovery of route in reactive routing protocols and to decrease the control overhead of proactive routing protocols [11].

Black Hole Attack

It is one of the serious attacks in MANET. This attack affects the traffic in the network. In this attack, the malicious node waits for the neighbors to initiate RREQ packet. It starts advertising itself as having the shortest path to all the nodes in the environment by sending fake route reply with a modified sequence number. This makes the source node to assume that this node is having a new route to the destination. Thus the source node ignores the RREP packet from other nodes and begins to send data packets over malicious node.

In black hole attack, the malicious node waits for the neighbors to initiate RREQ packet. As the node receives RREQ (Route Request) packet, the malicious node advertises itself as having the shortest path to all the nodes in the environment by sending fake route reply with a modified sequence number. So that the source node assumes that the node is having a fresh route towards destination. The source node ignores RREP (Route Reply) packet received from other nodes and begins to send data packets over malicious node. By doing this, the malicious node can deprive the traffic from source node and does not allow forwarding any packet anywhere. Thus, all packets in the network are dropped.

Methodology

In this paper, we propose two solutions to prevent nodes from black hole attack. They are

An efficient algorithm using watchdog:

In general, watchdog is a monitoring mechanism that is used to detect the misbehaving nodes in the network. A sample data
is sent from source to destination node in all the available routes periodically. Destination node will broadcast the received details to watchdog. A routing table is maintained by watchdog with route Id, size of data sent, size of data received, failure count and continuous/not columns. Watchdog identifies the malicious node within a specified time interval in each route. The accumulation of data response from destination helps watchdog to decide whether that route has malicious node or not.

When the data loss is continuous, then watchdog identifies the presence of malicious node in that route and deletes the route from the table. Else, the data loss threshold value is used by watchdog to find malicious node’s route. The advantage of this approach is, using watchdog, we detect the data loss not only in single route, but also in all the available routes. The watchdog does not spend time in waiting for the reply from destination node from each route, since the sample data is sent periodically in all the routes. One more advantage is, unlike other watchdog process, it accumulates the data count sent and received for specified number of times and uses the same for finding the malicious node in the particular route. This approach helps in avoiding unwanted over load of watchdog. The following routing table shows the details maintained in terms of data accumulation.

### Table 1: Routing table to identify the data loss

<table>
<thead>
<tr>
<th>Route Id</th>
<th>Size of Data Sent</th>
<th>Size of Data Received</th>
<th>Failure Count</th>
<th>Continuous or Not</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1024</td>
<td>998</td>
<td>1</td>
<td>Yes</td>
</tr>
<tr>
<td>3</td>
<td>900</td>
<td>900</td>
<td>0</td>
<td>No</td>
</tr>
<tr>
<td>5</td>
<td>1590</td>
<td>1500</td>
<td>1</td>
<td>Yes</td>
</tr>
<tr>
<td>7</td>
<td>1350</td>
<td>1350</td>
<td>0</td>
<td>No</td>
</tr>
</tbody>
</table>

### Algorithm

**Step-1:** Consider a network with N elements.

**Step-2:** Let \( N_i \) be a stream of sample data.

**Step-3:** The data is treated as discrete time series (for the loss of data).

**Step-4:** Stream of sample data is sent and monitored by watchdog until time ‘\( t \)’ becomes 5ms (say). (ie) \( X_1^t, X_2^t, \ldots X_i^t, X_i^t = 0 \)

**Step-5:** The monitored data values are denoted by \( W_i = (X_i^t, \ldots X_i^t), \) where \( X \) is the accumulated data and \( k \) is the most recently seen data.

**Step-6:** For a function ‘\( f \)’ which is defined as \( f(W_i) \) in time interval, ‘\( t \)’, if \( f(W_i) \) exceeds threshold value \( v_i \), watchdog identifies that node as malicious.

**Step-7:** Therefore the watchdog event in a network is a random variable, \( RV_i \) such that,

\[
RV_i = \begin{cases} 
0, & \text{if } f(W_i) >= v_i \\
1, & \text{otherwise} 
\end{cases}
\]

### Two way Routing Protocol:

The source node sends RREQ (Route Request) to the destination node in two different routes at the same time. In this method, we use two different protocols namely Ad-hoc On Demand Distance Vector (AODV) protocol for one route and Dynamic Source Routing (DSR) protocol in another route for forwarding the data packets to one destination. When attack occurs in any one protocol, the data reaches the destination through the other route with a different protocol, since both the protocols carry the same data. In our simulation, the data through AODV protocol is attacked by the malicious node and DSR protocol is used as an alternate for forwarding the data to the destination.

**Algorithm**

data (dt) starts from source (AODV protocol) to destination, D
data (dt) starts from source (DSR protocol) to destination, D

if (attack occurs in AODV protocol) then data (dt) reaches destination, D through DSR

end if

if (attack occurs in DSR protocol) then data (dt) reaches destination, D through AODV

end if

**Simulation Results**

We have used NS-2 for our simulation. The parameters used for simulation is summarized in the table.
Table 2: Simulation Parameters

<table>
<thead>
<tr>
<th>S.no</th>
<th>Parameters</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Channel type</td>
<td>Wireless</td>
</tr>
<tr>
<td>2</td>
<td>Propagation model</td>
<td>Two way ground</td>
</tr>
<tr>
<td>3</td>
<td>MAC type</td>
<td>802_11</td>
</tr>
<tr>
<td>4</td>
<td>Mobility model</td>
<td>random waypoint model and City section mobility model</td>
</tr>
<tr>
<td>5</td>
<td>Maximum packet</td>
<td>50</td>
</tr>
<tr>
<td>6</td>
<td>Protocols used</td>
<td>AODV and DSR</td>
</tr>
<tr>
<td>7</td>
<td>Simulation Period</td>
<td>100ms</td>
</tr>
</tbody>
</table>

Performance Metrics

Throughput:
It is the average rate of successful message delivery over a communication channel. It can be calculated as

Throughput (Kbps) = received packet size * 8 / data transmission period

Packet delivery ratio:
It is ratio between the amount of incoming data packets and actually received data packets. It can be given as
Packet Delivery Ratio (PDR) = total of received packets / total of sent packets

End-to-end delay:
It is the time taken by a packet to travel a path from source to destination. It can be given as, Delay = (total number of packets delivered) * (end time – start time) * 1000

Simulation Results

Algorithm using watchdog:

Throughput:

Figure 3: Throughput rates – with watchdog and without watchdog

Packet Delivery Ratio:

Figure 4: Packet Delivery Ratio – with watchdog and without watchdog

End-to-end delay:

Figure 5: End-to-end delay – with watchdog and without watchdog
Two way routing protocol:

Throughput:

Packet Delivery Ratio:

End-to-end delay:

Conclusion

Mobile Ad-hoc Networks (MANETs) are vulnerable to various kinds of attack because of its dynamic infrastructure. We have given two different solutions (i) algorithm using watchdog and (ii) two way routing protocol for blackhole attack, which is one of the serious attack in MANET. In our simulation, we have used random way point model for watchdog and city section mobility model for two way routing protocol. The simulation results shows better performance in throughput under two way routing protocol. The number of packets delivered is more when watchdog is used and the delay is also consistently reduced under watchdog method. So, we conclude that watchdog can be considered as a better solution in securing data from blackhole attack.

Future Enhancement

We have used random waypoint model and city section mobility model for our simulation. The same work can be carried over with different mobility models and with different protocols.

References


