Chapter VII

PERFORMANCE OF SWARM BASED INTRUSION DETECTION SYSTEM UNDER DIFFERENT MOBILITY CONDITIONS IN MANET

7.0 INTRODUCTION

In mobile ad hoc network (MANET), the issues such as limited bandwidth availability, dynamic topology, etc. cause the process of intrusion detection to be more complex. The movement of nodes plays the major role. Here, three (Swarm based Intrusion detection) SBDTs are created namely SBDT-LOW-MOBILITY, SBDT-MEDIUM-mobility and SBDT-HIGH-MOBILITY. In all the three SBDTs, the nodes with the highest trust value, residual bandwidth and residual energy are selected as active nodes using the swarm agents. Every active node examines its neighbor nodes within its radio transmission range and gathers the trust value from all monitored nodes. The active nodes will always be changing as per the trust thresholds. Upon collaborative exchange of the trust values of the monitored nodes among the active nodes, if the active node finds any node below a minimum trust threshold, then the node is marked as malicious. When the source receives alert message about the malicious node, a defense technique is deployed to filter the corresponding malicious node from the network. By simulation results, we show that the SBDT-HIGH-MOBILITY is producing better results while varying the nodes and SBDT-LOW-MOBILITY is producing better results while varying the attackers. From this it is found that the mobility condition also plays a major role during the swarm based intrusion detection.

7.1 SBDT CREATION AND NODE MONITORING STRATEGY

Here in this work, the Random waypoint mobility model [28] with three different mobility conditions are used. They are low mobility, medium mobility and high mobility. In low mobility, the pause time used
is 400 sec. In medium mobility, the pause time used is 300 sec. In high mobility, the pause time used is 120 sec. Pause time is nothing but the rest period required for a node to move from one location to another. In high mobility, the nodes will start moving from a location quickly. In low mobility, the nodes will start moving from a location slowly, and in medium mobility the nodes will start moving from a location between the low mobility and high mobility. The header of the ant agents (SBDTs) includes the fields which are illustrated in table 3.1. The procedure used by the three SBDTs to select the active nodes is shown in the following algorithm. So it is possible to identify which mobility condition based SBDT performs well when compared to the others.

**Algorithm:**

1) Here three SBDTs are created using the three mobility conditions and they are named as SBDT-LOW-MOBILITY, SBDT-MEDIUM-MOBILITY and SBDT-HIGH-MOBILITY.

2) In each SBDT, the FA is launched in S and it traverses through all intermediate nodes along the path towards D.

3) FA, on reaching every node, computes the parameters residual energy, residual bandwidth, connectivity and trust (as explained in section 3.2.1.1, 3.2.1.2, 3.2.1.3, and 3.2.1.4), and updates its header with the information about the node (as per fig 3.1).

4) With the gathered information from all the hops, FA reaches D.

5) When FA reaches D, D generates BA and transfers all the information of FA into BA. The BA takes the same path as that of its corresponding FA, but in the reverse direction.

6) The BA updates the header field at the neighboring nodes for all the entries related to the FAs destination node.

7) The BA upon reaching the source delivers the status of all the nodes. The source then selects the nodes with the maximum trust value, residual bandwidth and residual energy as the active nodes. (shown in fig 3.1).
8) The steps from 3 to 7 are performed for all three SBDTs mentioned in step 1.

After going through the above 8 steps by the three different SBDTs, the malicious nodes are identified by each SBDT and it is informed to the source node by the alert messages. So the source node can employ a defense mechanism to ignore those malicious nodes in the path selection.

7.2 PERFORMANCE EVALUATION AND ENHANCEMENT

Here the comparison of three SBDTs is performed for the Routing Attacks and their performance is evaluated using various metrics namely, Average Packet Delivery Ratio, end to end delay and Average Packet Drop.

Network Simulator Version-2 (NS2) [27] is used to simulate our proposed algorithm. It is the most popular and one of the most widely used network simulators for wired and wireless networks. Moreover, it is the most commonly used simulator for studies on MANETs, and it comes with a rich set of algorithms and models. In our simulation, the channel capacity of mobile hosts is set to the same value: 2 Mbps. The distributed coordination function (DCF) of IEEE 802.11 for wireless LANs is used as the MAC layer protocol. It has the functionality to notify the network layer about link breakage. The simulation settings and parameters are summarized in table 8.1.

In this simulation, mobile nodes move in a 1000 meter x 1000 meter region for 50 seconds simulation time. The number of nodes is varied as 20, 40, 60, 80 and 100. It is assumed that each node moves independently with the same average speed. All nodes have the same transmission range of 250 meters. In this simulation, the node speed is 10 m/s. The simulated traffic is Constant Bit Rate (CBR). The mobility model used by the nodes in the MANET environment is random way point model which is the most widely used mobility pattern scenario.
Table 7.1 Simulation Settings in ns2 Used by Different Mobility Conditions

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>NO. OF NODES</td>
<td>20, 40, 60, 80 AND 100.</td>
</tr>
<tr>
<td>AREA SIZE</td>
<td>1000 X 1000</td>
</tr>
<tr>
<td>MAC</td>
<td>802.11</td>
</tr>
<tr>
<td>RADIO RANGE</td>
<td>250M</td>
</tr>
<tr>
<td>SIMULATION TIME</td>
<td>50 SEC</td>
</tr>
<tr>
<td>TRAFFIC SOURCE</td>
<td>CBR</td>
</tr>
<tr>
<td>PACKET SIZE</td>
<td>512</td>
</tr>
<tr>
<td>SPEED</td>
<td>10M/S</td>
</tr>
<tr>
<td>NO. OF ATTACKERS</td>
<td>2, 4, 6, 8 AND 10.</td>
</tr>
<tr>
<td>LOW MOBILITY(PAUSE TIME)</td>
<td>400 SEC</td>
</tr>
<tr>
<td>MEDIUM MOBILITY(PAUSE TIME)</td>
<td>300 SEC</td>
</tr>
<tr>
<td>HIGH MOBILITY(PAUSE TIME)</td>
<td>120 SEC</td>
</tr>
</tbody>
</table>

7.3 RESULTS AND DISCUSSION

Here the three different SBDTs are evaluated using the following performance metrics.

7.3.1 Performance Metrics

**Average Packet Delivery Ratio:** It is the ratio of the number of packets received successfully and the total number of packets transmitted.

**Average-end-to-end Delay:** It is the total time delay taken by the nodes to transmit the data to the receiver.

**Average Packet Drop:** It is the average number of packets dropped by the misbehaving nodes.

7.3.2 Results

Here two different experiments are conducted:

A. Based On Nodes

In the first experiment, the number of nodes is varied as 20, 40, 60 and 80 and 100 and the attackers are set to 2.
Fig 7.1: Nodes Vs Packet Delivery Ratio

In Figure 7.1, as the nodes are increasing, the packet delivery ratio of SBDT-HIGH-MOBILITY is higher than the other two SBDTs.

Fig 7.2: Nodes Vs Delay

In Figure 7.2, even as the nodes are increasing, the delay of SBDT-HIGH-MOBILITY is considerably lower than the other two SBDTs.

Fig 7.3: Nodes Vs Packets Drops

In Figure 7.3, even as the nodes are increasing, the packet drops of SBDT-HIGH-MOBILITY are lower than the other two SBDTs.
B. Based on Attackers

In the second experiment, the number of attackers is varied as 2, 4, 6, 8 and 10 in a 100 nodes environment. Now the performance of three SBDTs is examined as follows.

**Fig 7.4: Attackers Vs Packet Delivery Ratio**

In Figure 7.4, even as the attacker nodes are increasing, the PDR of SBDT-LOW-MOBILITY is better than the other two SBDTs.

**Fig 7.5 Attackers Vs End to End Delay**

In Figure 7.5, even as the attacker nodes are increasing, the delay of SBDT-LOW-MOBILITY is better than the other two SBDTs.
In Figure 7.6, even as the attacker nodes are increasing, the packet drop of SBDT-LOW-MOBILITY is considerably lower than the other two SBDTs.

**7.4 CONCLUSION**

This chapter examines the performance of swarm based intrusion detection system under three mobility conditions and is compared for the routing layer attacks in MANET. All the three SBDTs use the forward and backward ants to select the active nodes (valid nodes) for data transmission. The performance of SBDT-high-mobility is found to be better while varying the nodes and the performance of SBDT-low-mobility is found to be better while varying the attacker nodes.

In future, the performance of these three SBDTs can be compared using some more performance metrics.