CHAPTER VI

PERFORMANCE COMPARISON OF TWO SWARM BASED INTRUSION DETECTION SYSTEMS FOR THE VARIOUS ROUTING ATTACKS IN MANET

6.0 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. In order to overcome these drawbacks, this chapter proposes the comparison of two swarm based efficient distributed intrusion detection systems for MANET. In the first technique, swarm agents are utilized to select the nodes with highest trust value, residual bandwidth and residual energy as active nodes. Each active node monitors its neighbor nodes within its transmission range and collects the trust value from all monitored nodes. The active nodes adaptively changes 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. In the second technique in addition to the first technique, forward and backward ants are utilized to obtain the mean value of nodes between the first received RREQ and RREP packets. Based on this estimation, the source node decides the node as valid or malicious. By simulation results, we show that the second technique is more efficient intrusion detection mechanism than the first technique for identifying more attackers in MANET.
6.1 SWARM BASED NODE MONITORING STRATEGY 1

6.1.1 Parameters for Active Nodes Selection

The parameters used to select the active nodes are residual energy, bandwidth, coverage and connectivity and trust which are described in the following sections.

6.1.1.1 Computation of the Residual Energy

Table-6.1: Header fields used by ant agents in SDIDS1

<table>
<thead>
<tr>
<th>NODE ID</th>
<th>SEQ. NO.</th>
<th>RESIDUAL ENERGY</th>
<th>RESIDUAL BANDWIDTH</th>
<th>CONNECTIVITY</th>
<th>TRUST</th>
</tr>
</thead>
</table>

After time $t$, the energy consumed by the node ($E(t)$) is computed as follows.

$$E(t) = P_{tx} \alpha + P_{re} \beta$$

(6.1)

Where $P_{tx} =$ Number of data packets transmitted by the node after time $t$, $P_{re} =$ Number of data packets received by the node after time $t$, $\alpha$ and $\beta$ are constants. Its value ranges between 0 and 1.

The residual energy $E_R$ of a node at time $t$, can be calculated using the initial energy as:

$$E_R = E_i - E(t)$$

(6.2)

6.1.1.2 Residual Bandwidth Calculation

The residual bandwidth is calculated using the local bandwidth and the minimum bandwidth among the neighboring nodes. The difference between the local bandwidth $BW_{loc}$ and $BW_{min}$ is the residual bandwidth.
6.1.1.3 Trust value \( T \)

The trust values of the nodes can be estimated from the forwarding behavior of the intermediate nodes. The trust value of a node is decremented \([71]\) if the node does not forward sufficient number of packets or the forwarding delay is high or malicious packets are injected.

The active nodes are adaptively changed depending on the above 3 factors.

6.1.1.4 Coverage and Connectivity Criteria

For predicting the future state of the network \([24]\), the mobility is estimated which is defined as follows.

\[
RS_i = \frac{1}{\Delta t} |D_{avg_i}(t) - D_{avg_i}[t + \Delta t]| 
\]

(6.3)

\[
D_{avg_i} = \frac{1}{n} \sum_{j=1}^{n} D_{(i,j)}(t) 
\]

(6.4)

\[
D_{(i,j)} = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2} 
\]

(6.5)

Where \( RS_i \) represent the relative speed of the nodes

\( D_{avg_i}(t) \) represent the average distance among the node \( i \) and its neighbors at time \( t \).

\( n \) is the number of neighbors of node \( i \)

\( D_{(i,j)}(t) \) is the distance between node \( i \) and node \( j \).

\( x \) and \( y \) represent the coordinates of the node.
The degree of the node is calculated as follows.

\[ Z_i(t) = \sum c_{i,j}(t) \]

(6.6)

Where \( c_{i,j} \) is a direct wireless link between node i and j at time t.

Thus the node connectivity is computed using the following equation.

\[ \text{Connectivity} = \delta \cdot R_{Si} + \sigma \cdot Z_i \]

(6.7)

where \( \delta \) and \( \sigma \) are constants.

6.1 SELECTION OF THE ACTIVE NODES

Swarm intelligence technique based on ant colony optimization (ACO) is used for selecting active nodes. The forward ant agent (FA) establishes the pheromone track to the source node (S), while backward ant agent (BA) establishes the pheromone track to the destination (D). The header of the ant agents (SDIDS1) includes the fields which are illustrated in table 6.1. The procedure for selecting the active nodes is given in algorithm-1.

Algorithm -1:

[1] The FA is launched in S and it traverses through all nodes along the path towards D.

[2] FA on reaching every node, computes the parameters residual energy, residual bandwidth, connectivity and trust (as explained in sections 6.1.1.1, 6.1.1.2, 6.1.1.3, and 6.1.1.4), and updates its header with the information about the node (as per fig 3.1).

[3] With the gathered information from all the hops, FA reaches D.
[4] 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.

[5] The BA updates the header field at the neighboring nodes for all the entries related to the FAs destination node.

[6] 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).

[7] If this algorithm decides a particular node as an active node then the node status field in MN-table is set to 1 (valid node).

Otherwise the node state for that node in MN-table is set to 0 (malicious node).

6.3 SWARM BASED NODE MONITORING STRATEGY 2

The MAC and routing layer must support each other to detect attacker and adversaries during the operations in MAC layer. It is possible to have more attacks in MAC layer. The attacker may pretend the channel as busy such that no node or user transmits their data. This attack consequently leads to DoS attack in the network, which drastically reduces the network performance. To detect and prevent such kind of attacks, our technique utilizes swarm based node monitoring strategy2.

Table-6.2 Format of C-Table Used by SDIDS2

<table>
<thead>
<tr>
<th>NODE ID</th>
<th>SID</th>
<th>DID</th>
<th>RECEIVED TIME OF RREQ PACKET</th>
<th>SEQ. NUMBER OF RREQ PACKET</th>
<th>RECEIVED TIME OF RREP PACKET</th>
<th>SEQ. NUMBER OF RREP PACKET</th>
</tr>
</thead>
</table>

When the source has data to be transmitted, it broadcasts RREQ message and the destination broadcasts back the RREP message towards the source. While receiving RREQ message, each intermediate node records the time of first RREQ packet it has received. The RREQ packet is kept tacked with its RREQ sequence number. Similarly, each intermediate node stores the time and sequence number of first RREP packet it has
received. The table that contains this information is known as counter table (C-Table). The format of C-table is shown in table-6.2.

To monitor the network, the source periodically injects forward ants (FA) in the network. Each FA travels towards random destination to collect mean time between received times of RREQ and RREP packets. While returning from the destination, the backward ant (BA) updates this mean time in its pheromone table. Finally, the FA reaches the destination.

Every source has mean table (MN-Table) to store the mean times of nodes collected by ants. When the BA reaches the source node, it updates the mean value of nodes in MN-Table. Let $Th_{rd}$ be the route discovery threshold value. The source compares the mean value of every node with $Th_{rd}$. Mean values of nodes less than or equal to $Th_{rd}$ are noted as valid nodes. Nodes that have mean value more than $Th_{rd}$ are noted as malicious nodes.

**Algorithm-2**

1. Let $Th_{rd}$ be the route discovery threshold value.
2. Consider $n_i$ be the mobile node, where $i=1, 2 \ldots n$ and $mv_i$ be the mean value of node $i$.
3. Each node stores time of first received RREQ and RREP packet in C-Table.
4. FA and BA collect and update $mv$ values of intermediate nodes in M-Table.
5. Source compares $mv_i$ with $Th_{rd}$
   5.1 If $(mv_i \leq Th_{rd})$ then
      a) Node is considered as valid node.
      b) For this valid node the node state2 field in MN-table is set to 1
      Else if $(mv_i > Th_{rd})$ then
      c) Node is considered as malicious node.
      d) For this malicious node the node state 2 is set to 0.
While constructing path from source to destination, the source considers the valid nodes rather than malicious nodes. The state of node is maintained by each node in MN-Table. The MN-Table has the following format.

<table>
<thead>
<tr>
<th>NODE ID</th>
<th>MEAN VALUE</th>
<th>NODE STATE1</th>
<th>NODE STATE2</th>
</tr>
</thead>
</table>

### 6.4 MODULAR ARCHITECTURE FOR THE TWO SWARM BASED INTRUSION DETECTION SYSTEMS IN MANET

A modular architecture for the intrusion detection in MANET for identifying the various routing attacks is shown in fig 6.1. It has nine modules namely

a) MANET test bed environment creation
b) Traffic data collection module for SDIDS1
c) Traffic data collection module for SDIDS2
d) Processing module for SDIDS1
e) Processing module for SDIDS2
f) Event handling module for SDIDS1
g) Event handling module for SDIDS2
h) Alert generation module for SDIDS1
i) Alert generation module for SDIDS2

**a) MANET Test Bed Environment Creation**

In this module, MANET environment is created by using various parameters like topography, number of nodes, routing protocol, mobility scenario, connection pattern scenario, number of sources, destination node, node speed, traffic source, simulation time, etc., for the two swarm based intrusion detection systems namely SDIDS1 and SDIDS2. Without creating the MANET environment, it is not possible to go to the other modules.
b) Traffic data collection module for SDIDS1

This module collects the traffic data for the swarm based intrusion detection system namely SDIDS1. SDIDS1 requires the traffic data such as initial energy of the node, energy of the node after time t, local bandwidth of the node, minimum bandwidth among the neighboring nodes, coordinates of the current node and the neighboring nodes from the network. This data collection is actually performed by the active nodes. This traffic data collection module then forwards the collected traffic data to the processing module corresponds to SDIDS1.

c) Traffic data collection module for SDIDS2

This module collects the traffic data for the swarm based intrusion detection system namely SDIDS2. SDIDS2 requires the traffic data such as initial energy of the node, energy of the node after time t, local bandwidth of the node, minimum bandwidth among the neighboring nodes, coordinates of the current node and the neighboring nodes from the network, Received Time of RREQ Packet, Sequence Number of RREQ Packet, Received Time of RREP Packet, and Sequence Number of RREP Packet. This data collection is actually performed by the active nodes. This traffic data collection module then forwards the collected traffic data to the processing module corresponding to SDIDS2.

d) Processing module for SDIDS1

This module calculates the residual energy, residual bandwidth, connectivity and the trust value for the nodes present in the selected route. Based on these parameters, it selects the active nodes. Active nodes are the nodes which are having the highest bandwidth, highest energy and highest trust value. These active nodes monitor their neighbor nodes and calculate the trust values of them. This processing module then forwards the trust values of the neighbor nodes monitored to the Event handling module for SDIDS1.

e) Processing module for SDIDS2

This module calculates the mean value of the nodes using the RREQ and RREP packets whenever the route discovery takes place. Then
This module forwards the calculated mean values to the event generation module for SDIDS2. This module also calculates the residual energy, residual bandwidth, connectivity and the trust value for the nodes present in the selected route during the data transmission. Based on these parameters, it selects the active nodes. Active nodes are the nodes which are having the highest bandwidth, highest energy and highest trust value. These active nodes monitor their neighbor nodes and calculate their trust values. This processing module then forwards the trust values of the neighbor nodes monitored to the Event handling module for SDIDS2.

**f) Event handling Module for SDIDS1:**

This module generates the event whenever the trust value of any node is below the minimum threshold trust value. The corresponding nodes are considered the malicious nodes. The generated events are sent to the alert generation module.

**g) Event handling module for SDIDS2**

This module generates the event whenever the mean value of any node is above the minimum route discovery threshold value or the trust value of any node is below the minimum threshold trust value. The corresponding nodes are considered the malicious nodes. The generated events are sent to the alert generation module for SDIDS2.

**h) Alert generation module for SDIDS1 and SDIDS2**

These modules generate the alert message to the source node so that that source node can employ some defense mechanism to remove the malicious nodes from the network. The alert generation module for SDIDS2 can generate more alert messages when compared to the alert generation module for SDIDS1.
6.5 PERFORMANCE EVALUATION AND ENHANCEMENT

Here the comparison of two Swarm Based Intrusion Detection systems (SDIDS1 and SDIDS2) was performed for the Routing Attacks and their performance is evaluated using various metrics namely throughput, Average Packet Delivery Ratio, Average Packet Drop and energy consumption.

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 6.4.

<table>
<thead>
<tr>
<th>Table 6.4 Simulation Settings in ns2 Used by SDIDS1 and SDIDS2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NO. OF NODES</strong></td>
</tr>
<tr>
<td><strong>AREA SIZE</strong></td>
</tr>
<tr>
<td><strong>MAC</strong></td>
</tr>
<tr>
<td><strong>RADIO RANGE</strong></td>
</tr>
<tr>
<td><strong>SIMULATION TIME</strong></td>
</tr>
<tr>
<td>TRAFFIC SOURCE</td>
</tr>
<tr>
<td>------------------</td>
</tr>
<tr>
<td>PACKET SIZE</td>
</tr>
<tr>
<td>SPEED</td>
</tr>
<tr>
<td>NO. OF ATTACKERS</td>
</tr>
</tbody>
</table>

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.

### 6.6 RESULTS AND DISCUSSION

SDIDS1 and SDIDS2 performances are evaluated using the following metrics. These metrics indicate how SDIDS1 and SDIDS2 function when increasing the nodes and the attackers.

#### 6.6.1 Performance Metrics

**Throughput**: It is the number of packets successfully received by the receiver.

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

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

**Energy Consumption**: It is the amount of energy consumed during the packet transmission.

#### 6.6.2 Results

Here two different experiments are conducted namely

A. Based On Nodes
In the first experiment, the number of nodes is varied as 20, 40, 60, 80 and 100.

Fig 6.2: Nodes Vs Throughput

In Fig 6.2, as the nodes are increasing, the throughput of both SDIDS1 and SDIDS2 is also increasing but the throughput of SDIDS2 is more than the corresponding values of SDIDS1.

Fig 6.3: Nodes Vs Packet Delivery Ratio

In Figure 6.3, as the nodes are increasing, the packet delivery ratio of SDIDS2 is slightly more than SDIDS1.

Fig 6.4: Nodes Vs Packets Drop

In Figure 6.4, even as the nodes are increasing, the packet drops of SDIDS2 are slightly less when compared to SDIDS1.
In Figure 6.5, even as the nodes are increasing, the energy consumption of SDIDS2 is less than SDIDS1.

**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.

In Figure 6.6, even as the attacker nodes are increasing, the throughput of both SDIDS1 and SDIDS2 is decreasing, but the throughput of SDIDS2 is more than SDIDS1.
Fig 6.7: Attackers Vs Delivery Ratio

In Figure 6.7, even as the attacker nodes are increasing, the PDR of SDIDS1 and SDIDS2 is almost same.

Fig 6.8: Attackers Vs Packets Drop

In Figure 6.8, even as the attacker nodes are increasing, the packet drop of SDIDS2 is increasing and the packet drop of SDIDS2 is less than the corresponding values of SDIDS1.

Fig 6.9: Attackers Vs Energy

In Figure 6.9, even as the attacker nodes are increasing, the energy consumption of SDIDS2 is slightly less than the corresponding values of SDIDS1.

6.7 CONCLUSION

This chapter compares two swarm based intrusion detection systems (SDIDS1 and SDIDS2) for the various routing layer attacks in MANET. SDIDS1 uses the forward and backward ants to select the active nodes (valid nodes) for data transmission. For these active nodes, SDIDS1
sets the nodestate1 field to 1. SDIDS2 executes algorithm2 which uses
the forward and backward ants, to obtain the mean value of nodes, which
is the difference between first received RREQ and RREP packets. While
receiving the mean value of nodes, the source compares mean value with
predefined threshold value and marks node as valid and malicious node.
SDIDS2 sets the nodestate2 field to 1 if the node is a valid node. SDIDS2
then executes algorithm1 to identify the valid nodes. Now SDIDS2 sets the
nodestate1 field in the MN table to 1 if the node examined is a valid node.
SDIDS2 selects the node for data transmission only when both nodestate1
and nodestate2 in the MN-table is 1(valid node). In both SDIDS1 and
SDIDS2, the source constructs path to the destination by omitting the
malicious nodes. The performances of both the techniques are proved
through simulation results. SDIDS2 is able to identify more malicious
nodes when compared to SDIDS1. The performance of SDIDS2 is found to
be better than SDIDS1 and improves network performance.

In future, performance of SDIDS2 can also be evaluated using
some more metrics.