Chapter IV

SWARM BASED INTRUSION DETECTION AND DEFENSE TECHNIQUE FOR MALICIOUS ATTACKS

4.0 INTRODUCTION

During route discovery process in AODV protocol, the malicious flooding attacker floods the route request packets through the victim node symbolizing as setting up a path. Following the path establishment, the attacker floods data packets through the victim node for paralyzing the node. As the packet size of these data packets is much larger than the route request packet, the victim nodes get congested easily. The attackers consume the battery power of the victim node, thus separating them from the network. Hence, the malicious flooding attack leads to denial of service (DoS) attack on the victim node. Thus, there is worsening in the act of processing the valid packets at the victim node. As the malicious flooding attack congests the victim node as well as the entire network, it is very harmful to the mobile ad hoc network. Also it is very difficult to avoid this attack when it is caused by the multiple attackers. The flooding and packet dropping attacks preventing the network service availability result in ineffective secure routing.

A malicious node can manipulate routing messages and also cause packet drops selectively which may result in network dysfunctioning. The general form of security violation is the DDoS attack where the attackers floods huge incoming packets over the victim nodes. Generally in wireless networks, attackers introduce the false packets effortlessly imitating another sender which is termed as spoofing attack. Whatever is the type of attack that has happened in MANET, the data communication among the nodes may not be valid. The action taken by the malicious nodes depends on the type of attack. In order to overcome all these issues, it is
necessary to develop a defense mechanism against malicious flooding attacks.

4.1 DEFENSE MECHANISM IN MANET

The passive attack on routing information can be countered with the same methods that protect data traffic. Some active attacks, such as illegal modification of routing messages, can be prevented by mechanisms source authentication and message integrity. DoS attacks on a routing protocol could take many forms. DoS attacks can be limited by preventing the attacker from inserting routing loops, enforcing the maximum route length that a packet should travel, or using some other active approaches. The wormhole attack can be detected by an unalterable and independent physical metric, such as time delay or geographical location. For example, packet leashes are used to combat wormhole attacks [98].

In general, some kind of authentication and integrity mechanism, either the hop-by-hop or the end-to-end approach, is used to ensure the correctness of routing information. For instance, digital signature, one-way hash function, hash chain, message authentication code (MAC), and hashed message authentication code (HMAC) are widely used for this purpose. IPsec and ESP are standards of security protocols on the network layer used in the Internet that could also be used in MANET, in certain circumstances, to provide network layer data packet authentication, and a certain level of confidentiality; in addition, some protocols are designed to defend against selfish nodes, which intend to save resources and avoid network.

The DoS attacks, impersonation attacks, man-in-the-middle attacks, and many other attacks can target multiple layers. The countermeasures for these attacks need to be implemented at different layers. For example, directional antennas [31] are used at the media access layer to defend against wormhole attacks, and packet leashes [98] are used as a network layer defense against wormhole attacks. The countermeasures for multi-layer attacks can also be implemented in an integrated scheme. For example, if a node detects a local intrusion at a higher layer, lower layers are notified to do further investigation.
Defense against DoS attacks

In MANET, two types of DoS attacks [56] are quite common. One is at the routing layer, and the other is at the MAC layer. Attacks at the routing layer could consist of but is not limited to the following misbehaviors:

1. THE MALICIOUS NODE PARTICIPATES IN A ROUTE BUT SIMPLY DROPS SOME OF THE DATA PACKETS.
2. THE MALICIOUS NODE TRANSMITS FALSIFIED ROUTE UPDATES.
3. THE MALICIOUS NODE COULD POTENTIALLY REPLAY STALE UPDATES.
4. THE MALICIOUS NODE REDUCES THE TTL (TIME-TO-LIVE) FIELD IN THE IP HEADER SO THAT THE PACKET NEVER REACHES THE DESTINATION.

If end-to-end authentication is enforced, attacks by independent malicious node of types (2) and (3) may be thwarted. An attack of type (1) may be handled by assigning confidence levels to nodes and using routes that provide the highest level of confidence. An attack of type (4) may be countered by making it mandatory that a relay node ensures that the TTL field is set to a value greater than the hop count to the intended destinations. If nodes collude, the authentication mechanisms fail, and it is an open problem to provide protection against such routing attacks.

At the MAC layer DoS attacks could include, among others, the following misbehaviors:

1. KEEPING THE CHANNEL BUSY IN THE VICINITY OF A NODE LEADS TO A DENIAL OF SERVICE ATTACK AT THAT NODE.
2. BY USING A PARTICULAR NODE TO CONTINUALLY RELAY SPURIOUS DATA, THE BATTERY LIFE OF THAT NODE MAY BE DRAINED.

End-to-end authentication may prevent the above two cases from succeeding.

If the node does not have a certificate of authentication, it may be prevented from accessing the channel. Usually the nodes are outsiders. However, if nodes collude, and the colluding nodes include the sending node and the destination, MAC layer attacks are very feasible.
The defense mechanism [61] for distributed denial of service (DDoS) involves the following three actions:

I) ATTACK DETECTION
II) ATTACKING SOURCE DETECTION
III) FILTERING THE DISTRUSTFUL PACKETS BY CONTROLLING THE ATTACKING TRAFFIC.

When the source node wants to forward the data packet to D, it discards the malicious nodes in the path and bypasses the data through other nodes in alternate selected path towards D (shown in figure 4.2) and source performs the key revocation process for defending against the malicious nodes (explained in 4.3). An example of intrusion detection is illustrated in Figure 4.1.

Fig 4.1 Intrusion Detection
In path 1, active node NA4 monitors N3, N8, and N5. It collects the trust information from all these nodes and exchanges the gathered information with NA9. From the exchanged information, it is found that trust value of N8 is below a minimum threshold. This reveals that N8 is a malicious node. Then NA4 sends an alert message (MA) to source node S about the malicious node. S stores path number (path 2) and node ID of N8 in its routing table. When S forwards the data through path 2, it
discards N8 and uses N3 in path 1 as alternate node to proceed with DP forwarding towards D using bypass routing technique.

Similarly in path 3, NA13 monitors the N12, N14, N17, and N18. It collects the trust information from all these nodes and exchanges the gathered information with NA19. It is found that trust value of N18 is below a minimum threshold. This means that N18 is a malicious node. Then NA13 sends an alert message (MA) to S regarding malicious node. S stores path number (path 2) and node ID of N8 in its routing table. When S forwards the data through path 4, it discards N18 and uses N12 in path 3 as alternate node to proceed with DP forwarding towards D using bypass routing technique.

![Figure 4.2: Bypass Routing](image)

The active node keeps changing adaptively as per the threshold levels of trust value.

### 4.2 NECESSITY OF DEFENSE MECHANISM IN MANET

- During route discovery process in AODV protocol, the malicious flooding attacker floods the route request packets through the victim node symbolizing as setting up a path.
• Following the path establishment, the attacker floods data packets through the victim node for paralyzing the node. As the packet size of these data packets is much larger than the route request packet, the victim nodes get congested easily.

• The attackers consume the battery power of the victim node thus separating them from the network. Hence, the malicious flooding attack leads to denial of service (DoS) attack on the victim node. Thus, there is worsening in the act of processing the valid packets at the victim node.

• As the malicious flooding attack congests the victim node as well as the entire network, it is very harmful to the mobile ad hoc network. Also it is very difficult to avoid this attack when it is caused by the multiple attackers [33].

• The flooding and packet dropping attacks preventing the network service availability result in ineffective secure routing [87].

• A malicious node can manipulate routing messages and also cause packet drops selectively which may result in network dysfunctioning [92].

• The general form of security violation is the DDoS attack where the attackers flood huge incoming packets over the victim nodes [34].

• Generally in wireless networks, attackers introduce the false packets effortlessly imitating another sender which is termed as spoofing attack [98].

In order to overcome all these issues, it is necessary to develop a defense mechanism against malicious flooding attacks.

4.3 PROACTIVE SECRET SHARING TECHNIQUE

The threshold cryptography helps in sharing the secret [94] among the nodes. A proactive secret sharing technique (PSS) can be employed
along with the threshold cryptographic technique in order to make the sharing scheme more secured. This scheme permits refreshment of all shares by generating a new set of shares for a similar secret key from the old shares exclusive of renovating the secret key.

Let K represent the secret key and $k_{i1}, k_{i2}, \ldots, k_{in}$ represent the sub-key. Let the node $N_i$ hold the key.

The Proactive secret sharing technique can be described using the following steps.

a) $N_i$ randomly generates its sub-keys $k_{i1}, k_{i2}, \ldots, k_{in}$

b) Every sub-key $k_{ij} (i=1, 2, \ldots, n)$ is distributed to node $N_j$ through secure link.

c) When $N_j$ receives the sub-keys $k_{1j}, k_{2j}, \ldots, k_{nj}$, it calculates a new key from the received sub-keys and old keys using the following equation.

$$k'_j = k_j + \sum_{i=1}^{n} k_{ij}$$

(4.1)

d) Each new key ($k'_1, k'_2, \ldots, k'_n$) is sharing the secret key $K$, since

$$\sum_{i=1}^{n} k_{ij} = 0, i \in \{1, \ldots, n\}$$

4.4 CERTIFICATE RENEWAL PROCESS

Each node deployed in the network holds a certificate signed by the secret key $K$ that contains the fields such as Node ID, signature period, and expiration period (using equation 4.1). Also each node holds a certificate revocation list (CRL) based on certificate revocation mechanism and each CRL is associated with the soft-state timer. As nodes are certified, a malicious node has no possibility to reveal the certificate of any other nodes.
Node $n \leftarrow K [ ID, t_s, t_e ]$

Prior to the expiry of the current certificate, each node looks for its neighbours within two-hop distance for certificate renewal (CR). The steps involved in the CR are as follows:

- The node that needs CR broadcasts a certificate renewal request ($CR_{req}$) packet to its neighbors that include current certificate and time stamp (TS).
- A node upon receiving $CR_{req}$ packet from its neighbors extracts the certificate from the packet and compares it with the CRL. i.e. verifying whether the certificate has previously been revoked.
- On comparison, if the certificate is valid, then a new certificate is constructed similar to the older one that holds the equivalent time stamp as that in $CR_{req}$ packet. On the other hand, if $CR_{req}$ has revoked certificates, then it is dropped.
- Then the new certificate is signed with its own private key ($k_{pr}$) and the certificate reply packet $CR_{rep}$ encapsulated by this partially signed certificate is unicast back to the node from which it received $CR_{req}$.
- When the requested node receives $CR_{rep}$ packets from its different neighbours, it gathers all the partially signed certificates into a single certificate signed with $k_{pr}$.

4.5 CERTIFICATE REVOCATION PROCESS

When a malicious node is detected, MA is sent to S by the active nodes (explained in section 3.4). When S receives a multiple MA for the same node, it performs the following actions:

- Generates the certificate revocation ($C_{rev}$) notification.
- Signs the $C_{rev}$ using its own share of $k_{pr}$.
- Broadcasts $C_{rev}$ to other nodes.
• The certificate revocation process is initiated.

When a node receives a $C_{rev}$ packet, it verifies whether the packet is signed and also whether the revoked certificate is already in the CRL. If $C_{rev}$ packets are not signed by the $k_{pr}$ or contain certificates on CRL, then it is dropped. Otherwise node adds the revoked certificate to its own CRL and re-broadcasts the $C_{rev}$ packet. This process allows every node to add the revoked certificate into its CRL. As only nodes with valid certificates can take part in the network operations, this certificate revocation mechanism guarantees that a malicious node is isolated following its detection. Also to make sure that a malicious node should not renew its certificate, a revoked certificate has to be kept in CRL until it expires, after which it can be deleted.

4.6 PERFORMANCE EVALUATION AND ENHANCEMENT

Here the SBDT architecture is examined and its performance is evaluated using various metrics namely Average Packet Delivery Ratio, Average Packet Drop and delay. SBDT performance is also compared and evaluated with the performance of CAPMAN [68].

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.

In our simulation, mobile nodes move in a 1000 meter x 1000 meter region for 50 seconds simulation time. The nodes are varied from 20 to 100 in steps of 20. Moreover, assume that each node moves independently with the same average speed. All nodes have the same transmission range of 250 meters. In our simulation, the node speed is 10 m/s. The simulated traffic is Constant Bit Rate (CBR). Our simulation settings and parameters are summarized in table 4.1.
Table 4.1. Simulation Settings in ns2 used by SBDT

<table>
<thead>
<tr>
<th>NO. OF NODES</th>
<th>20, 40, 60, 80 AND 100.</th>
</tr>
</thead>
<tbody>
<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>1, 2, 3, 4 AND 5.</td>
</tr>
<tr>
<td>INITIAL ENERGY</td>
<td>10.5 J</td>
</tr>
<tr>
<td>TRANSMISSION POWER</td>
<td>0.660</td>
</tr>
<tr>
<td>RECEIVING POWER</td>
<td>0.395</td>
</tr>
<tr>
<td>IDLE POWER</td>
<td>0.035</td>
</tr>
</tbody>
</table>

4.7 RESULTS AND DISCUSSION

SBDT performance is evaluated using the following metrics. These metrics indicate how SBDT functions when increasing the nodes and the attackers.

4.7.1 Performance Metrics

The performance of SBDT is compared with CAPMAN according to the following 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.
**False Detection Percentage:** It is obtained from dividing false alarms by all normal activities.

**Detection Accuracy:** It is calculated as the percentage of detected attacks among all the attacks mounted.

The false detection ratio and detection accuracy are measured in terms of percentage.

Here two different experiments are conducted namely

### 4.7.2 Results

a) Based On Attackers

In the first experiment, the number of attackers varies from 1 to 5 in a 100 nodes network.

![Figure 4.3: Attackers Vs. Packet Delivery Ratio](image)

In Figure 4.3, even as the attacker nodes are increasing SBDT is producing higher packet delivery ratio (PDR) when compared to CAPMAN. In both SBDT and CAPMAN, as the attacker nodes are increasing, the PDR is decreasing.
In Figure 4.4, as the attacker nodes are increasing, the delay is increasing but it is well below the corresponding delay of CAPMAN. So the delay is very much reduced in the proposed SBDT.

In Figure 4.5, the packet drop of SBDT is very smaller than the corresponding values of CAPMAN. In SBDT, the packet drops are almost constant whereas in CAPMAN the packet drops are increasing as the attacker nodes are increasing.

Figure 4.4: Attackers Vs Delay

Figure 4.5: Attackers Vs Packets Drop

Figure 4.6: Attackers Vs False Detection Percentage
In Figure 4.6, as the attacker nodes are increasing, the false detection percentage is also increasing, but the false detection percentage of SBDT is considerably less than CAPMAN.

![Attackers Vs Detection Accuracy](image)

**Figure 4.7: Attackers Vs Percentage of Detection Accuracy**

In Figure 4.7, as the attacker nodes are increasing, the detection accuracy is decreasing but the detection accuracy of SBDT is slightly more than CAPMAN.

**b) Based on Nodes**

In the second experiment the number of nodes varies from 20 to 100 in steps of 20 and keeping the number of attackers as 4.

![Nodes Vs Packet Delivery Ratio](image)

**Figure 4.8: Nodes Vs Packet Delivery Ratio**

In Figure 4.8, as the nodes are increasing, the SBDT is producing higher PDR when compared to CAPMAN.
In Figure 4.9, as the nodes are increasing the delay is increasing for CAPMAN, but it is not so for SBDT. The delay of SBDT is also less than the corresponding delay of CAPMAN.

In Figure 4.10, as the nodes are increasing, the packets drop of CAPMAN is more but SBDT is producing very less packets drops.

4.8 CONCLUSION

This chapter discusses a swarm based intrusion detection and defense technique for malicious attacks in mobile ad hoc networks (MANET). In this technique, multiple paths are established between source and destination for data transmission. In the selected routes, the nodes with highest trust value, residual bandwidth and residual energy are selected as active nodes using swarm intelligence based ant colony optimization. Each active node monitors its neighbor nodes within its transmission range and collects the trust value from all monitored nodes. The active nodes adaptively change 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. Upon detecting malicious node, the active node sends an alert message to the source node. When the source node wants to forward the data packet to D, it discards the malicious nodes in that path and bypasses the data through other nodes in alternate selected path towards D and performs the certificate revocation process for defending against the malicious nodes. By simulation results, it is shown that the proposed approach accurately detects the attacks and minimizes the packet drops due to attacks. So this form of defense mechanism is better in filtering the malicious nodes from the path selection and can also be used for removing the malicious nodes irrespective of the type of attack that happened in MANET.