CHAPTER 3

ANALYSIS OF SELFISH NODE BEHAVIOR ATTACKS IN MANET USING AODV ROUTING PROTOCOL

3.1 OVERVIEW

In this chapter, the analysis of different selfish behavior attacks and the simulation results under various performance metrics is made.

3.2 MODELING OF SELFISH BEHAVIOR ATTACKS IN AODV

The following pseudocode segments explain the implementation of two types of selfish behavior attacks in AODV routing agent as depicted in Figure 3.1. The receive function of AODV is the main entry point from where the behavior of the routing agent can be manipulated and it makes it behave maliciously. The node, after receiving the AODV packet, checks for various cases. If the packet is an RREQ packet, it will receive the request. If the packet is an RREP packet, then it will check for two conditions, the first condition is that if it checks that it belongs to malicious behavior type=0 or 1, then it is normal AODV or selfish behavior type I. The second condition is that it checks for malicious behavior type =2, and it checks if source and destination belong to the same node and then receives the packet. The same criteria would be considered for RERR packet. In HELLO case, if it is a malicious behavior type 2, then it will drop the packet maliciously.
Figure 3.1 Pseudocode for Modifications in AODV::recv

The drop malicious function is invoked when there is a malicious behavior among the nodes. If a packet comes from a malicious node, it will drop the packet and record the reason for it. This function will be implemented under ns2 trace event generation mechanism which is shown in Figure 3.2.

```
    RecvAODVPkt (Pkt, AODVPktType) {
        switch(AODVPktType) {
            case TYPE_RREQ:
               RecvRequest(Pkt)
                break
            case RREP:
                if (MaliciousBehaviorType=0 or 1) then {
                    // Normal AODV or Selfish Behavior Type I
                    RecvReply(Pkt);
                } elseif (MaliciousBehaviorType= 2) then {
                    // Selfish Behavior Type II
                    if (src= self) or (dst= self) then {
                        RecvReply(Pkt);
                    } else {
                        DropMaliciously(pkt, MALICIOUS)
                    }
                } break
            case RERR:
                if (MaliciousBehaviorType=0 or 1) then {
                    // Normal AODV or Selfish Behavior Type I
                    RecvError (Pkt);
                } elseif (MaliciousBehaviorType= 2) then {
                    // Selfish Behavior Type II
                    DropMaliciously(pkt, MALICIOUS)
                }
        }
    }
```

```// Selfish Behavior Type II
    if (src= self) or (dst= self) then {
        RecvError (Pkt);
    } else {
        DropMaliciously(pkt, MALICIOUS)
    }
```

Figure 3.2 Pseudocode for Modifications in trace event generation

```
    DropMaliciously (pkt, reason)
    {
        Drop the Pkt
        Record the reason of dropping for trace analysis
    }
```
OnReceivingAPacket(Pkt) {
    if (PT_AODV) {
        RecvAODVPkt(Pkt, AODVPktType)
    } elseif (MaliciousBehaviorType=0) then {
        // Normal AODV
        Process the Pkt Normally.
    } elseif (MaliciousBehaviorType=1 or 2) then {
        // AODV Selfish Behavior Type I or II
        if (src=self) or (dst=self) then {
            Process the Pkt Normally.
        } else {
            DropMaliciously(pkt, MALICIOUS)
        }
    }
}

Figure 3.3 Modifications in AODV:: recvAODV

Figure 3.3 depicts the process of receiving a packet during routing. If the received packet is an AODV packet, then it will process normally. If the packet belongs to malicious behavior type=0, then it will process like a normal AODV packet. Else, it will check for malicious behavior type=1 or 2, then it will be categorized as selfish behavior type I or type II. At last, if the packet does not satisfy any of the conditions, then the node drops the packet maliciously.

RecvRequest (pkt) {
    if (src=self) then {
        Free(pkt)
        return
    }
    if (MaliciousBehaviorType=0 or 1) then {
        // Normal AODV or Selfish Behavior Type I
        Process the Request Normally
        SendGenuineRouteReply()
    } elseif (MaliciousBehaviorType= 2) then {
        // Selfish Behavior Type II
        DropMaliciously(pkt, MALICIOUS)
    }
}

Figure 3.4 Pseudocode for Modifications in AODV:: recvRequest
The receive request function is another location from which the behavior of the routing agent can be manipulated and it makes it behave maliciously with respect to the type of an AODV packet as represented in Figure 3.4.

3.3 SIMULATION ENVIRONMENT AND PARAMETERS

NS 2.35 is used as a simulation tool in the present research. The following Table 3.1 and Table 3.2 represent the common node parameters and simulation setup parameters are used in the analysis part in the present study. The number of background traffic flow is 10 and the traffic type is CBR. User Datagram Protocol (UDP) is used as a transport agent. The packet size is 512 bytes forwarded at an interval of 1s and CBR rate is 10 kb. Traffic starts at 30th sec and stops at 100th sec. The system environment and parameters which are represented in this section are used in all the simulations but the simulated attacks and AODV states vary from part of study.

Table 3.1 Common Node Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channel</td>
<td>WirelessChannel</td>
</tr>
<tr>
<td>Propagation</td>
<td>TwoRayGround</td>
</tr>
<tr>
<td>Phy</td>
<td>WirelessPhy</td>
</tr>
<tr>
<td>Mac</td>
<td>802_11</td>
</tr>
<tr>
<td>Antenna</td>
<td>OmniAntenna</td>
</tr>
<tr>
<td>Link layer</td>
<td>LL</td>
</tr>
<tr>
<td>Queue</td>
<td>DropTail-PriQueue</td>
</tr>
<tr>
<td>Queue Length</td>
<td>50</td>
</tr>
<tr>
<td>Routing Protocol</td>
<td>AODV</td>
</tr>
<tr>
<td>Node-txPower</td>
<td>0.28183815</td>
</tr>
<tr>
<td>Node-rxPower</td>
<td>0.2819</td>
</tr>
<tr>
<td>Node-idlePower</td>
<td>0.14</td>
</tr>
<tr>
<td>Node Initial Energy</td>
<td>1000.0 Joules</td>
</tr>
</tbody>
</table>

(Note: rxPower and idlePower are intentionally set high to simulate quick energy consumption)
Table 3.2 Parameters for Simulation Setup

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>X dimension of Topography</td>
<td>800m</td>
</tr>
<tr>
<td>Y dimension of Topography</td>
<td>800m</td>
</tr>
<tr>
<td>Total Number of Nodes</td>
<td>30, 40, 50</td>
</tr>
<tr>
<td>Mobility</td>
<td>10m/s</td>
</tr>
<tr>
<td>Pause Time</td>
<td>20s</td>
</tr>
<tr>
<td>Total Simulation Time</td>
<td>100s</td>
</tr>
<tr>
<td>Mobility Model</td>
<td>Random WayPoint (RWP)</td>
</tr>
<tr>
<td>No.of Malicious Nodes</td>
<td>0, 1, 5 &amp; 10</td>
</tr>
</tbody>
</table>

3.4 RESULTS AND DISCUSSION FOR SELFISH BEHAVIOR ATTACKS & NORMAL AODV

The simulation results represent the performance of normal AODV, Selfish Behavior Type I and Selfish Behavior Type II by changing the number of the nodes in the network. Except normal AODV, the malicious node count is retained as 5. The performance metrics considered are maliciously dropped packets at Routing Layer, dropped packets at Application Layer, Throughput, PDF, Routing Load and MAC Load.

3.4.1 Throughput

As far as throughput is concerned, Selfish Behavior Type I affects the throughput considerably. Selfish Behavior Type I attack shows an improvement in throughput with 40 nodes due to random placement of malicious nodes and low congestion in network. It is a randomly selected topology and so there occurs a sudden change. Even though, Selfish Behavior Type I attack shows a rise in throughput with 40 nodes, it is less when compared to Selfish Behavior Type II attack. The performance of normal
AODV and Selfish Behavior Type II is equal and it produces a good throughput as shown in Figure 3.5.

![Average Throughput](image)

**Figure 3.5 Average Throughput**

### 3.4.2 Packet Delivery Fraction (PDF)

The Selfish Behavior Type I attack produces a low PDF of about 49.26% which is less than normal AODV and Selfish Behavior Type II which generates the PDF of 80.62% and 80.65% respectively. The reason is that Selfish Behavior Type I attack drops more packets and shows a low PDF. The PDF of Selfish Behavior Type II attack and Normal AODV is similar and it exhibits good performance which is represented in Figure 3.6.

![Average PDF](image)

**Figure 3.6 Average PDF**
3.4.3 Packets Dropped at Application Layer

The performance of selfish behavior attacks for the metric packets dropped at application layer is depicted in Figure 3.7. As a result of malicious activity and high network collision, there is a sudden change after 40 nodes in Selfish Behavior Type I attack. The topology selected is random and so there is more packets dropped at application layer when compared to Selfish Behavior Type II attack and Normal AODV.

![Figure 3.7 Packets Dropped at Application Layer](image)

3.4.4 Packets Maliciously Dropped at Routing Layer

The performance in terms of dropped packets at routing layer is depicted in Figure 3.8. It is inferred from the figure that more packets are dropped maliciously at routing layer by Selfish Behavior Type I attack as a result of selfish behavior. As Selfish Behavior Type II attack absorbs more network congestion, it affects the routing layer by dropping more packets. Routing process functions well in normal AODV and so no packet is dropped maliciously at routing layer.
3.4.5 Average Routing Load

The routing load in the Selfish Behavior Type I attack is higher than the Selfish Behavior Type II attack. Because Selfish Behavior Type II attack does not exchange the data between the nodes. Hence the routing load is low and it shows a good performance as shown in Figure 3.9.

Figure 3.9 Average Routing Load
3.4.6  **Average MAC Load**

The Selfish Behavior Type I attack causes high MAC load because the frames are corrupted by introducing extra bits in this MAC layer, but in the case of normal AODV and Selfish Behavior Type II attack, MAC load is low as there is no opportunity for the corruption of frames in MAC layer which is shown in Figure 3.10.

![Figure 3.10 Average MAC Load](image)

3.5  **COMPARISON OF THE PERFORMANCE METRICS WITH DIFFERENT MALICIOUS NODES UNDER SELFISH BEHAVIOR ATTACKS**

The simulation results represent the performance of normal AODV, Selfish Behavior Type I attack and Selfish Behavior Type II attack in the presence of malicious nodes as 1, 5 and 10 respectively. The total numbers of nodes retained are 50.
3.5.1 Throughput of Selfish Behavior Attacks

It is observed from Figure 3.11 that the Selfish Behavior Type I attack affects the throughput because it takes control of the network and drops more packets in the presence of malicious environment. The Selfish Behavior Type II attack does not involve in route discovery and forwarding packets, and hence the throughput is good.

![Average Throughput](image)

Figure 3.11. Average Thoughput of Selfish Behavior Attacks

3.5.2 PDF of Selfish Behavior Attacks

Selfish Behavior Type I attack is compared with Selfish Behavior Type II attack in terms of PDF which is shown in Figure 3.12. As inferred from the figure, Selfish Behavior Type I attack shows a gradual decrease in PDF when increasing the number of malicious nodes and affects the PDF to a great extent. In contrast, Selfish Behavior Type II attack forwards only its own packet to save its energy, and hence produces high PDF.
In Selfish Behavior Type I attack, more packets are dropped at application layer and when increasing the number of malicious node from 5 the packet dropping is constant. This is due to node mobility, there is a chance for the new malicious node to place near to another malicious node and the area is already affected with the previous malicious node. So, the new malicious node does not have much impact on packet dropping is shown in Figure 3.13.
3.5.4 Packets Maliciously Dropped at Routing Layer under Selfish Behavior Attacks

The performance of selfish behavior attacks for packets maliciously dropped at routing layer is shown in Figure 3.14. After 5 malicious nodes, Selfish Behavior Type I produces a steady decrease in the dropping of packets, whereas Selfish Behavior Type II shows a steady increase in the dropping of packets at routing layer.

![Figure 3.14 Packets maliciously Dropped at Routing Layer under Selfish Behavior Attacks](image)

3.5.5 Average Routing Load of Selfish Behavior Attacks

Figure 3.15 depicts the performance of the metric routing load. The Selfish Behavior Type I attack propagates more RREQ packets, which results in large routing load. RREQ packet sent by the Selfish Behavior Type II attack is less and so routing load was not affected by it.
Figure 3.15 Average Routing Load of Selfish Behavior Attacks

3.5.6 Average MAC Load of Selfish Behavior Attacks

The comparison of Selfish Behavior Type I attack and Selfish Behavior Type II attack in terms of MAC load is represented in Figure 3.16. It is observed from the figure that the Selfish Behavior Type I attack causes high MAC load as frames got corrupt in MAC layer while Selfish Behavior Type II attack performance was good at MAC load.

Figure 3.16 Average MAC Load of Selfish Behavior Attacks
3.6 SUMMARY

This chapter concludes that when increasing the nodes and malicious nodes, the Selfish Behavior Type I attack shows a poor performance than Selfish Behavior Type II attack. Selfish Behavior Type I attack performs route discovery and route maintenance, but do not involve in data forwarding. So, from the simulation it have been understood that Selfish Behavior Type I attack affects throughput, PDF, packets dropped at application layer, packets maliciously dropped at routing layer, routing load and MAC load, as a result of not forwarding the data. Selfish Behavior Type II attack does not perform route discovery phase and forwarding data packets, but they spend energy for forwarding their own packets. Hence, Selfish Behavior Type II attack shows good throughput and PDF. It drops less number of packets at application layer, routing layer, less routing load and MAC load. The performance of the MANET is affected with the Selfish Behavior Type I attack to a great extent, whereas Selfish Behavior Type II does not affect the performance of the network. In a 50 node environment, in the presence of 10 malicious nodes and Selfish Behavior Type I attack, the network cannot be used for an effective communication. So Selfish Behavior Type I attack is considered in the present study.