CHAPTER 7

RESULTS AND DISCUSSION

In this chapter we present the results and discussions of all our proposed schemes described in chapter 2 to chapter 6. NS2 is used as a tool for evaluating our proposed schemes. Finally, we present the conclusion and scope of future work in section 7.6 of this chapter.

7.1 RESULTS FOR FMON SCHEME

FMON scheme against data flooding attack has been discussed in Chapter 2. The performance of FMON is compared with that of the SWAN protocol and SPA-ARA protocol. The FMON protocol was implemented and evaluated in NS2 network simulation environment. The simulation parameters are listed in Table 2.1.

7.1.1 Results for Data Flooding Attack

In this section, we present 2 simulation scenarios.

In the first scenario, three traffic flows are established in the network as follows:

1) Flow f1 along a path from source node S0 to destination node D

2) Flow f2 along a path from source node S1 to destination node D
3) Flow f3 along a path from source node S2 to destination node D

Figure 7.1 describes the above scenario. In Figure 7.1, there are many intermediate nodes between source nodes and destination node.

![Diagram of network with 3 different flows](image)

**Figure 7.1 Network with 3 different flows**

All the source nodes negotiate a rate of 100 kbps for traffic flow and begin sending traffic on flow at a rate of 100 kbps at time t = 1 sec. The attacking flow is set at a rate of 400 kbps. The capacity of the link is set to 1 Mbps. We vary the number of attackers as 2, 4, 6 and 8.

Throughput:

Figure 7.2 shows the throughput obtained at the destination node with respect to the number of attackers. From the results, it is observed that our FMON protocol achieves 15% improvement in throughput over SWAN and 46.6% improvement over SPA-ARA when the no. of attackers is 2. If the no. of attackers is increased to 8, FMON protocol achieves 21% improvement over SWAN and 76.5% improvement over SPA-ARA. In our proposed FMON scheme, each intermediate node maintains FMT and identifies the attackers based on the detection scheme and effectively rejects the attacker.
based on the response scheme. This increases the bandwidth available for the legitimate user. Hence we are able to obtain greater throughput for FMON scheme than the SWAN and SPA-ARA scheme under the same networking conditions.

![Graph showing impact on throughput based on number of attackers]

**Figure 7.2 Impact on throughput based on no. of attackers**

Dropped Packets:

Figure 7.3 shows the impact on dropped packet, based on number of attackers. Since the attacking flows are rejected as soon as the attackers are identified, in our proposed scheme, the network resources are made available to the legitimate users, without much delay. This makes the dropping rate of legitimate packets lower compared to the other two schemes. However as the number of attackers increase the dropping rates increase.
Figure 7.3 Impact on Dropped Packets based on No. of attackers

Packet Delivery Ratio:

Figure 7.4 shows the impact on packet delivery ratio, based on number of attackers. It is observed that when the no. of attackers is 2, packet delivery ratio of FMON scheme is 31.4% more than SWAN scheme and 45.1% more than SPA-ARA. When the no. of attackers is increased to 8, FMON scheme achieves 48.8% improvement over SWAN and 51.1% improvement over SPA-ARA. The result shows that the number of legitimate packets received is higher in FMON scheme compared with SWAN and SPA-ARA schemes. However, the packet delivery ratio decreases as the number of attackers increases.
Figure 7.4 Impact on Packet Delivery Ratio based on No. of attackers

End to End Delay:

Figure 7.5 shows the impact on End to End Delay based on the number of attackers. The average end to end delay calculates the delay of all the packets which have been successfully transmitted from the source to the destination. It includes all possible delays caused by buffering during route discovery latency, queuing in the interface queue, retransmission delays at the MAC, propagation and transfer times. Since the attacking flows are detected by intermediate nodes and the attackers are effectively blocked in FMON scheme, the average end to end delay is less compared to other schemes. However, the delay increases as the number of attackers increases.
CPU usage and Memory usage:

We perform the computation of CPU usage and memory usage on Intel\textsuperscript{[R]} core \textsuperscript{TM} 2 Duo CPU, 789 MHz, 1.99GB of RAM. The methodology used is to measure the impact of the simulation on the processor by using the ‘Top’ program. Top program is used to find how much processing power and memory are being used. This program measures the load by applications on the processor in the UNIX/Linux operating system. From Figure 7.6 and Figure 7.7, we find that CPU usage for our scheme is slightly more than the other two schemes and the memory usage is slightly less than other two schemes. This is because, FMT size grows as a function of the number of neighbor nodes rather than the number of traffic flows traversing the node.
From Figure 7.8, it is seen that as the number of attackers increase the number of transmitted packets also increases. But the number of received
packets is proportionately reduced due to the attacking flow. It is observed from the simulation that when the attackers are 2, nearly 51% of transmitted packets are received by the destination node. As the number of attacker increases, number of correctly received packets is reduced. From Figure 7.8, it is clear that if the no. of attackers is 8, only 47% of transmitted packets are received.

![Image](image.png)

**Figure 7.8 Impact on Transmitted Vs Received packets**

Effect of Mobility:

To determine the impact on mobility, we consider our FMON scheme with 4 attacker’s case with the speed of the mobile nodes being 5m/s. The effect of mobility of a node with FMON is analyzed by varying the pause time. Pause time refers to the time that a mobile node can remain in one place and then continue moving. Pause time is varied as 5 sec, 10sec, 20 sec and 30 sec. In Figure 7.9 and Figure 7.10, these times are specified as P5, P10, P20 and P30 respectively. The simulation results in Figure 7.9 and Figure 7.10 show that the number of dropped packets decreases and packet delivery ratio increases as pause time increases. This is because low mobility allows more
stable routing paths. However, it is not possible to achieve 100% packet delivery due to the unreliable links in wireless networks.

Figure 7.9 Dropped Packet Vs Simulation Time

Figure 7.10 Packet Delivery Ratio Vs Pause Time
In the second simulation scenario, we take the simulation time of 180 sec.

- Legitimate flows started at a rate of 50kbps at 1 sec
- Attacker1 sends the attacking flow at a rate of 400kbps at 20 sec
- Attacker2 starts sending the same traffic at 40 sec
- Other attackers (from 3 to 8) are getting into the network after every 20 sec time interval

The network performance is analyzed with this scenario. All the performance metrics are evaluated as in the first scenario. We have performed the analysis with different sending rates viz., 50kbps, 100kbps, 150kbps and 200kbps. The results are shown from Figure 7.11 to Figure 7.16.

![Figure 7.11 Throughput Vs Sending Rate](image-url)
Figure 7.11 shows the throughput obtained at the destination node with respect to sending rate of traffic. From the results, it is observed that our FMON protocol achieves 21.5% improvement in throughput over SWAN and 75.5% improvement over SPA-ARA when the sending rate is 50 kbps. If the sending rate is increased to 200 kbps, FMON protocol achieves 22.6% improvement over SWAN and 60.5% improvement over SPA-ARA. We obtain greater throughput for FMON scheme than the SWAN and SPA-ARA scheme under the same networking conditions.

![Dropped Packet Vs Sending Rate](image)

**Figure 7.12 Dropped Packet Vs Sending Rate**

Figure 7.12 shows the impact on dropped packet, based on sending rate. Since the attacking flows are identified effectively, in our proposed scheme, the legitimate users will get the network resources. This makes the dropping rate of legitimate packets for our proposed FMON scheme is less compared to the other two schemes. However as the number of attackers increases, the dropping rates increase.
Figure 7.13 Packet Delivery Ratio Vs Sending Rate

Figure 7.13 shows the impact on packet delivery ratio, based on sending rates. It is observed that when the sending rate is 50 kbps, packet delivery ratio of FMON scheme is nearly 20% more than SWAN scheme and 30% more than SPA-ARA. When the sending rate is increased to 200 kbps, FMON scheme achieves 29% improvement over SWAN and 55% improvement over SPA-ARA. From graph, it is also observed that as the sending rate is increased, the packet delivery ratio is reduced. However, for all sending rates our proposed FMON scheme gives better result than the other two schemes.

Figure 7.14 shows the impact on End to End Delay based on the sending rates. Since our FMON protocol identifies the attackers at intermediate nodes, the attackers are immediately removed from the network. Hence the average end to end delay in FMON scheme is less compared to SWAN and SPA-ARA schemes. However, the delay increases as the sending rate increases.
Figure 7.14 Average End to End Delay Vs Sending Rate

Figure 7.15 CPU Usage Vs Sending Rate
Figure 7.16 Memory Usage Vs Sending Rate

From Figure 7.15 and Figure 7.16, it is observed that CPU usage for FMON scheme is more than SWAN and SPA-ARA schemes and the memory usage is slightly less than that of the other two schemes.

From the above simulation results it is clear that our FMON scheme outperforms the other two schemes.

7.1.2 Results for RoQ Attack

We have experimented our FMON scheme, discussed in chapter 2 against RoQ attack. The UDP traffic flows are established in the network. All the source nodes negotiate a rate of 100 kbps for traffic flow and begin sending traffic at a rate of 100 kbps at time \( t = 1 \) sec. A request is sent from a node to destination node for sending traffic at a rate of 100 kbps and if adequate bandwidth is available, the node sends traffic at 100 kbps. The attacking flow is set at a rate of 500 kbps. The RoQ attack flow is established with an attacking rate (\( \delta \)) of 500 kb over the short period of time (\( \tau \)) of 0.1sec and the period of the attack (\( T \)) is 1 sec. The capacity of the link is set to 2
Mbps. Each simulation run lasts for 180 sec in order to allow the network to experience some levels of congestion.

The simulation is carried out in 2 different scenarios. In the first scenario, three traffic flows are established in the network. The number of attacking flows is initially set as 2 and the attacking period of the attack is varied from 1 sec to 5 secs. The packet delivery ratio at the destination node is obtained and then the throughput and Average End to End Delay are obtained for varying number of attacking flows.

### Packet Delivery Ratio Vs Period of Attack

![Packet Delivery Ratio Vs Period of Attack](image)

**Figure 7.17 Packet Delivery Ratio Vs Period of Attack**

**Table 7.1 Packet Delivery Ratio in terms of attack period**

<table>
<thead>
<tr>
<th>Attack Period(T) in secs</th>
<th>AODV</th>
<th>FMON</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>66.67</td>
<td>87.14</td>
</tr>
<tr>
<td>2</td>
<td>69.2</td>
<td>89.46</td>
</tr>
<tr>
<td>3</td>
<td>70.12</td>
<td>90.04</td>
</tr>
<tr>
<td>4</td>
<td>70.87</td>
<td>90.78</td>
</tr>
<tr>
<td>5</td>
<td>71.3</td>
<td>90.92</td>
</tr>
</tbody>
</table>
From the simulation results of Figure 7.17, it is observed that if the attacking period of the RoQ attack is increased, the packet delivery ratio can be increased. For the attacking period of 1 sec, packet delivery ratio of 87.14% is achieved with the proposed FMON scheme. If the attacking period is increased to 5 secs, the packet delivery ratio is increased upto 90.92%. This reveals that if a burst attack occurs with a smaller value of T, the attack traffic occurs more often than with the case of greater value of T. As the attack traffic is increased, the packet delivery ratio is reduced. The values of packet delivery ratio are listed in Table 7.1.

![Figure 7.18 Average Throughput with different No. of attackers]

**Table 7.2 Average Throughput under different No. of attackers**

<table>
<thead>
<tr>
<th>No. of attackers</th>
<th>AODV (Mbps)</th>
<th>FMON (Mbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0.11</td>
<td>0.159</td>
</tr>
<tr>
<td>2</td>
<td>0.1</td>
<td>0.158</td>
</tr>
<tr>
<td>4</td>
<td>0.098</td>
<td>0.157</td>
</tr>
<tr>
<td>6</td>
<td>0.088</td>
<td>0.155</td>
</tr>
<tr>
<td>8</td>
<td>0.079</td>
<td>0.154</td>
</tr>
<tr>
<td>10</td>
<td>0.064</td>
<td>0.152</td>
</tr>
</tbody>
</table>
Figure 7.18 shows the throughput variation with respect to no. of attackers. Since the proposed scheme is able to detect the attacker, effectively based on the flow details and is able to block the attacking flow, we are able to achieve with FMON scheme up to 95.5% of throughput for 10 attacking flows, whereas only 40.2% of throughput could be achieved with AODV. The values of average throughput are shown in Table 7.2.

![Average End to End Delay Vs No. of Attackers](image)

**Figure 7.19** Average End to End Delay Vs No. of Attackers

**Table 7.3** Average End to End Delay under different attackers

<table>
<thead>
<tr>
<th>No. of Attackers</th>
<th>AODV (secs)</th>
<th>FMON (secs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>0.075</td>
<td>0.078</td>
</tr>
<tr>
<td>4</td>
<td>0.127</td>
<td>0.038</td>
</tr>
<tr>
<td>6</td>
<td>0.311</td>
<td>0.187</td>
</tr>
<tr>
<td>8</td>
<td>0.599</td>
<td>0.367</td>
</tr>
<tr>
<td>10</td>
<td>0.839</td>
<td>0.51</td>
</tr>
</tbody>
</table>
Figure 7.19 shows that when the number of attacking flows is increased, the average end to end delay incurred is increased. It includes all possible delays caused by buffering during route discovery latency, queuing in the interface queue, retransmission delays at the MAC, propagation and transfer times. Since the attacking flows are rejected in the proposed scheme, based on the flow state information at every node, we are able to achieve a lower value of average end to end delay. It is observed that when the number of attackers is increasing from 2 to 10, the delay is increased to 6.5% with the proposed FMON scheme. But, with AODV 11.2% of delay could be achieved. The particulars of average end to end delay with different attackers are given in Table 7.3.

In the second scenario, the number of UDP flows is varied, the Packet Delivery Ratio & Average End to End Delay are obtained. The offered load could be varied by changing the CBR packet size, the number of CBR flows or the CBR packet rate. Figure 7.20 shows that as the number of flows is increased, the packet delivery ratio gets reduced. As the offered load is increased, the packet delivery ratio is reduced due to the network congestion. Since distributed rate control is applied in the proposed scheme, we are able to achieve the packet delivery ratio of 70.38% for 7 CBR traffic flows. It is observed that in case of AODV with attack, we are able to achieve only 29.22% of packet delivery ratio. Figure 7.21 shows that as the number of UDP flows is increased the average end to end delay is also increased due to the same reason. However with the proposed system we are able to achieve less delay. The details are shown in Table 7.4 and Table 7.5.
Figure 7.20 Packet Delivery Ratio with variable No. of UDP flows

Figure 7.21 Average End to End Delay with variable No. of UDP flows
Table 7.4 Packet Delivery Ratio with different no. of UDP flows

<table>
<thead>
<tr>
<th>No. of UDP flow</th>
<th>AODV with no attack</th>
<th>AODV with Attack</th>
<th>FMON</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>99.86</td>
<td>80.33</td>
<td>87.14</td>
</tr>
<tr>
<td>5</td>
<td>99.78</td>
<td>54.15</td>
<td>83.26</td>
</tr>
<tr>
<td>7</td>
<td>96.11</td>
<td>29.22</td>
<td>70.38</td>
</tr>
<tr>
<td>9</td>
<td>72.29</td>
<td>21.16</td>
<td>38.89</td>
</tr>
<tr>
<td>11</td>
<td>63.5</td>
<td>19.69</td>
<td>32.65</td>
</tr>
<tr>
<td>13</td>
<td>59.7</td>
<td>14.95</td>
<td>34.88</td>
</tr>
<tr>
<td>15</td>
<td>54.2</td>
<td>12.51</td>
<td>24.34</td>
</tr>
</tbody>
</table>

Table 7.5 Average End to End Delay with different no. of UDP flows

<table>
<thead>
<tr>
<th>No. of UDP flow</th>
<th>AODV with no attack (secs)</th>
<th>AODV with Attack (secs)</th>
<th>FMON (secs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>0.023</td>
<td>0.302</td>
<td>0.178</td>
</tr>
<tr>
<td>5</td>
<td>0.029</td>
<td>0.606</td>
<td>0.052</td>
</tr>
<tr>
<td>7</td>
<td>0.494</td>
<td>0.819</td>
<td>0.5054</td>
</tr>
<tr>
<td>9</td>
<td>1.095</td>
<td>1.49</td>
<td>1.167</td>
</tr>
<tr>
<td>11</td>
<td>1.75</td>
<td>2.499</td>
<td>1.914</td>
</tr>
<tr>
<td>13</td>
<td>1.93</td>
<td>2.86</td>
<td>2.066</td>
</tr>
<tr>
<td>15</td>
<td>2.21</td>
<td>3.24</td>
<td>2.782</td>
</tr>
</tbody>
</table>

In addition, the proposed scheme works well along with different routing protocols. Since mobility causes frequent network topology changes, routing is difficult in MANETs. When the nodes move, the established paths may break and the routing protocols must dynamically search for other feasible routes. Hence, the proposed method is experimented with both
proactive and reactive protocols. Ad hoc On-demand Distance Vector (AODV) and Dynamic Source Routing (DSR) are the reactive protocols which use an on-demand approach for finding routes. In reactive protocols, route is established only when it is required by a source node for transmitting data packets. Destination Sequenced Distance Vector (DSDV) is one of the proactive routing protocols which maintain routes to all destinations, regardless of whether or not these routes are needed. Figure 7.22 shows the compatibility of working the proposed scheme with different routing protocols such as AODV, DSDV and DSR.

![Impact of Routing Protocols](image)

**Figure 7.22 Impact of Routing Protocols**

### 7.2 EVALUATION OF MANETS BASED ON MATHEMATICAL ANALYSIS

The mathematical analysis of security improvement in MANETs is discussed in chapter 3. The expressions for the packet loss rate and packet delivery ratio have been derived. Evaluation of our network model is performed with the comparison of theoretical results and simulation results. The ad hoc network is formed with 20 nodes. Constant Bit Rate traffic is considered for analysis. The size of data packet is 512 bytes. The evaluation
is carried out in two different scenarios. In the first scenario, five data flows with randomly selected sources and destinations are taken. The node’s packet processing rate is taken as 4 packets/s. The queue size is 50 packets/s. The source node transmits data packets at the rate from 1 packet/s to 10 packets/s. The attack rate is 5 packets/s. The PDR is computed using Equation 3.18. In the second scenario, each source node transmits data packets at the rate of 2 packets/s. The attack rate is varied from 1 packet/s to 10 packets/s. All the other parameters are identical to that of the first case. The PDR for this case is again computed. The computation of PDR is described with an example: The packet arrival rate is 2 packets/s and No. of flows is 5, the traffic experienced, \( T(x) \) by a node \( x \) is then 10 packets/s. Taking Queue length \( Q \) as 50 packets/s and node’s packet processing rate as 4 packets/s, the probability of packet loss is computed using Equation 3.13.

\[
P_{loss \, x} = 1 - \frac{10}{4} \left( \frac{10}{4} \right)^{50} = 0.6
\]

Then the packet loss rate \( L_{loss}(x) \) is computed using Equation 3.14 as \( L_{loss}(x) = 10 \times 0.6 = 6 \) packets/s. Thus the overall packet loss rate \( L_{loss} \) in the network due to 20 nodes is \( 20 \times 6 = 120 \) packets/s. Taking utilization factor of legitimate user \( \rho_l \) as 2 packets/s and utilization factor of malicious user as 5 packets/s, the normal packet loss rate is computed using Equation 3.16, as

\[
L_{loss-normal} = 120 \times \frac{2}{2+5} = 34.28 \text{ packets/s.}
\]

Finally, PDR is computed using Equation 3.18 as

\[
PDR = \frac{5 \times 20 \times 2 - 34.28}{5 \times 20 \times 2} \times 100 = 82.85 \%
\]

The network is simulated with the same parameters using NS2 network simulator. Figure 7.23 and Figure 7.24 show comparison of theoretical and simulated values of PDR.
In Figure 7.23, it is observed that packet delivery ratio is 96.6 % when the source node transmits data at a rate of 1 packet/s and most packets get to the destination nodes. However, the packet delivery ratio reduces to 0.09% when the source node transmits data at a rate of 10 packets/s. In
Figure 7.24, it is observed that packet delivery ratio is 81.66 % when an intruder transmits attack packet at a rate of 1 packet/s. It is also seen that packet delivery ratio decreases as the attack rate is increased. It is finally observed that PDR obtained from simulation is closer to our theoretical results. This validates our theoretical model. However, the simulated values in each case are slightly lower compared to the theoretical values.

7.3 RESULTS FOR LBDS UNDER FLOODING ATTACK

LBDS against flooding attack has been discussed in chapter 4. We have implemented ad hoc flooding attack and attack detection using LBDS. NS2 is used for simulation. We compare the proposed LBDS with FMON (discussed in Chapter 2), HHCC (Yi & Shakkottai 2007) and AODV (Perkins et al 2003). The distributed coordination function of IEEE 802.11 for wireless LANs is used at the MAC layer. The simulation parameters are given in Table 2.1. We perform the simulation for 300 sec.

Attack traffic can be achieved by randomly generating Constant Bit Rate flows. A traffic generator was used to provide constant bit rate sources. We use packet delivery ratio as the metric to evaluate the performance of the detected system. The system performance based on packet delivery ratio has been observed under two different scenarios.

In the first scenario, ten connections with randomly selected sources and destinations are simulated. Each source transmits data packets at the rate of 2 packets/s. We vary the rates of attacking packets as 10 packets/s, 20 packets/s, 30 packets/s, 40 packets/s and 50 packets/s. In other words, the attacker floods 10, 20, 30, 40 and 50 packets every second. Packet delivery ratio for each attacking rate is determined. It is observed that packet delivery ratio goes down when attacker sends attacking packets at increasing rates. When the rate of attacking packets is less than 20 packets/s, the performance
becomes better after a period. But when the rate of attacking packets is more than 20 packets/s, the network cannot bear the attack anymore and the performance goes down quickly. The impact of packet delivery ratio with respect to attack rate is given in Figure 7.25.

In second scenario, ten UDP connections with randomly selected sources and destinations are simulated. The number of attackers is varied from 1 to 5. Each attacking node sends the attack traffic at a rate of 30 packets/s. The effect of packet delivery ratio is given in Figure 7.26. Here, it is observed that as the number of attackers is increased, the packet delivery ratio is reduced. In both scenarios, we observe that, the proposed LBDS performs better than FMON (discussed in Chapter 2), HHCC (Yi & Shakkottai 2007) and AODV (Perkins et al. 2003). In FMON, the attackers are detected based on the sending rate only and HHCC uses only queue length as a congestion measure. Since AODV (Perkins et al 2003) does not deal with any kind of security actions, under the influence of attack, the packet delivery ratio is very low compared to all the other three techniques.

![Figure 7.25 Packet Delivery Ratio in terms of Attack Rate](image-url)
We have also analyzed the performance of the network in terms of average end to end delay with varying no. of connections. End to end delay computes the time taken by all the packets that have been successfully sent from source node to the destination node. Figure 7.27 shows the impact of average end to end delay with respect to number of UDP connections. Here, we perform the comparison of LBDS with other protocols. It is observed that the average end to end delay is almost same up to 5 connections for all the protocols. When the number of connections increases, the end to end delay of LBDS is more than that of AODV and FMON. This increase in delay could be compromised with improved packet delivery ratio. However, the end to end delay of LBDS is less than that of HHCC.
MAODV scheme against RREQ flooding attack has been discussed in Chapter 5. The performance of proposed scheme against RREQ flooding attack is analyzed for MANETs with and without the proposed defense scheme, MAODV. The proposed MAODV scheme is also compared with detection scheme called ‘Filtering Scheme against RREQ Flooding Attack’ (FSRFA) proposed by Song et al (2006). The MAODV protocol was implemented and evaluated in the NS2 network simulation environment. The details of simulation parameters are specified in Table 2.1. We have considered no. of nodes, pause time, simulation time and no. of RREQ packets as the varying parameters to evaluate the performance of MANETs.
Figure 7.28 shows how the packet delivery ratio (PDR) is varied with respect to change in number of nodes to account for system scalability. It is seen that the PDR was improved up to 76.9% when our protocol, MAODV was implemented. The pause time was also varied and the PDR was obtained. Pause time can be defined as time for which nodes waits on a destination before moving to other destinations. Low pause time means node will wait for less time thus giving rise to high mobility scenario. Simulation results from Figure 7.29 show how PDR is changed by varying the pause time of a node in the network. It is clear that PDR increases as pause time increases. This is because low mobility allows more stable routing paths. However, it is not possible to achieve 100% packet delivery due to the unreliable links in wireless networks.

![Figure 7.28 Packet Delivery Ratio Vs No. of nodes](image-url)
Figure 7.29 Packet Delivery Ratio Vs pause time

Figure 7.30 describes how packet delivery ratio varies with respect to the simulation time. Here, simulation time is varied from 100s to 900s. It is observed that when no attack is involved, the AODV protocol provides almost constant packet delivery ratio of 95% over the simulation period. When RREQ flooding attack is incorporated, the packet delivery ratio is reduced to 24.4 % for the simulation time of 100s and it goes down to the value of 4.8 % for the simulation time of 900s. Our proposed defense scheme MAODV, improves the packet delivery ratio to 76.7 % for the simulation time of 100s and it comes to 63.8 % for the simulation time of 900s.
Figure 7.30 Packet Delivery Ratio in terms of Simulation time

Figure 7.31 Packet Delivery Ratio with varying No. of attackers
In Figure 7.31, we show the effect of varying the no. of attackers on PDR. Here, we consider simulation time of 400s. It is observed that we can achieve the packet delivery ratio of 73.8% for 2 attacker case and it reduces to 68.2% when the no. of attackers is increased to 10. It is observed from this result that as the number of attackers is increased, more bogus packets are propagated in the network. This reduces the packet delivery ratio.

Figure 7.32 shows that when the no. of RREQ packet increases, i.e., flooding attack is increased from 15 RREQ packets to 40 RREQ packets, the PDR goes down from 58.6% to 20.5%. But, without MAODV protocol, PDR is in the range of 7.8% to 1.8% for the RREQ packets of 15 to 40 respectively. This clearly shows that under the influence of flooding attack, PDR is reduced to a very low value. With MAODV, we are able to achieve the maximum of 58.6%, for 15 RREQ packets. Figure 7.33 gives the idea of average end to end delay with respect to no. of attackers. Delay is more for RREQ flooding AODV case than the case of AODV and delay for FSRFA
protocol is slightly above the AODV. We are able to achieve lower end to end delay with our proposed MAODV protocol. Since our proposed MAODV protocol effectively isolates the attacker from the network, it achieves better performance in terms of average end to end delay.

![Average End to End Delay Vs No. of Attackers](image.png)

**Figure 7.33 Average End to End Delay Vs No. of Attackers**

The advantages of our proposed defense scheme compared to other existing defense schemes are as follows. The proposed MAODV scheme counteracts the RREQ flooding attack before the attack rate reaches the UT. Even the RREQ rate reaches the LT, RREQ packets are not forwarded to the other nodes. This increases the detection rate of attacking nodes. FSRFA scheme proposed by Song et al (2006), use two threshold values, namely Rate limit and Black list limit to detect the attack. In our scheme, we not only use LT and UT to check the rate for detection of RREQ packet but also take steps to bypass the attack traffic based on checking whether the nodes adopt binary exponential back off or not. The traffic is again checked for its legitimacy using LT and UT. Hence, the proposed scheme improves the detection rate.
7.5 RESULTS FOR NRMT SCHEME AGAINST BLACK HOLE ATTACK

The network simulator NS2 is used to simulate the proposed NRMT detection algorithm. In our simulation, the channel Capacity of mobile hosts is set to 2 Mbps. The DCF of IEEE 802.11 is used for wireless LANs as the MAC layer protocol. The simulation parameters are listed in Table 2.1.

We have implemented the simulation of MANET under 4 different cases. In the first case, we have established the network with a single Black Hole node and in the second case, 2 Black Hole nodes are taken for analysis. A modified AODV protocol that simulates the behavior of a Black Hole node has been implemented and 50 scenarios each involving different ad hoc networks with 30 nodes each moving randomly were simulated. We have introduced a Black Hole in each scenario and compared the performance of the networks with and without a Black Hole. We then implemented the proposed protocol to detect and discard the Black Hole node.

The performance of the network is evaluated based on the packet loss rate. The total packet loss rates are calculated according to the ratio of missing packets to sent packets; in other words, the ratio of number of packets that failed to reach their destinations, to the total number of packets that are transmitted from all source nodes of the entire network. A MANET may have missing packets due to the mobility of nodes, even without an existing Black Hole attack.

Ten different UDP connections are taken for consideration. We measured the number of packets sent by the source node and received by the destination node. The total number of lost packets at the destination node and the number of lost packets at the Black Hole nodes are observed. The packet delivery ratio and packet loss rate are tabulated in Table 7.6.
Table 7.6  Packet delivery ratio and packet loss rate for different protocols

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Average No. of packets sent</th>
<th>Average No. of packets received</th>
<th>Packet Delivery Ratio (%)</th>
<th>Loss rate at destination (%)</th>
<th>Loss rate at Black Hole node(s) (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>AODV</td>
<td>1066</td>
<td>1025</td>
<td>96.15</td>
<td>3.85</td>
<td>-</td>
</tr>
<tr>
<td>AODV under single black hole node</td>
<td>1080</td>
<td>44</td>
<td>4.75</td>
<td>95.25</td>
<td>43.31</td>
</tr>
<tr>
<td>NRMT under single black hole node</td>
<td>1081</td>
<td>454</td>
<td>40.44</td>
<td>59.56</td>
<td>18.29</td>
</tr>
<tr>
<td>AODV under two black hole nodes</td>
<td>1075</td>
<td>12</td>
<td>1.12</td>
<td>98.88</td>
<td>72.49</td>
</tr>
<tr>
<td>NRMT under two black hole nodes</td>
<td>1076</td>
<td>236</td>
<td>21.93</td>
<td>78.07</td>
<td>31.02</td>
</tr>
</tbody>
</table>

From the results specified in Table 7.6, the following observations are made. In the absence of a Black Hole node, the average packet loss rate by AODV is about 3.85%; with one Black Hole node the average loss rate rises sharply to about 95.25%. This loss is partially due to packets dropped in the Black Hole node and partially due to congestion in the network over the paths towards the Black Hole node. The Black Hole node experiences the average loss rate of 43.31%. With the deployment of the proposed NRMT scheme, the average loss rate at the destination nodes can be successfully reduced to about 59.56% which is an improvement of 37.46% compared to the AODV protocol. It is also observed that the average loss rate at the Black Hole node is reduced from 43.31% (without NRMT) to 18.29%. (with
NRMT). With 2 Black Hole nodes, the average loss rate increases to 98.88%. This loss rate is greater than that of the case with a single Black Hole node. In the two Black Hole nodes case, the average loss rate at Black Hole nodes is 72.50%. The loss rate at the destination node is reduced to 78.07% with the NRMT scheme. Here, the average loss rate at the Black Hole nodes is reduced from 72.50% (without NRMT) to 31.04% (with NRMT).

In the third case, we have established two UDP traffic flows with the data rate of 10 kbps and the packet size of 512 bytes. An AODV protocol that simulates the behavior of a black hole has been implemented. 50 scenarios have been simulated each involving different ad hoc networks. A black hole has been introduced in each scenario. The performance of the networks with black hole (BHAODV) and without black hole (AODV) has been compared. The NRMT scheme has been implemented to detect and discard the black hole node. The proposed method is also compared with DPRAODV (Raj et al 2009) to show its effectiveness.

The performance of the network is evaluated based on the packet delivery ratio. The effect of black hole attack in AODV and the effect in NRMT method are observed from Figure 7.34. Since the black hole attack is effectively detected based on NRMT, it can be informed to all other nodes in the network immediately. Hence the attacker is removed or isolated from the network. The number of successfully received packets is increased and thus the packet delivery ratio increases. With black hole attack the packet delivery ratio is reduced to 16.1% for the network with 10 nodes. With our proposed NRMT protocol, we were able to achieve nearly 55% of packet delivery ratio. However, the packet delivery ratio for the AODV protocol without attack will be more for any number of nodes in the network.
The delay of all the packets that have been successfully transmitted from the source to the destination is used to compute the average end to end delay. All possible delays caused by buffering during route discovery latency, queuing in the interface queue, retransmission delays at the MAC, propagation, and transfer times are included for computation of average end to end delay. In the proposed NRMT scheme, we have adopted 2 step procedure to detect the black hole attack. Hence the average end to end delay for the NRMT scheme is greater than that in other cases. The effect of average end to end delay is shown in Figure 7.35. From the graph, it is clear that the average end to end delay is almost same up to 20 nodes in the network. But, when the number of nodes gets increased, the average end to end delay for the proposed scheme is increased more than the other protocols.

Routing overhead is calculated from the number of routing packets transmitted per data packet delivered at the destination. Each hop wise transmission of a routing packet is counted as one transmission. The routing load metric evaluates the efficiency of the routing protocol. The routing overhead is also evaluated with varying number of nodes. The overhead with
the proposed scheme is greater than the black hole attack case. This is because of the control packets that are sent to the nodes in the network by the node which detects the black hole. The routing overhead required for NRMT method is greater than that required for the AODV protocol without attack and also DPRAODV. The effects of routing overhead are shown in Figure 7.36.

Figure 7.35  Impact of Average End to End Delay with varying No. of Nodes

Figure 7.36  Impact of Routing Overhead with varying No. of Nodes
In the fourth case of simulation the number of UDP flows is varied. The packet delivery ratio, average end to end delay and routing overhead are evaluated. The impact is shown from Figure 7.37 to Figure 7.39. From Figure 7.37, it is seen that, when the number of flows is 2, under black hole attack, we are able to achieve packet deliver ratio of only 9.5%. The proposed NRMT scheme gives packet delivery ratio of around 59%. It is observed that the proposed scheme gives better packet delivery ratio than the black hole attack case and DPRAODV. But the average end to end delay and the routing overhead are greater than the black hole attack case.

![Figure 7.37 Impact of Packet Delivery Ratio with varying No. of Flows](image)

It is also observed from Figure 7.38 that the average end to end delay is almost same for all the cases when the no. of flow is below 4. But as the no. of flows increases from 4, delay gets increased. With our proposed scheme, the average delay obtained is increased by 8.2 times more when the no. of flows is increased from 4 to 10.
Figure 7.38 Impact of Average End to End Delay with varying No. of Flows

Impact of Routing Overhead with varying no. of flows is specified in Figure 7.39. The routing overhead is also nearly equal for all cases as the no. of flow takes lower values of 2 to 4. As no. of flows is increased from 4, the routing overhead also increases much. It is increased by 6.7 times that of initial overhead, when the no. of flows is increased to 10.

Figure 7.39 Impact of Routing Overhead with varying No. of Flows
Intel® core™ 2 Duo CPU, 789 MHz, 1.99GB of RAM is used to perform the computation of CPU usage and memory usage. ‘Top’ program is used to measure the impact of the simulation on the processor. From Figure 7.40 and Figure 7.41, the impact of CPU usage and memory usage with the mobility of MANET is observed. It is seen from the figures that CPU usage for our scheme is slightly more than the other two schemes and the memory usage is slightly more than AODV and less than DPRAODV. This is because NRMT grows as a function of neighborhood nodes. We also find that low mobility allows more stable routing paths.

![Figure 7.40 Impact of CPU usage with pause time](image)

Figure 7.40 Impact of CPU usage with pause time
Figure 7.41 Impact of Memory usage with pause time

In normal AODV, when the node receives the RREP packet, it first checks the sequence number value in its routing table. If the sequence number of RREP is higher than the sequence number in its routing table, the RREP packet is accepted. In BHAODV, the black hole node assigns a high value of sequence number. Hence, the traffic is sent to black hole node. This reduces the no. of packets successfully delivered to the destination node. This effect results a significant reduction in packet delivery ratio. In DPRAODV, RREP sequence number is checked whether it is higher than the threshold value. If the value of RREP sequence number is higher than the threshold value, the node is suspected to be malicious. If the node detects an anomaly, it sends a control packet, ALARM to its neighbors. The neighboring nodes then find that RREP packet from the node is discarded. In our proposed NRMT scheme, we perform double check to identify the black hole node. The first check is based on the time of reply and the second check is based on the threshold value. Because of the double check, the probability of identifying the attacker is more. Hence the packet delivery ratio of NRMT is more than
BHAODV and DPRAODV. However, due to this double check, the average end to end delay and no. of control packets for NRMT is greater than the other protocols. Though the average delay and routing overhead are greater for NRMT, the increased value of packet delivery ratio improves the network performance significantly.

7.6 CONCLUSIONS AND SCOPE OF FUTURE WORK

MANETs are highly vulnerable to attacks because of their particular characteristics such as open network architecture, shared wireless medium, stringent resource constraints and highly dynamic network topology. In particular, DDoS attacks can severely degrade network performance with relatively little effort expended by the attacker. DDoS attacks in MANETs are difficult to detect. MANETs are particularly more vulnerable to ad hoc routing attacks. There are a wide variety of routing attacks that target the weakness of MANETs. This work focuses on mobile ad hoc network's routing vulnerability and analyzes the network performance under two types of attacks namely, flooding attack and black hole attack. These attacks can easily be employed against the MANETs. The resistive schemes against these attacks are proposed in this work.

In chapter1, we have discussed the security attacks and its countermeasures in detail. In Chapter 2, we have discussed the DDoS data flooding attack and a special case of DDoS attack, which is a low rate RoQ attack. Main research efforts to counter these attacks are also discussed. We have proposed a congestion based defense scheme to mitigate DDOS attacks in MANETs which has both reliability and security features.

The FMON protocol could be an important component in an overall architecture of MANETs to provide security and QoS. By simulation results, we found that our proposed FMON scheme achieves higher throughput and
higher packet delivery ratio with varying no. of attackers and different sending rates. This is due to the fact that the attacking flows are detected by intermediate nodes using FMT and the attackers are effectively blocked in our proposed FMON scheme. Hence, the network resources are made available to legitimate users in MANETs. Since, FMT size grows as a function of the number of neighbor nodes rather than the number of traffic flows traversing the node, the average end to end delay is also low. We also observed that better performance is achieved for lower pause time. This is because low mobility allows more stable routing paths. We also found that that our FMON scheme works well along with different routing protocols such as AODV, DSDV and DSR.

Chapter 3 deals with mathematical analysis for MANETs with DDoS flooding attack. In this work, we have analyzed the packet loss rate and packet delivery ratio in MANETs. The performance of MANET is evaluated with FMON by comparing theoretical results and simulated results. It is observed that packet delivery ratio of simulation results and theoretical results are in close agreement. Since collision is also taken into account in addition to congestion for simulation, simulated values are slightly lower compared to theoretical values.

In Chapter 4, we have discussed our proposed LBDS. We have developed a detection scheme against flooding attack which uses load balancing method along with active queue management technique. The results obtained from the NS2 based simulations show that we are able to achieve greater packet delivery ratio with varying no. of attackers and attack rate compared to other protocols with which we have simulated. Generally, queue size is used as load information. But in our proposed LBDS, we use Channel Occupancy Time and Queue size as the basis for load balancing. Hence our technique can detect flooding attacks more accurately. However,
the average end to end delay for our proposed scheme is slightly more than the other methods that we have taken for comparison. Since our proposed LBDS involves the computation of load metric value, it takes some additional time for the detection of malicious node. Hence, the average end to end delay takes a larger value.

In Chapter 5, we have discussed RREQ flooding attack and our proposed MAODV scheme. By simulation results, we found that our proposed MAODV scheme achieves higher packet delivery ratio with varying no. of nodes, pause time, no. of attackers and no. of RREQ packets. Generally, the RREQ flooding attacks are detected based on the threshold values. In our MAODV protocol, we apply an additional step to bypass the attack traffic based on checking whether the nodes adopt binary exponential back off or not. This improves the detection rate of attackers in MANETs. Hence, our proposed scheme achieves greater packet delivery ratio. Since the attackers are effectively identified and removed from the network, we are able to achieve lower value of average end to end delay.

In Chapter 6, we have discussed black hole attacks and our proposed NRMT scheme to detect black hole attacks. By attacking the routing protocols, attackers can absorb network traffic, injecting themselves into the path between the source and destination. We have presented a feasible solution for the detection of black hole attack on top of AODV protocol. The solution overcomes the effect of black hole attacks and prevents the network from further malicious behavior.

By simulation results, we have analyzed the performance of the MANETs with and without a black hole node. We have also tested the performance of MANETs with two black hole nodes. The results show that the presence of black hole nodes increases the packet loss in the network considerably. Generally, for the detection of black hole attacks, destination
sequence numbers checking is used. In our proposed NRMT method, we include the additional checking based on time of reply of a packet. Hence, the proposed NRMT scheme effectively reduced the packet loss due to black hole attacks. Therefore, the packet delivery ratio gets increased. However, the average end to end delay and the routing overhead are increased due to this extra checking in the detection process of NRMT scheme. Simulation results validate the effectiveness of our protocol against black hole attack. The experimental results prove that the proposed solution improves the network performance considerably.

In Section 7.1 to Section 7.5 of this chapter, we present results and discussions of all proposed schemes described in Chapter 2 to Chapter 6. The results are compared with other existing protocols and it is observed that our proposed schemes outperform the other protocols with which we have compared.

Future works in these areas could be to develop a detection scheme for securing the network from other types of attacks such as wormhole attack, byzantine attack and rushing attack and also to experiment with the scheme for preventing cooperative attacks in MANETs. The proposed mechanism can also be applied for securing the network from other routing attacks by changing the security parameters in accordance with the nature of the attacks.