5. Analysis of Results

5.1 Introduction

A detailed evaluation of the simulation procedure followed to create the Mobile ad hoc network and the estimating the performance of AODV routing protocol under Blackhole attacks is discussed in the previous chapter. As mentioned in the previous chapter there are three important scenarios where the first scenario has idle working conditions of AODV routing protocol, second scenario has Blackhole attacks on the network and the third scenario has improved performance of AODV. Three scenarios are run for one hour and the corresponding results are explained in this chapter. Performance metrics are chosen at global level like AODV, FTP, HTTP and Wireless LAN level and the corresponding graphs are explained as below

5.2 AODV metrics considered for three scenarios

As the main aim of this simulation is to evaluate the performance of AODV under black hole attacks, AODV routing protocol parameters are chosen. Comparison graphs of three scenarios for the AODV parameters is as given below
**Number of hopes per route**

Number of hopes per route indicates the overall hopes traversed during the communication process and it plays an important role in evaluating the performance of AODV routing protocol. The actual number of hopes traversed across the route by the three scenarios is given below.

![Graph showing number of hops per route](image)

From the above graph it is clear that across the first scenario the number of hopes is constant at the beginning of simulation and later it was decreased against its normal working conditions. When the case with attacks scenario is considered the
number of hopes traversed is always increasing and also more when compared to rest of the scenarios. In the third scenario a standard rate of hopes are traversed and this indicates that the performance of AODV has increased even in case of Blackhole attacks[20,21,55].

5.2.1 Route discovery time

Route discovery time indicates the overall time taken to discover the route across the communication process. Route discovery time depends on several factors like the overall traffic over the network and the nature of the applications and the actual comparison of the scenarios is as given below
From the above graph it is clear that across the first scenario the route discovery time is constant at the beginning of simulation and later it was decreased against its normal working conditions. When the case with attacks scenario is considered the discovery time is high initially and later on decreased due to increase number of hopes when compared to rest of the scenarios. In the third scenario a standard route discovery time is recorded and this indicates that the performance of AODV has increased even in case of Blackhole attacks[56].
5.2.2 AODV routing traffic received in bits per sec

Routing traffic received across the network indicates the overall performance of the mobile nodes and the wireless LAN server. The actual performance of AODV is estimated based on the routing traffic received in bits per sec and the actual bit rate for the three scenarios is as given below.

From the above graph it is clear that the overall traffic received in bits per sec is more across the first scenario as there are normal working conditions. When the
case with second scenario is considered the overall traffic received is very less due
to the Blackhole attacks and in the third scenario the overall traffic received has
increased and the performance of AODV has improved a lot when compared to
second scenario[57].

5.2.3 AODV Routing traffic received in packets per sec

Routing traffic received across the network indicates the overall performance of
the mobile nodes and the wireless LAN server. The actual performance of AODV
is estimated based on the routing traffic received in packets per sec and the actual
bit rate for the three scenarios is as given below

![Graph showing routing traffic received](image)
From the above graph it is clear that the overall traffic received in packets per sec is more across the first scenario as there are normal working conditions. When the case with second scenario is considered the overall traffic received is very less due to the Blackhole attacks and in the third scenario the overall traffic received has increased and the performance of AODV has improved a lot when compared to second scenario[58].

5.2.4 AODV Routing traffic sent in bits per sec

Routing traffic sent across the network indicates the overall performance of the mobile nodes and the wireless LAN server. The actual performance of AODV is estimated based on the routing traffic sent in bits per sec and the actual bit rate for the three scenarios is as given below
From the above graph it is clear that the overall traffic sent in bits per sec is more across the first scenario as there are normal working conditions. When the case with second scenario is considered the overall traffic sent is very less due to the Blackhole attacks and in the third scenario the overall traffic received has increased and the performance of AODV has improved a lot when compared to second scenario[59].
5.2.5 AODV Routing traffic sent in packets per sec

Routing traffic sent across the network indicates the overall performance of the mobile nodes and the wireless LAN server. The actual performance of AODV is estimated based on the routing traffic sent in packets per sec and the actual bit rate for the three scenarios is as given below
From the above graph it is clear that the overall traffic sent in packets per sec is more across the first scenario as there are normal working conditions[60]. When the case with second scenario is considered the overall traffic sent is very less due to the Blackhole attacks and in the third scenario the overall traffic received has increased and the performance of AODV has improved a lot when compared to second scenario.

5.2.6 AODV Total cache replies sent

Total cache replies sent indicates the overall response sent from the wireless LAN server and the actual performance of AODV routing protocol depends on the cache replies sent[61,62]. Cache replies should be less for the idle working conditions of AODV and the actual comparison graph is as shown below
From the above graph it is clear that the overall cache replies are less in the first scenario and thus indicates the idle working conditions of the network. When the case with second scenario is considered the overall cache replies sent is more due to the Blackhole attacks and thus the value has increased a lot[63,64,65]. When the case with third scenario is considered the number of cache replies are reduced when compared to the second scenario and thus the performance of the AODV has increased.
5.2.7 AODV Total packets dropped

Total packets dropped indicate the traffic conditions over the network due to routing protocol performance. The actual number of packets dropped across the network and performance of AODV for the three scenarios is given in the below screen.
From the above graph it is clear that across the first scenario initially the packet drop is low and later on the value has maintained a constant value due to the idle working conditions of the network and AODV[66,67]. When the case with second scenario is considered due to Blackhole attacks the packet drop is regularly increasing as the overall intruder traffic has increased. When the case with third scenario the performance of AODV has improved a lot and the packet drop has decreased throughout the simulation time.

5.3 File Transfer Protocol results

Two applications are used across the simulation like FTP and HTTP and the performance metrics of FTP are evaluated in this section and given below

5.3.1 Download response time

Download response time indicates the actual time taken to download a file from the server by the clients. The actual download response time consumed across the three scenarios is given as below
From the above graph it is clear that the overall download response time is increasing across the first scenario and later on the value has reduced due to idle working conditions[68]. When the case with second scenario is considered the download response time has increased due to Blackhole attacks over the network and initially the value was very high and due to less traffic conditions the value has reduced maintained a constant value. Performance of the AODV routing protocol has increased across the third scenario and the download response time is reduced
when compared to rest of the scenarios and thus the performance has improved a lot[4,8,69].

5.3.2 Traffic received bytes per sec

Traffic received due to the FTP application across the network indicates the overall performance of the AODV routing protocol across the network. In general the overall traffic received should be less for a better performance of AODV and the actual comparison of the scenarios is given below
From the above screen it is clear that the overall traffic received is less across the first scenario and this is due to the idle working conditions of the network. When the case with second scenario is considered the overall traffic received is more due to the Blackhole attacks as the attacks always pretend fake traffic to access the file access and thus the server can’t be reached. The overall traffic received has reduced when compared to attacks scenario and thus the performance has increased[61,70,71].

5.3.3 Traffic sent in bytes per sec

Traffic sent due to the FTP application across the network indicates the overall performance of the AODV routing protocol across the network. In general the overall traffic sent should be less for a better performance of AODV and the actual comparison of the scenarios is given below
From the above screen it is clear that the overall traffic received is less across the first scenario and this is due to the idle working conditions of the network. When the case with second scenario is considered the overall traffic received is more due to the Blackhole attacks as the attacks always pretend fake traffic to access the file access and thus the server can’t be reached. The overall traffic received has reduced when compared to attacks scenario and thus the performance has increased[72].
5.3.4 Upload response time

Upload response time indicates the actual time taken to upload any file to the server and the role of AODV routing protocol is significant in this context. The actual upload response time recorded across the three scenarios is given in the below screen.

Upload response time is high across the first scenario due to the normal and ideal conditions across the network and the values are varying as well. When the second
scenario is considered due to the Blackhole attacks the upload response time is reduced a lot and the upload response time has improved in the case with the third scenario. Due to the wireless LAN parameters and AODV configuration parameters set across the third scenario the overall performance of AODV under Blackhole attack has increased exponentially[62,73].

5.4 HTTP application results

HTTP application is used to estimate the performance of web applications against the AODV routing protocol under Blackhole attacks[74]. There are many aspects under HTTP that can be considered while estimating the performance of AODV and few of them are listed as below

5.4.1 Page response time

Page response time indicates the actual time taken to load a page from the web server and in ideal conditions the response time should be high. When the three scenarios are compared the actual comparison graph is as given below
From the above graph it is clear that the overall page response time is high across the first scenario due to the normal working conditions of the MANET and AODV routing protocol[75]. When the case with second scenario is considered the overall page response time is very low due to the Blackhole attacks. Across the third scenario is considered performance of AODV is improved due to the integral configurations and the overall page response time is also increased.
5.4.2 Traffic received bytes per sec

Traffic received across the web server indicates the application range and also the performance of AODV routing protocol. The actual traffic received in bytes per sec across all the three scenarios is as shown below
From the above screen it is clear that the application traffic received across the web server for the first scenario is low when compared to other scenarios and this is due to the normal working conditions of AODV. When the case with second scenario is considered the overall traffic received is very high when compared to rest of the scenarios as the routing protocol is affected with Blackhole attacks. Third scenario has improved a lot in terms of overall traffic received and thus the performance of AODV has improved due to the internal configurations done to AODV and Wireless LAN server[52,76,77].

5.4.3 Traffic sent in bytes per sec

Traffic sent across the web server indicates the application range and also the performance of AODV routing protocol. The actual traffic sent in bytes per sec across all the three scenarios is as shown below
From the above screen it is clear that the application traffic sent across the web server for the first scenario is low when compared to other scenarios and this is due to the normal working conditions of AODV. When the case with second scenario is considered the overall traffic sent is very high when compared to rest of the scenarios as the routing protocol is affected with Blackhole attacks[64,78]. Third scenario has improved a lot in terms of overall traffic received and thus the
performance of AODV has improved due to the internal configurations done to AODV and Wireless LAN server[79].

Following are some of the important tables that can be used to compare the performance of the network with tested IDS with rest of the normal and attacks scenario. AODV routing protocol parameters are as listed in the tabular format

<table>
<thead>
<tr>
<th>Parameter Description</th>
<th>Normal scenario</th>
<th>Attacks scenario</th>
<th>AODV Performance scenario</th>
</tr>
</thead>
<tbody>
<tr>
<td>AODV route discovery time</td>
<td>0.0487 sec</td>
<td>0.1986</td>
<td>0.1288</td>
</tr>
<tr>
<td>Routing traffic received in packets per sec</td>
<td>667.24</td>
<td>637.13</td>
<td>667.59</td>
</tr>
<tr>
<td>Routing traffic sent in packets per sec</td>
<td>29.79</td>
<td>29.47</td>
<td>29.49</td>
</tr>
<tr>
<td>Total packets dropped</td>
<td>19.88</td>
<td>39.5</td>
<td>8.41</td>
</tr>
<tr>
<td>Total route errors</td>
<td>11.40</td>
<td>1</td>
<td>12.14</td>
</tr>
</tbody>
</table>
5.5 Wireless LAN Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Normal scenario</th>
<th>Attacks scenario</th>
<th>AODV performance scenario</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data dropped bits per sec</td>
<td>221.97</td>
<td>504.48</td>
<td>53.44</td>
</tr>
<tr>
<td>Load</td>
<td>46568.55</td>
<td>49264.2</td>
<td>47907.1</td>
</tr>
<tr>
<td>Network Load</td>
<td>46411.3</td>
<td>49023.4</td>
<td>47959.68</td>
</tr>
<tr>
<td>Retransmission attempts</td>
<td>0.1163</td>
<td>0.1404</td>
<td>0.1408</td>
</tr>
<tr>
<td>Throughput bits per sec</td>
<td>302598.8</td>
<td>288330.26</td>
<td>278858.26</td>
</tr>
</tbody>
</table>