Chapter 3
Digital Security Certificate Chains to Detect Black Hole Attack in MANET

3.1 Introduction

MANET provides a possibility of creating a network in situations where setting the infrastructure would be impossible or prohibitively expensive. The dynamic changing nature of network topology makes any node in MANET to join and move out of the network at any instant. The control towards the management of the nodes in the MANET is distributed and this feature does not give assurance towards the security aspects of the network. There are many routing attacks caused due to lack of security. In general, attacks are the threats against the physical, MAC and network layer which are the most important layers that functions for the routing mechanisms of MANETs. The network layer is affected by the black hole attack, where the black hole node either does not forward the packets or edits the messages by adding or changing the parameters in the routing messages. Most of the routing protocols do not address the issues of the black hole routing attack. This results in a strategy requirement to overcome the black hole attacks in MANET. The solution is proposed to detect and prevent the black hole attack using the digital security certificate and it is implemented in AOMDV and DSR protocols.

3.2 SAOMDV Protocol Scheme

The proposed scheme Security Enhanced AOMDV (SAOMDV) is implemented in AOMDV to authenticate the node by issuing the digital security certificate to all the other nodes in the network. The digital security certificate authentication avoids the black hole node during the route discovery process. The scheme proposed to detect the black hole node is divided into route discovery process, authentication process and the black hole node detection process. SAOMDV enters into the route discovery process and the nodes on the selected route will start exchanging the digital security certificate with the neighboring
nodes, which in turn is verified for authenticating the neighboring nodes. Node authentication is followed by the black hole node detection process.

### 3.2.1 Route Discovery Process

When a source node S wants to find a route to a destination node D, it checks in the routing table whether the route to the destination node D is already available. If there is no previous route to the destination then the node S broadcasts a RREQ packet to the neighboring nodes. When a RREQ packet arrives at an intermediate node, RREQ is scanned and if the destination address of the RREQ is same as the address of intermediate node then the intermediate node will send the RREP otherwise it rebroadcasts the RREQ. The destination node that receives the RREQ will unicast the RREP packet to the source. Any malicious node may reply fast to the request from the source by claiming to have the shortest path to the destination. Once the RREP is received, the source node checks whether the RREP has arrived within the delay time. If the RREP has arrived too earlier than the delay time, then the source node assumes that node as the malicious node and simply ignores the concerned RREP. If the RREP from the nodes are valid then all the nodes on the routes enter into the authentication phase. All the disjoint routes are stored in the routing table. The stored routes in the routing table are sorted based on the shortest communication cost. The route with the shortest communication cost is established as the selected route. The following Algorithm 3.1 elaborates the route discovery process of SAOMDV protocol scheme.

```plaintext
1. BEGIN
2. Initialize Source, Destination.
3. Assign S= Source, I- Intermediate node, D= Destination, α- small step value
4. Calculate the Delay Time for all the node in the Network
5. DT = (α · Old_DT) + ((1 − α) · New_DT)
6. Route Discover(data packet)
7. BEGIN
8. IF (S) THEN Lookup Route Table (Dest_id)
9. |
10. IF(Route_not_found) THEN addRouteEntry(Destination_id)
11. |
12. Dest_seq_no= undefined;
13. seq_no= seq_no +2;
14. |
15. ENDIF
```

54
16. } 
17. ELSE 
18. { 
19. Bcast_id = Bcast_id +1; 
20. Broadcast_RREQ(source_id:seq_no:0,0,Destination_id:Dest_id,Dest_seq_no:
21. Dest_seq_no,advertisedHopCount:0) 
22. } 
23. ENDIF 
24. IF (I is NOT( D)) THEN {Rebroadcast RREQ} 
25. ELSE 
26. { 
27. D return RREP 
28. D unicasts RREP 
29. forward the RREP 
30. } 
31. ENDIF 
32. IF (RREP reaches S) THEN 
33. { 
34. IF (RREP Time < the Delay time )THEN 
35. Ignore RREP 
36. } 
37. ELSE 
38. { 
39. Route is established between S and D 
40. } 
41. ENDIF 
42. STORE the Alternate Routes 
43. END; 

Algorithm 3.1: Route Discovery process of SAOMDV

### 3.2.2 Authentication Process

To prevent the black hole nodes from dropping the packets, the selected route is not used for the data transmission immediately. After the route discovery process the nodes enter into the authentication phase for being authenticated by the neighboring nodes in the path. All the nodes in the selected route try to authenticate its neighbors by issuing the digital security certificates. To generate the digital security certificate, secured public key of the node should be created. The nodes request the IP address of its neighbor and it generates the secured public key by applying the hash function.

\[ \text{HMAC}_p(K) = h(K + \text{spad}) || h(K + \text{epad}) || M) \] (3.1)
where $HMAC_{pk}(M)$ is the hash function of the message $M$ and the message is the IP address of the node. $h()$ is the underlying hash function, $spad$ and $epad$ are the starting and ending padding sequence. $K$ is the secret key. $HMAC$ provides the secured public key which cannot be attacked by the intruders [69].

The digital security certificate is a self organized PKI certification where the public key is authenticated by the chain of nodes. A node in the network can issue certificate to every other node within the radio communication range of each other. Every node in the network should be able to authenticate the other nodes in the network, by creating and issuing the certificates to the neighbors. The node also maintains the certificates received from the other neighbors. The certificates are issued based on security trust value. The nodes make a periodical request for the certificates from the neighbors. The digital certificates are validated based on the public key which is one of its components. The digital certificate contains the following components.

$$[IP-ADDRESS, PK, TV, ET] \text{ KEY OF THE ISSUE NODE}$$

For example, the certificate issued by source $S$ to an intermediate node $I$ is given in the following form.

$$DSC(S \rightarrow I) = [IP,key_I,TV,ET] \text{ key } S$$

$PK$ is the public key of the receiver node. $TV$ is the Trust Value of the node and $ET$ is the Expiration Time of the certificate. Before generating a certificate the issuer node checks whether the $TV$ value is feasible. If it is feasible, the public key is generated and the certificate is issued to the receiving node and a copy of the same is stored in the routing table of the issuer. $TV$ is calculated based on the time taken to process the RREQ packet and the location of the node. The malicious node which receives the RREQ will immediately process the RREQ by sending the RREP immediately without verifying the route table for the availability of the node’s routing information. When the source node receives the RREP too earlier than the expected time, it suspects the RREP initiator to be the black hole node and it ignores the route with the black hole node and selects the
alternate route [48] [67]. The certificates exchanged periodically between the neighboring intermediate nodes are as follows.

\[ DSC( S \rightarrow A )DSC( A \rightarrow B )DSC( B \rightarrow D ) \]

Here A and B are the intermediate nodes, S and D are the source and destination nodes respectively. The source waits for the authenticated reply from the destination node. The destination node sends the authenticated message appended with the digital security certificate that is issued by the neighboring node in the network [93]. The authenticated RREP packet from the destination would be in the given form.

\[[Source ID, NextHop ID, Final Dest ID, DSC]\]

The RREP packet from D would be [D, B, S, DSC(B \rightarrow D)]. When this packet reaches the node B, it checks its routing cache to verify whether DSC(B \rightarrow D) is available. It checks whether D is the black hole node by verifying the list of certificates issued by B. If D is the promiscuous node then it forwards the RREP packet to A by appending its certificate. The process is continued by all the intermediate nodes in the route until the RREP reaches the source node. B forwards the RREP to the intermediate node to A. Finally, RREP that reaches S from A will be in the form as follows.

\[[ D, B, A, S, DSC( B \rightarrow D ), DSC( A \rightarrow B ), DSC( S \rightarrow A )]\]

When the RREP reaches S, it checks the whole certificate group. If there are no issues in the certificate, node S trusts that the route is secured and starts sending the packets through the route and the trust value of the intermediate nodes on the route is incremented. If any issues are found then the trust value of the node is decremented and the route is announced as the malicious route. The following Algorithm 3.2 explains the node authentication process of SAOMDV protocol scheme.
1. **BEGIN**
2. Nodes forming the route certify each other
3. 
4. Request ID and security parameters of Intermediate nodes
5. Generate public key of Intermediate nodes based on ID
6. Issue Certificates encrypted with public key
7. Store Certificates in route cache
8. Exchange Certificates with neighbor nodes
9. }
10. D sends certified RREP appended with Digital Security certificate from Intermediate nodes. Assign $TV = 1$
11. For $I = N$ to 1
12. 
13. IF isAvailable(DSC(D)) in I THEN
14. 
15. IF(I DSC(D)) = DSC(D) THEN
16. Append their certificates and forward the certified RREP}
17. ELSE
18. Revoke the DSC from the Node
19. }
20. RREP reaches S
21. S verifies certificate chain of the route unicasted by D.
22. IF isVALID(Certificate Chain) THEN send the Data Packets through the Route.
23. $TV = TV + 1$
24. Else
25. Broadcast the route as malicious route to all the other nodes in the network.
26. Stop forwarding data packets.
27. Select the alternative route from Route Cache.
28. **END**;

Algorithm 3.2: Node Authentication Process

### 3.2.3 Black Hole Node Detection Process

If any of the digital security certificates is found to be mismatching, which means that if two different nodes holds the digital security certificate with the same public key or two different digital security certificates are assigned for the same node then the corresponding node is assumed to be a black hole node. The route including the black hole node is ignored. The alternate route is selected from the routing table. The source ignores the alternate paths if it includes the malicious node which is been traced in the previous route.

The Algorithm 3.3 explains the alternate path selection approach in the black hole node detection and removal process for the secured data transmission in MANET. The
source node implements this algorithm to select the alternate route, when the route selected for the transmission is attacked by the malicious nodes.

To prevent a legitimate node turning malicious over a period of time, the node’s behavior would be recorded and if the behavior of the node is found to be unsatisfactory, then the certificate would not be renewed after its expiry time, therefore the node is isolated from further participation in the network activities. Since the security levels of participating nodes are updated based on their faithful participation in the network, any black hole node between the source and destination can be very well isolated from the network as these nodes would not be able to provide the certificates to be appended with the RREP message.

Algorithm 3.3: Alternate path selection Algorithm

1. BEGIN
2. Let $S$ is a set of $S-1$ Alternate paths
3. Let $p_1,p_2,p_3,........,p(s-1)$ be the alternate paths that are stored at two dimensional array $S$.
4. Let $N$=set of paths that are node disjoint and free from malicious links.
5. Initialize $N=0$.
6. Let $P_m$ be the path with malicious node.
7. For $k=1$ to $S-1$ do
8. {
9. Select $P_k$ from $S$ and Check whether it includes the malicious link.
10. If ($P_k \cap P_m = 0$ )
11. then add $P_k$ to $N$
12. }
13. If $N=0$ then
14. Goto Route Discover(data _packet)
15. Else
16. Route selected = $P_k$ // $P_k$ is the shortest path with no malicious link.
17. END

SAOMDV computes the multiple loop free paths during the route discovery process and all the disjoint routes are stored in the routing table. With the availability of the multiple paths, the protocol switches from one route to the next possible best route when the previous route fails. The new route discovery process is initiated only when all the paths to a specific destination fails. The loop free link disjoint paths and multipath routing are very effective in reducing the routing overheads and supporting in better load balance.
A switch to the alternative routes will avoid the node congestion. This factor reduces the overheads to perform a new route discovery at each time when a route in use breaks.

### 3.3 SDSR protocol Scheme

The proposed Security Certified DSR (SDSR) protocol scheme is an extension of DSR where the route discovery phase is extended and messages are signed to guarantee their authentication. The extended route discovery process of SDSR consists of the route discovery process followed by an authentication phase. The route cache of DSR protocol stores the route for each node in the network. This route cache can be refreshed periodically to store the fresh routes.

Once the route is established between the source and the destination, the nodes forming the route enter into an authentication phase. The source node requests the identity of the next hop node and generates a public key based on its identity. The time taken to process the RREQ packet and the location of the node are the ideal parameters to determine the security level of the node with respect to black hole attack. The security parameters of the next hop node are requested and security certificates are issued if the issuer is convinced about the security parameters. The malicious node which receives the RREQ replies by sending the RREP immediately without any time delay. In this case the source node sets a minimum time delay to receive the RREP. If it receives the RREP in advance, then the source suspects the RREP initiator to be black hole node and initiates the black hole node detection and removal process.

All digital security certificates issued are stored in the repositories of the issuer. Exchange of certificates between the neighboring nodes takes place periodically. By this certificate exchange mechanism, nodes accumulate certificates in their repositories at a low communication cost because the exchanges are performed locally in one hop. The Route discovery phase, Authentication and Black hole node detection phase of SDSR is similar to the proposed protocol scheme SAOMDV. In case of the SDSR protocol once if the route is affected by the black hole nodes, the source node checks for the availability of the route in the route cache and use another cached route.
3.4 Performance Evaluation

The proposed scheme to detect and prevent the black hole attack in MANET are simulated using NS2.34 simulator. This research work assumes the network model to be asynchronous, where there is no reliability for the delivery of the message at the suitable destination. The four types of mobile nodes defined in the network are source node(S), destination node (D), intermediate nodes (I, A, B, C) and the malicious node (M). The source node S generates the traffic and sends it to the destination node D. One or more intermediate nodes are connected to each other to form a route between the source node and the destination node and it is used to forward the traffic from S to D. At the destination node, the traffic sent by the source node is received and the packet delivery ratio is measured at this node.

3.4.1 Simulation set up of the Network Model

The NS2.34 simulator helps to analyze the performance of the proposed protocol schemes. The initial topology is selected by creating an empty scenario and the network scale. In this simulation, 100 mobile nodes move in a network size of 1200 x 1200 m.sq region for the simulation period of 60 seconds. The data rates of the mobile nodes are 512 bytes with the default transmitting power of 0.005 watts. The nodes can move with different speed, hence random way point mobility is selected with the constant speed of 10 m/s and with the pause time of 100 seconds. This pause time is taken only after the data reaches the destination [109].

The Table 3.1 summarizes the parameter setting applied for the simulation study. MANET normally generates the monitoring data which has the same data size. Constant Bit Rate (CBR) traffic is used in this simulation as it represents the typical data that is retrieved from MANET. The traffic is sent from the source node to the destination node with different data rates. The use of different data packet sizes may affect the network performance. A smaller data packet size may always provide the best throughput rate than a bigger data packet size. The data packet sizes used in this simulation is 512 bytes. The default buffer queue length is 50 packets, therefore 5 pkts/sec is recommended as Buffer Queue Length.
Table 3.1: Simulation Settings and Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>No. of Nodes</td>
<td>100</td>
</tr>
<tr>
<td>Area Size</td>
<td>1200 X 1200</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>60 sec</td>
</tr>
<tr>
<td>Traffic Source</td>
<td>CBR</td>
</tr>
<tr>
<td>Packet Size</td>
<td>512 bytes</td>
</tr>
<tr>
<td>Mobility Model</td>
<td>Random Way Point</td>
</tr>
<tr>
<td>Packet rate</td>
<td>5 pkt/s</td>
</tr>
<tr>
<td>Protocols</td>
<td>AOMDV, DSR</td>
</tr>
</tbody>
</table>

3.4.2 Metrics for Performance Evaluation

The results of the simulation are evaluated based on the various metrics like Packet delivery ratio, Average throughput, Average end to end delay time, Routing overhead, Misbehavior detection efficiency and Network life time [35] [89] [92].

- **Packet Delivery Ratio (PDR)** is the ratio of the packets received to the packets sent successfully. This metric indicates both the loss ratio of the routing protocol and the effort required to receive the data. In an ideal scenario the ratio should be equal to 1. If the ratio falls significantly below an ideal ratio, then it could be an indication of some faults in the protocol design. However, if the ratio is higher than the ideal ratio, then it is an indication that the destination node receives a data packet more than once. It is not desirable because the reception of the duplicate packets consumes the network’s valuable resources. The relative number of duplicates received by the destination node is also important to take an appropriate action to reduce the redundancy [58] [87] [92].

\[ PDR = \frac{\text{Number of Packets Delivered}}{\text{Number of Packets Transmitted}} \times 100 \] (3.2)

- **Average Throughput** is the average rate of successful data delivery measured at the destination node (bytes) divided by the simulation duration time (sec). It measures the elapsed time between the time that the source node started sending a RREQ and the time the destination node receives the last data packet [58] [87] [92].
\[ \text{Average Throughput} = \frac{\text{Total Amount of Data Received at Destination}}{\text{Time (sec s)}} \times 100 \quad \ldots \ldots (3.3) \]

- **Routing Overhead (ROH)** is defined as the total number of routing control packets normalized by the total number of received data packets [92].

\[ \text{Routing Overhead} = \frac{\text{Total Number of Packets Normalised}}{\text{Total Number of Packets Received}} \quad \ldots \ldots (3.4) \]

- **Misbehavior Detection Efficiency Ratio (MDR)** is the ratio of the misbehaving nodes detected to the total number of nodes. The nodes can misbehave randomly any time in the network.

\[ \text{MDR} = \frac{\sum_{i=1}^{N} \text{Detected Nodes}}{\text{Total No of Nodes}} \times 100 \quad \ldots \ldots (3.5) \]

- **End-to-End Delay Time (EED)** is an average delay between the sending of packets by the source and its receipt by the receiver. This includes all possible delays caused during data acquisition, route discovery, queuing, processing at intermediate nodes, retransmission delays and propagation time. [58] [87] [92].

\[ \text{End to End Delay} = \frac{\sum_{i=1}^{n} \text{Emission Time at Source} - \text{Time to reach Destination}}{\text{Total Number of Packets received}} \quad \ldots \ldots (3.6) \]

- **Network Life Time (NLT)** is the time of the first node failure due to the exhaustion of battery power charge during the simulation with a particular routing protocol. The network life time decreases as the offered traffic load increases.

\[ \text{NLT} = \frac{\text{Exhaustion Time} - \text{Node Failure Time}}{\text{Time}} \quad \ldots \ldots (3.7) \]
Table 3.2 illustrates the analysis of evaluation of the PDR results by varying the number of black hole nodes.

Table 3.2: Evaluation of PDR by varying the number of black hole nodes

<table>
<thead>
<tr>
<th>Number of black hole nodes</th>
<th>PDR (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>DSR</td>
</tr>
<tr>
<td>20</td>
<td>75.7498</td>
</tr>
<tr>
<td>40</td>
<td>73.6424</td>
</tr>
<tr>
<td>60</td>
<td>71.2120</td>
</tr>
<tr>
<td>80</td>
<td>70.8115</td>
</tr>
<tr>
<td>100</td>
<td>69.8105</td>
</tr>
</tbody>
</table>

Table 3.3 illustrates the comparative analysis of the performance evaluation of SAOMDV protocol, based on the above mentioned parameters by varying the speed.

Table 3.3: Performance Evaluation of SAOMDV by varying Speed

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Speed variation at Nodes(m/s)</th>
<th>PDR (%)</th>
<th>ROH (pkts)</th>
<th>EED (msec)</th>
<th>MDR (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSR</td>
<td>20</td>
<td>75.7490</td>
<td>0.0038</td>
<td>29.2820</td>
<td>0.0000</td>
</tr>
<tr>
<td></td>
<td>40</td>
<td>73.6420</td>
<td>0.0051</td>
<td>46.8430</td>
<td>0.0000</td>
</tr>
<tr>
<td></td>
<td>60</td>
<td>71.2120</td>
<td>0.0063</td>
<td>50.0210</td>
<td>0.0000</td>
</tr>
<tr>
<td></td>
<td>80</td>
<td>70.8110</td>
<td>0.0077</td>
<td>70.0060</td>
<td>0.0000</td>
</tr>
<tr>
<td></td>
<td>100</td>
<td>69.8100</td>
<td>0.0087</td>
<td>95.9870</td>
<td>0.0000</td>
</tr>
<tr>
<td>SDSR</td>
<td>20</td>
<td>82.2560</td>
<td>0.0031</td>
<td>20.6050</td>
<td>53.3000</td>
</tr>
<tr>
<td></td>
<td>40</td>
<td>79.2870</td>
<td>0.0038</td>
<td>30.4590</td>
<td>49.9300</td>
</tr>
<tr>
<td></td>
<td>60</td>
<td>77.4940</td>
<td>0.0053</td>
<td>42.8360</td>
<td>42.6500</td>
</tr>
<tr>
<td></td>
<td>80</td>
<td>75.1350</td>
<td>0.0067</td>
<td>65.9050</td>
<td>37.7600</td>
</tr>
<tr>
<td></td>
<td>100</td>
<td>73.5650</td>
<td>0.0075</td>
<td>90.7030</td>
<td>11.5000</td>
</tr>
<tr>
<td>AOMDV</td>
<td>20</td>
<td>79.7490</td>
<td>0.0033</td>
<td>18.3500</td>
<td>0.0000</td>
</tr>
<tr>
<td></td>
<td>40</td>
<td>77.6420</td>
<td>0.0038</td>
<td>36.9070</td>
<td>0.0000</td>
</tr>
<tr>
<td></td>
<td>60</td>
<td>75.2120</td>
<td>0.0041</td>
<td>43.0990</td>
<td>0.0000</td>
</tr>
<tr>
<td></td>
<td>80</td>
<td>74.8110</td>
<td>0.0048</td>
<td>55.4710</td>
<td>0.0000</td>
</tr>
<tr>
<td></td>
<td>100</td>
<td>72.8100</td>
<td>0.0051</td>
<td>85.3430</td>
<td>0.0000</td>
</tr>
<tr>
<td>SAOMDV</td>
<td>20</td>
<td>85.6030</td>
<td>0.0010</td>
<td>14.4180</td>
<td>70.3000</td>
</tr>
<tr>
<td></td>
<td>40</td>
<td>82.6890</td>
<td>0.0016</td>
<td>23.3330</td>
<td>60.4400</td>
</tr>
<tr>
<td></td>
<td>60</td>
<td>81.3190</td>
<td>0.0020</td>
<td>39.0760</td>
<td>50.8600</td>
</tr>
<tr>
<td></td>
<td>80</td>
<td>80.8880</td>
<td>0.0026</td>
<td>52.3880</td>
<td>40.0900</td>
</tr>
<tr>
<td></td>
<td>100</td>
<td>79.8090</td>
<td>0.0031</td>
<td>58.8010</td>
<td>15.6600</td>
</tr>
</tbody>
</table>
Table 3.4 illustrates the performance evaluation results of SAOMDV protocol by varying the node mobility.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>No of Nodes</th>
<th>PDR (%)</th>
<th>ROH (pkts)</th>
<th>EED (msec)</th>
<th>Throughput (kb/s)</th>
<th>NLT (secs)</th>
<th>MDR (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSR</td>
<td>10</td>
<td>65.7400</td>
<td>0.0067</td>
<td>29.4100</td>
<td>1893.7400</td>
<td>345.2000</td>
<td>0.0000</td>
</tr>
<tr>
<td></td>
<td>30</td>
<td>63.6400</td>
<td>0.0070</td>
<td>46.9710</td>
<td>1841.0600</td>
<td>233.7000</td>
<td>0.0000</td>
</tr>
<tr>
<td></td>
<td>50</td>
<td>61.2100</td>
<td>0.0077</td>
<td>60.1490</td>
<td>1780.3000</td>
<td>127.2000</td>
<td>0.0000</td>
</tr>
<tr>
<td></td>
<td>70</td>
<td>60.8100</td>
<td>0.0081</td>
<td>70.1340</td>
<td>1770.2900</td>
<td>97.3000</td>
<td>0.0000</td>
</tr>
<tr>
<td></td>
<td>90</td>
<td>59.7800</td>
<td>0.0086</td>
<td>91.1150</td>
<td>1745.2600</td>
<td>70.2000</td>
<td>0.0000</td>
</tr>
<tr>
<td>SDSR</td>
<td>10</td>
<td>87.2560</td>
<td>0.0050</td>
<td>21.7330</td>
<td>1993.7400</td>
<td>352.8000</td>
<td>60.3000</td>
</tr>
<tr>
<td></td>
<td>30</td>
<td>84.2800</td>
<td>0.0057</td>
<td>40.5870</td>
<td>1941.0600</td>
<td>241.7000</td>
<td>48.9300</td>
</tr>
<tr>
<td></td>
<td>50</td>
<td>81.1300</td>
<td>0.0062</td>
<td>52.9640</td>
<td>1880.3000</td>
<td>132.8000</td>
<td>40.6500</td>
</tr>
<tr>
<td></td>
<td>70</td>
<td>79.4900</td>
<td>0.0076</td>
<td>66.0330</td>
<td>1870.2900</td>
<td>107.4000</td>
<td>37.5600</td>
</tr>
<tr>
<td></td>
<td>90</td>
<td>75.5600</td>
<td>0.0084</td>
<td>87.8280</td>
<td>1820.2600</td>
<td>107.4000</td>
<td>10.5000</td>
</tr>
<tr>
<td>AOMDV</td>
<td>10</td>
<td>72.7400</td>
<td>0.0040</td>
<td>20.4780</td>
<td>2131.4100</td>
<td>450.1000</td>
<td>0.0000</td>
</tr>
<tr>
<td></td>
<td>30</td>
<td>70.6400</td>
<td>0.0045</td>
<td>37.0350</td>
<td>2057.1800</td>
<td>339.3000</td>
<td>0.0000</td>
</tr>
<tr>
<td></td>
<td>50</td>
<td>68.2100</td>
<td>0.0048</td>
<td>43.2270</td>
<td>2037.3700</td>
<td>229.5000</td>
<td>0.0000</td>
</tr>
<tr>
<td></td>
<td>70</td>
<td>67.8100</td>
<td>0.0055</td>
<td>55.5990</td>
<td>1978.3900</td>
<td>120.1000</td>
<td>0.0000</td>
</tr>
<tr>
<td></td>
<td>90</td>
<td>65.8000</td>
<td>0.0058</td>
<td>79.4710</td>
<td>1899.1300</td>
<td>82.4000</td>
<td>0.0000</td>
</tr>
<tr>
<td>SAOMDV</td>
<td>10</td>
<td>88.9000</td>
<td>0.0020</td>
<td>11.5460</td>
<td>2237.5900</td>
<td>641.5000</td>
<td>70.1000</td>
</tr>
<tr>
<td></td>
<td>30</td>
<td>86.3000</td>
<td>0.0028</td>
<td>19.4610</td>
<td>2157.5000</td>
<td>572.3000</td>
<td>60.1400</td>
</tr>
<tr>
<td></td>
<td>50</td>
<td>85.4000</td>
<td>0.0033</td>
<td>25.2040</td>
<td>2135.0000</td>
<td>483.5000</td>
<td>50.2600</td>
</tr>
<tr>
<td></td>
<td>70</td>
<td>84.0090</td>
<td>0.0045</td>
<td>36.5160</td>
<td>2000.2300</td>
<td>323.6000</td>
<td>39.0900</td>
</tr>
<tr>
<td></td>
<td>90</td>
<td>83.1000</td>
<td>0.0050</td>
<td>48.9280</td>
<td>1977.5000</td>
<td>201.8000</td>
<td>12.6600</td>
</tr>
</tbody>
</table>

3.4.3 Packet Delivery Ratio of SAOMDV

The Packet Delivery Ratio is a performance metric which provides an idea about how efficiently the protocol performs in delivering the packet at the destination. The packet delivery ratio decreases when the number of black hole nodes increases. The increase in the speed of transmission decreases the packet delivery ratio and also when the mobility of the nodes increases the packet delivery ratio is decreased. Here in this simulation, the proposed protocol scheme SAOMDV is simulated and performance is evaluated by comparing the simulation results with Security Certified DSR (SDSR), AOMDV and DSR protocols.

The Figure 3.1 shows the comparative analysis of the packet delivery ratio by varying the number of black hole nodes. SAOMDV protocol provides a very high packet
delivery ratio of 96.9010 % due to the fact that the protocol is highly authenticated and data packets are transmitted only through the secured and reliable route. When the number of the black hole node increases, it results in more rerouting of packets. This slowly decreases the packet delivery ratio to 91.1491% when the black hole node increases to 100 nodes.

Figure 3.1: SAOMDV: Packet Delivery Ratio Vs No of Black Hole Nodes

Figure 3.2: SAOMDV: Packet Delivery Ratio Vs Speed
The comparative analysis of the packet delivery ratio by varying the transmission speed of the nodes is shown in the Figure 3.2. When compared with SDSR, AOMDV and DSR protocol, SAOMDV protocol provides very high packet delivery ratio of 85.6030 % due to the fact that the protocol can route the packets through the alternate route and guarantees the delivery of the packets. The increase in the speed of transmission makes most of the packets to get timed out. The timed out packets are dropped thereby decreasing the packet delivery ratio to 79.8090%.

![Figure 3.2: SAOMDV: Packet Delivery Ratio Vs Node Speed](image)

The Figure 3.3 illustrates the evaluation of packet delivery ratio by varying the mobility of the nodes. SAOMDV provides the highest packet delivery ratio of 88.9% when compared with SDSR, AOMDV and DSR protocols. When the mobility of the nodes increases the position of the nodes will be changing more frequently. The source nodes will be using the invalid outdated route for routing the packets. This cause the packets to get exceed the maximum level of time-to-live (TTL). The packets exceeding the maximum TTL levels are dropped. This results in the decrease of packet delivery ratio to 83.1%.

![Figure 3.3: SAOMDV: Packet Delivery Ratio Vs Node Mobility](image)
3.4.4 End to End Delay Time of SAOMDV

An End to End delay time is the average time taken by the packet to reach the destination. Generally End to End delay time will increase when there is an increase in the speed of transmission, mobility of the nodes and increase in the number of black hole node participation.

![End to End Delay](image)

Figure 3.4: SAOMDV: End to End Delay Time Vs Speed

The Figure 3.4 illustrates the evaluation of end to end delay time of SAOMDV and SDSR on comparing with AOMDV and DSR. SAOMDV has shown a remarkable low end to end delay time of 14.41 to 58.801 msec by varying the speed of transmission. This is because SAOMDV can immediately use the routing information that it receives from the intermediate nodes and it can update with the latest route information. SDSR also achieved low end to end delay time of 20.605 msec at 20 m/s. However when the speed increases to 100 m/s, the end to end delay time increases dramatically to 90.703 msec.

The evaluation of end to end delay time by varying the node mobility is shown in Figure 3.5. The SAOMDV protocol has achieved the very low delay time of 11.546 msec with the mobility of 10 nodes. When the mobility of the nodes increases to 90 nodes it results in the higher delay time of 48.928 msec. A remarkable increase is observed in case
of SDSR and DSR protocols. The reason is that at high mobility of the nodes, the nodes move away from the connectivity range and cause the currently used link to fail resulting in destination path loss. Hence the new route discovery process introduces a momentous amount of delay that severely affects the performance of DSR protocol.

![Figure 3.5: SAOMDV: End to End Delay Time Vs Node Mobility](image)

3.4.5 Misbehavior Detection Efficiency of SAOMDV

This performance metric enables to evaluate how efficiently the protocol is detecting the misbehaving nodes. The proposed solution is evaluated to analyse the misbehavior detection efficiency at different scenarios by varying the speed and mobility of the nodes.
The Figure 3.6 illustrates the Misbehavior detection efficiency of the SAOMDV and SDSR protocols. SAOMDV has achieved the comparatively higher detection efficiency of 70.3% at the speed of 20 m/s. The ratio drops down with the increase in the speed. The ratio decreases drastically to 15.66% at 100 m/s.
The Figure 3.7 illustrates the impact of the misbehavior detection efficiency of SAOMDV and SDSR by varying the mobility of the nodes. It is observed that SAOMDV has shown higher detection efficiency of 70.1% at the mobility of 10 nodes. When the mobility of the nodes increases to 90 nodes the detection efficiency ratio decreases radically to 12.66%. The mobility of the nodes makes the nodes to move in and out of the communication range frequently. This makes it difficult to identify the malicious nodes. The SDSR protocol has also achieved the good detection efficiency ratio of 60.3% at low mobility rate of 10 nodes.

3.4.6 Routing Over Head of SAOMDV

Routing over head is the average number of routing packets required to deliver a single data packet. It gives an idea about the bandwidth consumed to deliver the data packets. Performance evaluation of the proposed protocol scheme based on routing overhead by varying the speed of the nodes is illustrated in the Figure 3.8. SAOMDV has achieved the low routing overhead of 0.0010 (pkts) at 20 m/s. In SDSR protocol the route cache property is useless when the mobile nodes are moving at higher speeds and links are lost more frequently.

![Figure 3.8: SAOMDV: Routing Over Head Vs Speed](image)
Consequently, intermediate mobile nodes frequently engaging the new route discovery, causes the dramatic increase in the routing overhead to 0.0031\((pkts)\). In SAOMDV the new route discovery process is initiated only when all the alternate routes to the destination node is trapped by the black hole node.

Figure 3.9 illustrates the evaluation of routing overhead of the proposed solutions by varying the mobility of the nodes. It is observed that the routing over head of the SAOMDV protocol is very low with 0.0050\((pkts)\) at the mobility rate of 90 nodes. SDSR experiences high routing overhead of 0.0084\((pkts)\) with the increase in the node mobility of 90 nodes. This is because, the mobility of the nodes increases the route failure. To find the fresh new routes the source nodes have to generate more number of RREQs resulting in the increased routing overhead.

\[\text{Figure 3.9: SAOMDV: Routing Over Head Vs Node Mobility}\]

**3.4.7 Network Lifetime of SAOMDV**

The network lifetime metric enables to estimate the life time of the link after the failure due to the exhaustion of battery power. Figure 3.10 illustrates the performance of the SAOMDV by varying the speed and mobility of the nodes.
The SAOMDV protocol scheme resulted with the high network life time of 641.5 sec at the mobility rate of 10 nodes. The network life time decreases to 201.8 sec when the speed and mobility of the nodes increases. SDSR has comparatively low lifetime, because of frequent link failure. The rapid link failure exhaust the life time of the node. In SDSR, at node mobility of 10 nodes, the battery power consumed by the node is less and the life time of the node is 352.8 sec. The hop count plays a significant role in deciding the amount of energy consumed by the node. At low node mobility, the amount of energy spent in route discoveries becomes significant and neutralizes the effect of the reduced hop count. In large networks, SDSR paths are more unbalanced compared to that at of the small networks as hops with the physical link distance that are close to the transmission range are bound to break soon.

### 3.4.8 Average Throughput of SAOMDV

The Figure 3.11 illustrates the average throughput of SAOMDV by varying the mobility of the nodes from 10 to 90 nodes.
The throughput range of DSR is 1893.74-1745.26 (kb/s). SDSR resulted with the throughput range of 1993.74-1820.26 (kb/s). AOMDV has the average throughput in the range of 2131.41-1899.13 (kb/s). It is observed that SAOMDV resulted with the higher throughput of 2237.59 (kb/s) at the low mobility of the nodes than AOMDV, SDSR and DSR. SAOMDV with the throughput range of 2237.59-1977.50 (kb/s) is able to select multiple paths to achieve more load balancing in high node mobility to delivery packets.

When the mobility of the nodes increases the throughput decreases because most of the packet will get dropped. In case of SAOMDV and AOMDV protocols, most of the missing packets are retransmitted again over multiple reliable routes from source or intermediate node to destination.

3.5 Chapter Summary

The most common security threat experienced by the MANET is the black hole attack. The black hole node severely affects the performance of the network layer and results in denial of service. DSR and AOMDV routing protocols experiences rigorous undesirable impact on the performance due to the black hole attack. To avoid the adverse
effect of the black hole nodes on DSR and AOMDV protocols, SAOMDV and SDSR protocol schemes are proposed with a feasible methodology using digital security certificate.

The SAOMDV protocol scheme is used to find the secured routes and to detect the black hole nodes in the MANET. The Digital security certificates are proposed for authenticating the nodes in the selected route. Data transmission process is monitored by the neighboring nodes. Certificate is revoked when the nodes fail during the authentication. Alternate route is selected, in case if any of the black hole node is detected. The results of the proposed schemes are compared with normal AOMDV and DSR protocols.

The SAOMDV protocol scheme results in good performance when compared with SDSR, AOMDV and DSR protocol. The SDSR routing protocol suffers from increased control over head because it is necessary to add the routing information in the packet header of each packet to be transmitted. The end to end delay time is high because once if the route is failed, it has to search its routing cache to find another route to the destination. It has to check whether that route includes the detected malicious node. The DSR leads to higher routing overhead when compared with AOMDV protocol.

The simulation results prove that SAOMDV routing protocol scheme provides efficient packet delivery ratio. This protocol results in low routing over head and delay time because the link disjoint routes are already listed in the routing table. SAOMDV will detect the black hole node during the route discovery process and ensures that any kind of black hole node cannot be a participating node in the route to transmit the data packets from the source to destination. During the data transmission any legitimate node can tend to behave maliciously. However this scheme does not prevent the black hole node that exhibit malicious behavior at instant of time.