CHAPTER 5

EDSR: THE PROPOSED SOLUTION FOR BLACK HOLE ATTACK

This Chapter will present and discuss the proposed protocol to detect one of the most severe attacks in ad hoc networks. The previous Chapter showed that most of the previously proposed techniques to detect black hole attacks require either promiscuous monitoring of nodes which results in energy loss in individual nodes or introduce more routing overhead in the network or incurs high computational complexity at individual nodes which results in performance degradation of the network.

In this Chapter, we propose an approach called Enhanced Dynamic Source Routing (EDSR) protocol, which is a variation of normal DSR routing protocol to detect the black hole attack launched by a malicious node and to eliminate it from the network. In this approach, the source node selects the secure route based on the negative acknowledgements coming from the destination node. Since black hole attack can be easily launched on reactive routing protocols like AODV and DSR, in this dissertation, DSR routing protocol is selected to study this attack. DSR is one of the most popular reactive routing protocols and has been extensively discussed in research papers. Also DSR employs source routing and selects loop free routes for data transmission. Since AODV discovers route on hop–by-hop basis, finding loop free routes is not guaranteed. Also, in AODV, the increase in network
size has an impact on end-to-end delay of the network (Perkins et al 2003). The detailed comparison of DSR and AODV is given in Appendix 1. Therefore, this study deploys and evaluates the proposed method on DSR-based MANETs.

5.1 BLACK HOLE ATTACK IN DSR

In DSR routing protocol, if a source node needs a path to the destination, it broadcasts RREQ packet to the network. Any intermediate node receiving the RREQ can send a RREP if having path to reach the destination. The source node will select the shortest path among the advertised routes and send data packets to destination node through that path.

The malicious node exploits this route discovery process of DSR and launches the black hole attack. In a black hole attack, the malicious node, referred to as black hole node replies to every routing request it receives, saying that it has a route to the given destination. So, unsuspecting nodes start sending data to the destination through the black hole. This way a black hole diverts most of the traffic in the network to itself, and later drops it.

![Figure 5.1 Black hole attack in DSR](image-url)
In Figure 5.1 node 2 is a malicious node and nodes 1 and 4 are source and destination respectively. Initially node 1 broadcasts a RREQ packet to find the route to reach node 4. The RREQ packet is received by both node 2 and node 6. Node 6 forwards the RREQ packet to its neighbor because it may not have the route. Node 2 being the black hole node sends immediately a RREP packet to the source node claiming that it has the route to reach the destination even though it has not. The source i.e., node 1 receives the first RREP packet from node 2 and assumes it is having the shortest route to reach node 4 and starts sending the data packet through node 2. The black hole node then simply drops all the data packets without forwarding it thus launching a DOS attack on the destination.

5.2 ENHANCED DYNAMIC SOURCE ROUTING PROTOCOL

The proposed solution called Enhanced DSR (EDSR) is an enhancement of the basic DSR routing protocol, which will be able to detect the presence of black hole nodes in the network. Our solution assumes that all the nodes are authenticated and can participate in communication. According to DSR protocol, the source node has to broadcast the RREQ packet to find a path to reach the requested destination. The requested destination, or any intermediate node having the path, can send back the reply to the source node.

5.2.1 Detection of Black Hole Attack

In our proposed work, the destination node, when it receives the RREQ packet can learn the information that the source node is having some data to send to it because it is initiating the route discovery process. This information can be obtained by the destination node because the RREQ packet contains both the source node id and destination node id for which the source node requesting the route. The destination node then sends back a RREP packet to the source node. Then it creates an entry into its neighbor monitor table that records the source id requesting the route and the path
taken by the RREP packet it sent for the corresponding RREQ. After a periodic interval, the destination node checks whether it has received data packets from the corresponding source. If so, then it deletes the recorded information from the table. Otherwise, it generates a Negative Acknowledgement packet (NACK) to the source informing that it has not received any data packet from that source. The NACK packet will be sent using the path information of the corresponding source node stored in the table. Once the source node receives the NACK, it detects that the intermediate node which send the route reply packet advertising a shortest route to the destination, is a malicious node launching black hole attack. Hence the source node starts transmitting the data packets in the new path traversed by NACK packet. After transmitting NACK packets and if the destination node still does not receive any data packets and the time interval expires again, it may be due to the loss of NACK packet while transmission. This is because the path taken by NACK packet is no longer available due to high mobility in the network. In that case, the destination node has to broadcast the NACK packet to the source node. Once the source node receives the NACK, it starts transmitting data packets in that path.

5.2.2 Elimination of Black Hole Node

When the source node receives the NACK packet from the destination, it detects the presence of black hole attack and sends the remaining data packets to the destination by reversing the path taken by the NACK packet and moves the intermediate node that sends the RREP into the malicious node list. Then the source node removes all the routes involving the black hole node from its route cache. It also informs the presence of black hole node and its identity to all its surrounding nodes which then propagate this information to their neighbors. All the nodes then delete the routes involving the black hole node from their route cache and also ignore any
routing information coming from it. Gradually the black hole node is isolated and eliminated from the network.

![Figure 5.2 Propagation of RREQ and RREP](image)

**Figure 5.2 Propagation of RREQ and RREP**

**Table 5.1 Neighbor monitor table of destination node 8**

<table>
<thead>
<tr>
<th>Source node Id</th>
<th>Route Reply Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>8-7-6-1</td>
</tr>
</tbody>
</table>

We illustrate the working principle of EDSR with an example. In Figure 5.2, node 1 is the source and node 8 is the destination node. BN is the black hole node. When the source node 1 has some data to send to the destination node 8, it initiates the route discovery process. Node 1 broadcasts the RREQ packet. When the black hole node BN receives the RREQ packet, it drops the RREQ packet without forwarding it. The node BN then claims that it has route to the destination node 8 and sends RREP packet back to the source node. The destination node 8 also receives the RREQ packet and sends a RREP packet back to the source node 1 by reversing the path of the RREQ packet i.e., 8-7-6-1. It also records the source id and the path of the RREP.
packet in the neighbor monitor table as shown in Table 5.1. The source node 1 receives the RREP packet sent by the BN node first, and starts sending the data packets to the BN node. The black hole node BN drops all the data packets without sending it to the destination.

The destination node 8 waits for a periodic time interval and checks whether it receives data packets from the source node. If not, it sends a Negative Acknowledgement packet (NACK) to the source node using the route information stored in the table. In Figure 5.3, node 8 sends a NACK packet back to source node 1. When node 1 receives the NACK packet, it understands that no data packets have reached the intended destination and have been grabbed by the intermediate node. So it moves the node BN to the malicious node list, and sends the remaining data packets using the path 1-6-7-8. The source node 1 then deletes all the routes involving the black hole node BN from its route cache. It also ignores all the control packets coming from that node in future. Figure 5.4 shows the actions of a node after receiving RREQ packet. Figure 5.5 shows the action of destination node after sending RREP and Figure 5.6 shows the actions of the source after receiving the NACK packet. Figure 5.7, 5.8 and 5.9 shows the flowcharts depicting the actions mentioned in figure 5.4, 5.5 and 5.6.

![Figure 5.3 Propagation of NACK packets from node 8 to node 1](image-url)
// When a node receives RREQ
If destination node
    Send a RREP back to the source node.
    Copy the source node id and the route to reach it as seen in the RREQ
    packet into the neighbor monitor table.
else (any intermediate node)
    Check whether route to the destination is available in its route cache.
    If available
        Send a RREP back to the source node
    else
        Forward the RREQ packet

**Figure 5.4** Action of a node after receiving RREQ

// Action of destination node after sending RREP
Check whether data packets are received from the source node whose node id
maintained in the neighbor monitor table.
If data packets received within a period of interval
    No action taken. The entry corresponding to the source node id is deleted
    from the neighbor monitor table.
else if data packets not received
    Send a NACK packet back to the source node using the route recorded in
    the table for that source node.

**Figure 5.5** Action of destination after sending RREP

// Action of source node after receiving NACK
If the source node receives NACK packet
    Send the data packets to the destination through the path taken by NACK
    packet.
    Move the intermediate node that sent the RREP into malicious node list.
    Delete all the routes involving that malicious node id from the route cache.
    Send the malicious node id to its neighbors.
Else (not received any NACK)
    Transmit all the data packets through the same path advertised by the
    intermediate node.

**Figure 5.6** Action of source node after receiving NACK
Figure 5.7 Flowchart for the action of a node after receiving RREQ
Figure 5.8 Flowchart for the action of destination node
Figure 5.9  Flowchart for the action of source node after receiving NACK

Start

If NACK packet received

no

yes

Send the remaining data packets through the path taken by NACK

Transmit all data packets through the same path advertised by intermediate node

Move the intermediate node that sends the RREP into malicious node list

Delete all routes involving malicious node from the route cache

End
5.2.3 Limitation of EDSR

EDSR suffers performance degradation and fails to detect black hole attack only when the source node is entirely surrounded by black hole nodes and also the destination node is not able to receive RREQ packet through any path. We further validated this by carrying out an experiment with static ad hoc nodes using grid topology. In that topology we placed 3 black hole nodes in one hop distance of source node which entirely blocks the source node from the rest of the network. So when the source node sends a RREQ packet to some destination, only the black hole nodes receive it and they drop the packet without forwarding.

5.3 SIMULATION RESULTS

5.3.1 Metrics

The network simulation is performed using Global Mobile Simulator (GloMoSim) (Xian et al 1998), to analyze the performance of the network by varying node mobility speed, node pause time and number of malicious nodes. Global Mobile Information System Simulator (GloMoSiM) is a simulation environment used for large scale wireless networks. GloMoSiM is capable of simulating a network that contains thousands of nodes and heterogeneous communication links. GloMoSiM has a scalable simulation library that is based on the Parsec simulation environment. It is developed as a set of library modules, each of which simulates a specific wireless communication protocol in the protocol stack. Ns-2 is another widely used open source network simulator. But the reason for choosing GlomoSim over Ns-2 is the time taken for computation. The computation time of
GLoMoSIM is quite low compared to NS-2. In terms of computation time and scalability, GLoMoSIM appears to be more efficient than Ns-2. GloMoSiM are capable of carrying out large scale network simulations with less computation time than NS-2 (Rehman 2012).

In an area of 1000 m by 1000 m, 50 nodes were randomly distributed with 10 malicious nodes, performing black hole attack. Fifteen pairs were randomly chosen for data communication, each sending 512 bytes UDP-CBR (Constant Bit Rate) per second. All normal nodes were moved in a Random-way point model, with random speeds ranging between 0 and 20 m/s. The simulation parameters are illustrated in Table 5.2, and all experimental data in this section refer to an average value, which result from running 10 experiments. To eliminate the randomness in the result, for each metric, simulation is done for ten different seed values with different random movement of nodes and the average value is taken for the result. Also our approach is compared with two existing approaches Deng’s Protocol (Deng and Agarwal 2002) and ABDSR (Bhalaji and Shanmugam 2009). The former approach is selected because similar to our approach, it is also an ACK based detection technique. The approach proposed by Bhalaji and Shanmugam (2009) has been selected because it is a recent technique and similar to our approach it doesn’t involve any cryptographic methods for detecting the attack. The simulation parameters are configured to set up the congestion free network. Then DSR protocol is tested in that network setup and the performance values of DSR protocol for various parameters are taken as the reference values for testing EDSR protocol.

The metrics used to evaluate the performance are given below:
• Packet Delivery Ratio: The ratio between the number of packets originated by the CBR sources of source nodes and the number of packets received by the CBR sinks at the destination nodes.

• Average End to End Delay: This is the average delay between the sending and receiving of the data packets by the respective source and the destination.

• Routing Overhead: This is the ratio of number of control packets generated to the data packet received.

• Dropped Packets: It is the number of data packets dropped by the black hole nodes without any route error messages being sent.

To simulate the EDSR protocol, some assumptions are made as follows:

• Packets are dropped only by malicious nodes. Therefore, no congestion is considered here.

• There is no error in the wireless channel.

5.3.2 Simulation Parameters

The simulation parameters are illustrated in Table 5.2.
Table 5.2 Simulation parameters for EDSR

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Nodes</td>
<td>50</td>
</tr>
<tr>
<td>Simulation Time</td>
<td>600S</td>
</tr>
<tr>
<td>Mobility</td>
<td>Random Way Point Model</td>
</tr>
<tr>
<td>Load</td>
<td>1200 packets, Data Payload 512 Bytes. Interdeparture Time is 0.5 S</td>
</tr>
<tr>
<td>Terrain Dimension</td>
<td>1000 m by 1000 m</td>
</tr>
<tr>
<td>Number of Transactions</td>
<td>15</td>
</tr>
<tr>
<td>Mobility Speed</td>
<td>10m/s to 50m/s</td>
</tr>
<tr>
<td>No of Black hole Nodes</td>
<td>10</td>
</tr>
</tbody>
</table>

5.3.3 Performance Comparison of EDSR and DSR

5.3.3.1 Packet delivery ratio

Figure 5.10 shows the packet delivery ratio in the presence of malicious node. Here 10 black hole nodes are randomly selected.

![Packet Delivery Ratio Graph](image)

Figure 5.10 Packet delivery ratios
From the above simulation results, we observe that the proposed solution provides a better packet delivery ratio under black hole attack at varying node speeds. At lower speeds the packet delivery ratio of standard DSR is very low because the node mobility is very low. The black hole node that includes itself in a transaction will not move quickly from its current location and drops all the packets without forwarding. But in EDSR, once a black hole attack is detected, then a secure alternate route is determined and all the packets are transmitted using the alternate route and so the packet delivery ratio is very high. However at higher speed, even though the performance of EDSR is much better than standard DSR, the packet delivery ratio drops. This is because when node mobility increases, more link break downs occurs and EDSR has to find secure route to transmit data whenever link break occurs.

5.3.3.2 Routing overhead

Figure 5.11 shows the routing overhead under the presence of black hole nodes. By comparing the routing overhead in standard DSR without having black hole attack and EDSR, our scheme has more control packets ratio. The higher routing overhead in EDSR is due to the transmission of NACK packets. But the routing overhead of DSR under black hole attack and EDSR are more or less similar.
5.3.3.3 Dropped packets

Figure 5.12 shows the number of packets dropped by black hole nodes in DSR and in Enhanced DSR. In EDSR, the destination node, after receiving the RREQ packet waits for only a periodic interval of time for the arrival of data packets. Within that period if it does not receive any data packets it informs the source node immediately through NACK packets. So the source node will start sending the remaining data packets in the safe alternate route. Because of this, irrespective of varying node speeds, the number of data packets lost is very less when compared to the standard DSR.
5.3.4 Performance Comparison of EDSR and Deng’s Protocol

5.3.4.1 Packet delivery ratio

![Node mobility Vs Packet Delivery Ratio](image)

Figure 5.13 Packet delivery ratios of EDSR and DENG scheme

As shown in Figure 5.13, the packet delivery ratio of EDSR under black hole attack is more than Deng’s protocol. For ex, when the node mobility is low, our protocol produces higher throughput when compared to Deng’s protocol since low mobility speed causes lesser link breaks resulting in lesser secure route discovery.

5.3.4.2 End to end delay

The end to end delay for sending data packets between the source and the destination is better in our approach when compared to the Deng’s approach as show in Figure 5.14. In Deng’s protocol, the source node must wait for FREP messages from each intermediate node before selecting the
route, so it takes a longer time to find a secure route before transmitting the data packets.

![End to End Delay in EDSR and DENG scheme](image)

**Figure 5.14** End to end delay in EDSR and DENG scheme

### 5.3.4.3 Routing overhead

The number of control packets overhead in EDSR is less when compared to the Deng’s technique as in Figure 5.15. This is because, in Deng’s scheme, for every route reply coming from the intermediate nodes, the source node has to send a FREQ packet to the next node of the intermediate nodes enquiring the correctness of the route. Also for every FREQ, a corresponding FREP packet has to be sent by the next hop nodes of the intermediate nodes. This results in more routing overhead to discover a secure route in Deng’s scheme.
5.3.5  Performance Comparison of DSR, EDSR and ABDSR under Black Hole Attack

5.3.5.1  Throughput

Figure 5.16 shows the packet delivery ratio in the presence of malicious node. Here 10 black hole nodes are randomly selected. The throughput achieved by DSR was approximately 21%, while the throughput achieved in EDSR under the same scenario was approximately 37%, increased by 16% i.e., EDSR improved the throughput achieved by DSR under attack. Similarly, the throughput achieved by ABDSR was approximately 27% which is 10% less than our scheme. At lower speeds the packet delivery ratio of standard DSR is very low because the node mobility is very low, so the black hole node that includes itself in a transaction will not move quickly from its current location and drops all the packets without forwarding. But in EDSR, once a black hole attack is detected, then a secure alternate route is determined and all the packets are transmitted using the alternate route and so the packet delivery ratio is very high. However at
higher speed, even though the performance of EDSR is much better than standard DSR, the packet delivery ratio drops due to link breaks.

Figure 5.16 Throughput

5.3.5.2 Routing overhead

Figure 5.17 shows the routing overhead due to additional control packets under the presence of black hole nodes. The higher routing overhead in our scheme EDSR is due to the transmission of additional control packet called NACK. The control packet overhead ratio of EDSR was approximately 94%, increased by 6%, when compared to the overhead ratio of DSR which was approximately 88%. However the control packet overhead ratio of ABDSR was approximately 107%, increased by 14% when compared to our scheme.
Figure 5.17  Routing overhead

5.3.5.3 Packet loss rate

Figure 5.18 shows the number of packets dropped by black hole nodes in DSR, EDSR and ABDSR. In EDSR, the destination node, after receiving the RREQ packet waits for only a periodic interval of time for the arrival of data packets. Within that period if it does not receive any data packets it informs the source node immediately through NACK packets. So the source node will start sending the remaining data packets in the safe alternate route. Because of this, irrespective of varying node speeds, the number of data packets lost is very less when compared to the standard DSR. The packet loss rate of DSR under attack was approximately 33%, while the packet loss rate of EDSR was approximately 2%, reduced by 31%. Similarly the packet loss rate of ABDSR was approximately 6%, which was increased by 4% when compared to our scheme EDSR.
We also tested the scalability of our algorithm by varying the number of nodes. The comparison results of EDSR and ABDSR with DSR by varying the number of nodes are shown in Figure 5.19. The metrics used are shown in Table 5.3. Here 10 black hole nodes are placed in appropriate positions such that each black hole node intrudes one data transmission path. During mobility, the black hole nodes choose and reach a destination point which is in the path of another data transmission. The experiment result shows the throughput achieved by DSR, EDSR and ABDSR in different network sizes. The packet delivery ratio achieved by DSR under attack was approximately 28%. It is 17% lesser than the packet delivery ratio of our scheme EDSR which was approximately 45%. This is because in DSR, the source nodes are not aware of the loss of the data packets due to the lack of acknowledgement scheme. Moreover the throughput achieved by ABDSR was approximately 36%, i.e., 9% lesser, when compared to EDSR.
Table 5.3 Simulation parameters for testing scalability

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>No of Nodes</td>
<td>25 - 200</td>
</tr>
<tr>
<td>Mobility Speed</td>
<td>10 m/s</td>
</tr>
<tr>
<td>No of Black hole Nodes</td>
<td>10</td>
</tr>
<tr>
<td>Connections</td>
<td>20 Pairs (40 nodes)</td>
</tr>
<tr>
<td>Traffic Type</td>
<td>UDP – CBR</td>
</tr>
<tr>
<td>Pause Time</td>
<td>60s</td>
</tr>
</tbody>
</table>

Figure 5.19 Scalability

5.4 SUMMARY

In this work, we propose a routing protocol called Enhanced Dynamic Source Routing Protocol (EDSR), which is based on DSR, to defend against black hole attacks in MANETs. The algorithm proposes a light weight solution methodology which is a simple acknowledgement scheme to
detect black hole nodes. So it can be incorporated with any existing on-demand routing protocols. With the help of NACK packets from the destination node, the source node finds the alternate secure route for data transmission. The experiment results show that the percentage of packets received through our proposed work is better than DSR in presence of multiple black hole nodes. EDSR suffers performance degradation and fails to detect black hole attack only when the source node is entirely surrounded by black hole nodes and also the destination node is not able to receive RREQ packet through any path. The simulation is done using GloMoSim and our scheme is found to achieve routing security with 16% increase in packet delivery ratio than standard DSR and also achieves 31% reduction in packet loss rate than DSR. Compared to other related works, the proposed protocol has more merits; the most important merit is that it achieves degradation in packet loss rate without any computational complexity or promiscuous listening. Moreover, cooperative black hole attack cannot be launched, because our technique is an ACK based detection technique and doesn’t employ neighbor node monitoring.