Chapter – 5

SIMULATION RESULTS

CHAPTER -5

Chapter - 1. SIMULATION RESULTS

CHAPTER - 5

SIMULATION RESULTS

5.1. INTRODUCTION

After having explained the way to implement blackhole attack, the simulations of the same is presented here with in this section in order to demonstrate as well as evaluate its effects in MANETs. Afterwards the new test beds of proposed secure routing protocols are tested with different MANET scenarios in the presence of blackhole nodes and their performance is evaluated and compared with the normal AODV protocol.

5.2. Testing the Black Hole AODV

The implementation of the blackhole is initially tested to know whether it is properly working or not. The NAM (Network Animator) tool of NS2 is used to make sure the proper working of the blackhole implementation. In the very initial scenario none of the MANET nodes are assigned with blackhole features. But in the second scenario, one blackhole node is added to the simulation. After that the simulation results of both the scenarios are compared using NAM. To obtain precise results from the simulations, a transport protocol called User Data Gram (UDP) is used. The source keeps on outputting CBR packets, even if the blackhole node drops them. Thus, during the simulation one can monitor the connection flow between sending and receiving nodes.

A miniature size network with 7 number nodes is created and there by an UDP connection between Node 2 and Node 5 is generated,

and a CBR traffic that produces constant packets at a constant rate throughout the UDP connection is attached. The data rate is set to 1 Mbyte and CBR packet size is selected to be 512 bytes. The duration of the simulation is 100 seconds and the CBR connections are set to start on time that equals to 1 second and continue until the completion of the simulation, in a 700 x 700 meter space. The suitable positions of the nodes are set manually to describe the data flow and the movement is introduced only to node one to illustrate the data flow changes within the network.

5.2.1. Assessment of the Simulation

If we look at the animation of the simulation of the first scenario where there is no blackhole node, one can easily notice that the connection between Node 2 and node 5 takes place nodes 1 and 6. Figure 3.11 shows the scenario of data flow from Node 2 to Node 5.

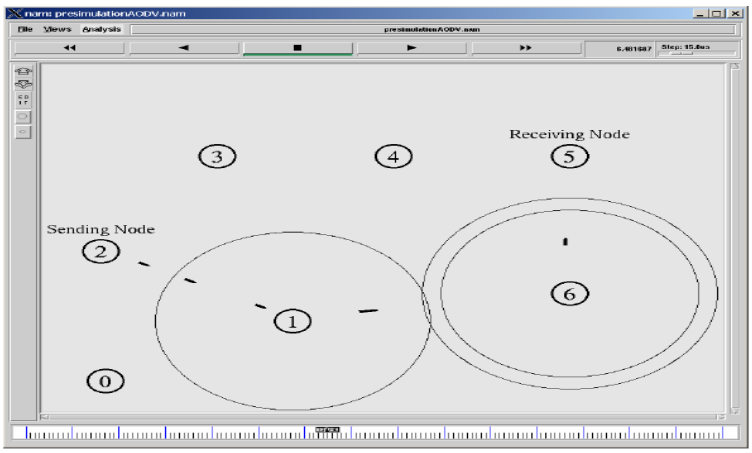


Fig 5.1: The Data flow between the nodes 2 and 5 through the nodes 1 and 6

When the Node 1 leaves the propagation range of the Node 2 while moving, the new connection is established via Node 3. The new connection path is shown in figure 5.2.

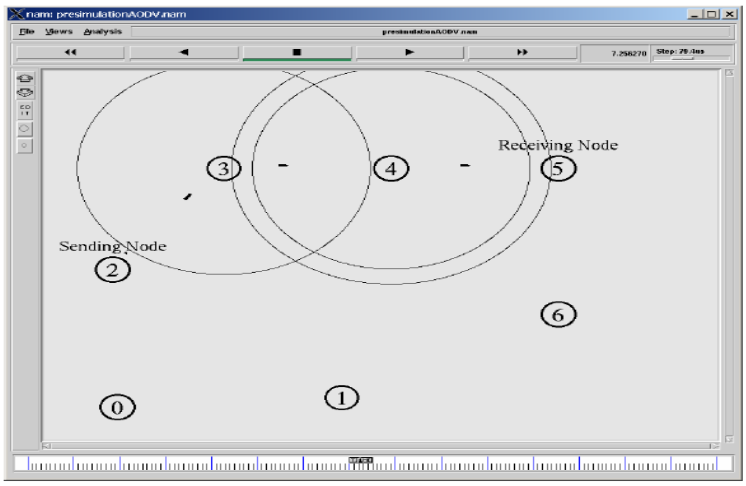


Fig 5.2: The Data flow between the nodes 2 and 5 through the nodes 3 and 4

As node 0 is being assigned with blackhole features, it absorbs the packets by sitting on the connection from node 2 to node 5. Figure 3.13 illustrates how the blackhole attracts the source node and then absorbs the traffic.

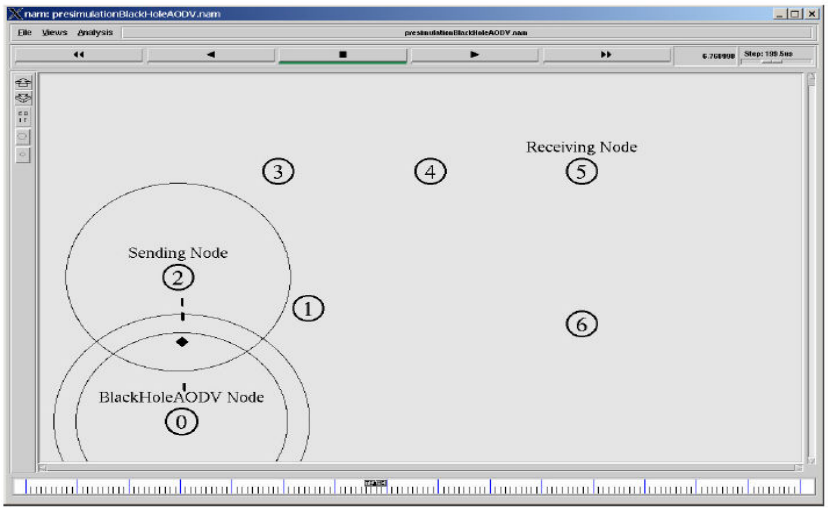


Fig 5.3: The blackhole node 0 drop the traffic from connection node 2 to node 5

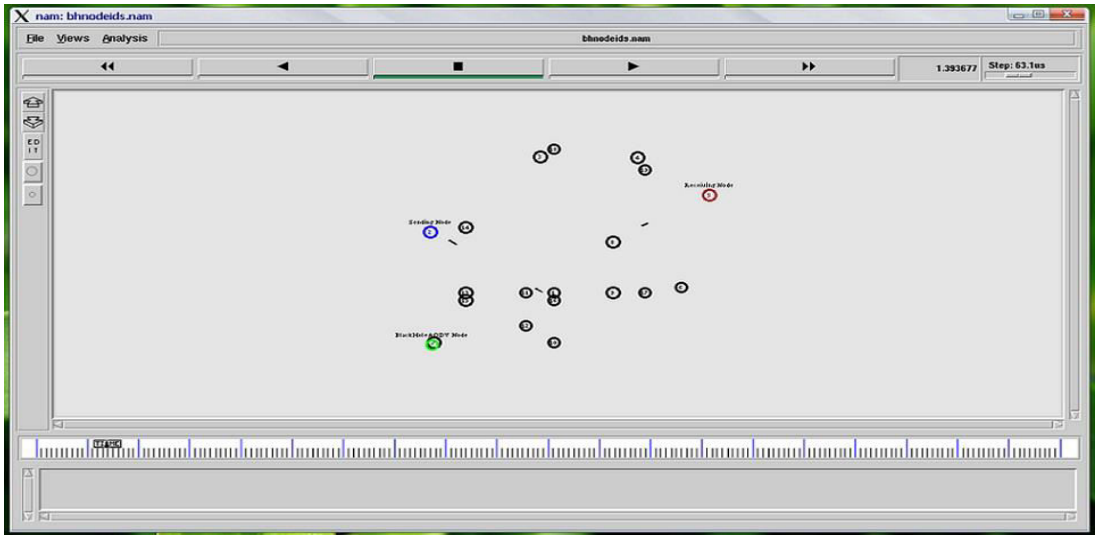
With this simulation test, we make sure that the blackhole implementation bh-AODV is working in a right direction. Then, the

actual simulation is performed with different MANET scenarios and discussed in detail. In every scenario, each single node is placed in diverse coordinates with different movements. This approach helps to get diverse results with the same number of nodes. The inbuilt third party application of NS2 "*./setdest*" is used to arbitrarily generate node positions and movements. The "*./setdest*" application generates a scenario among the nodes that move arbitrarily from an originator to a destination with a speed that is arbitrarily chosen, during 100 seconds, in a 700 x 700 meter space and every scenario is named using the parameters of the "*./setdest*". The CBR application is attached to each UDP connection for generating packets.. The CBR connections are set to start at the 1st second and last until the 99th second of the simulation. In our simulation the Random Way Point mobility model, packet size of 512 bytes and data rate of 10 kbps are used. The random packets are not used in the simulation. The simulation is tested for different number of mobile nodes 20, 30, 40, 40, 50, 60, 70, 80, 90, and 100 using the procedure as discussed above. The third party application of NS2 called "*./cbrgen*" is used to generate different connection types, and are saved in "ns-23.5/scenarios/cp" directory.

5.3. Testing the GTASA, SEA and ECCEA

After having implemented the new GTASA, SEA, and ECCEA protocols in NS2, the test simulations are done to ensure whether they are working properly or not. In this simulation seven static nodes are considered and their positions are fixed as in the test simulation,

shown in Figure 3.11. In this test Simulation SEA or GTASA protocols are used instead of AODV for all nodes except the black hole node (node 1). For instance, to change the AODV protocol to SEA, a small change is made in the Tcl program. That is in the instruction "$ns node-config - adhocRouting AODV", the AODV protocol is replaced with SEA. With the test simulation, it is ensured that the security extensions GTASA and SEA are working properly. Then, we have performed the same simulations on different scenarios to compare the performance of IDS approaches GTASA and SEA with the normal AODV routing protocol with and without the presence of blackhole nodes.



5.4: CBR packets reaching the destination properly

5.4. PERFORMANCE EVALUTION BASED ON EXPERIMENTAL RESULTS

To investigate the influence of blackhole nodes on the performance of proposed routing protocols, the wireless ad hoc network scenarios with and without blackhole nodes are created. Initially to study the effect of the blackhole attack [97], [98], [99] on the AODV and the

proposed GTASA, SEA and ECCEA routing protocols, the test network scenarios with 20 nodes are created. The CBR connections are established between even and odd numbered nodes in the test scenarios. In this simulation setup all the nodes labeled with odd numbers are considered as the sending nodes and the nodes labeled with even numbers are considered as the receiving nodes. For instance, the node 1 transmits to node 2, node 5 to node 6 etc. The nodes 19 and 20 are assigned with blackhole features during the simulations as needed. Consequently, we can easily count the number of packets sent and received between any two nodes. Including at the blackhole nodes, we can also count the number of packets dropped at every node. The simulations are repeated for 50 scenarios with the same nodes acting as a source and destination. But in every scenario, every single node is assigned with different movements and placed at different coordinates. The node movements and positions are arbitrarily created. For every scenario two simulations are performed. In the 1st scenario, each node is functioning in cooperation with every other node to keep the communication in the network. The packet loss in a MANET [100], [101] without any blackhole nodes is shown in Table 5.1. In the 2nd simulation two blackhole nodes are introduced to carry out the blackhole attack in the network. In this simulation, the nodes 19 and 20 are assigned with blackhole features. The number of packets sent and received by the source and destination respectively is measured based on the simulation results. Also an attempt is made to find the number of packets that could not reach the destination,

but are absorbed at the blackhole nodes. These numbers are illustrated in Table 5.2. After then the results of both the simulations are compared to understand the node and system behaviors. The simulation results indicate that the loss of packets with blackhole nodes increases in the network beyond the packets dropped by the blackhole nodes. This is due to the augmented congestion in the paths towards the blackhole nodes. The same simulations are repeated with the proposed GTASA, SEA and ECCEA routing protocols, and results are presented in Tables 5.3, 5.4 and 5.5 respectively.

Path	Packets Sent	Packets Received	Packets Drop (%)
Node 1-Node 2	1074	1061	1.21
Node 3-Node 4	1013	1005	0.78
Node 5-Node 6	1030	1020	0.97
Node 7-Node 8	1013	998	1.48
Node 9-Node 10	1052	1027	2.37
Node 11-Node 12	1081	1070	1.01
Node 13-Node 14	985	976	0.91
Node 15-Node 16	1039	1028	1.06
Node 17-Node 18	1015	1005	0.98
Total	9302	9190	1.20

Table 5.1. Packet loss in MANET for AODV without blackhole nodes

Path	Packets Sent	Packets Received	Packets Drop at Blackholes	Packets Drop (%)	Packets Drop at Blackholes(%)
Node 1-Node 2	1097	206	729	81.22	66.45
Node 3-Node 4	1110	209	732	81.17	65.94
Node 5-Node 6	1072	203	743	81.06	69.30
Node 7-Node 8	1111	219	753	80.28	67.77
Node 9-Node 10	1089	211	733	80.62	67.30
Node 11-Node	1130	228	749	79.82	66.28
Node 13-Node	1128	230	744	80.03	65.95
Node 15-Node	1113	228	736	79.81	66.12
Node 17-Node	1112	225	751	79.76	67.53
Total	9962	1959	6670	80.33	66.95

Table 5.2. Packet loss in MANET for AODV with two blackhole nodes

Path	Packets Sent	Packets Received	Packets Drop at Blackholes	Packets Drop (%)	Packets Drop at the Blackhole(%”
Node 1-Node 2	1024	386	288	62.30	28.16
Node 3-Node 4	1009	377	290	62.63	28.73
Node 5-Node 6	1025	387	296	62.22	28.90
Node 7-Node 8	996	385	289	61.35	29.03
Node 9-Node 10	1046	379	286	63.75	27.37
Node 11-Node	1030	376	297	63.49	28.85
Node 13-Node	1021	383	293	62.45	28.71
Node 15-Node	1028	376	296	62.39	28.74
Node 17-Node	1017	382	297	62.47	29.19
Total	9197	5765	2633	62.68	28.63

Table 5.3. Packet loss in MANETs for GTASA with two blackhole nodes

Path	Packets Sent	Packets Received	Packets Drop at Blackholes	Packets Drop (%)	Packets Drop at the Blackhole(%”
Node 1-Node 2	1064	426	298	59.97	28.01
Node 3-Node 4	1049	417	300	60.24	28.60
Node 5-Node 6	1064	427	306	59.86	28.76
Node 7-Node 8	1035	424	299	59.03	28.89
Node 9-Node 10	1086	419	296	61.41	27.26
Node 11-Node 12	1069	415	307	61.17	28.72
Node 13-Node 14	1060	423	303	60.09	28.58
Node 15-Node 16	1068	416	305	61.05	28.56
Node 17-Node 18	1057	421	306	60.17	28.95
Total	9552	3788	2720	60.34	28.48

Table 5.4 Packet loss in MANETs for SEA with two blackhole nodes

Path	Packets Sent	Packets Received	Packets Drop at Blackholes	Packets Drop (%)	Packets Drop at the Blackhole(%”
Node 1-Node 2	1093	874	107	20.04	9.79
Node 3-Node 4	1078	864	110	19.85	10.20
Node 5-Node 6	1093	890	98	18.57	8.97
Node 7-Node 8	1064	880	117	17.29	11.00
Node 9-Node 10	1115	901	109	19.19	9.78
Node 11-Node 12	1098	878	113	20.04	10.29
Node 13-Node 14	1089	869	197	20.20	18.09
Node 15-Node 16	1097	890	102	18.87	9.30
Node 17-Node 18	1086	872	111	19.70	10.22
Total	9813	7918	1064	19.31	10.84

Table 5.5.Packet loss in MANETs for ECCEA with two blackhole nodes

The simulation results show that the percentage packet loss is more in the presence of blackhole nodes. From the results we can also understood that the normal AODV protocol fails to compete with the blackhole nodes. However, our proposed security schemes succeed in countering the blackhole nodes producing a less percentage of packet loss. For further analysis of the effect of blackhole attacks on the performance of normal AODV and the proposed security extensions GTASA, SEA and ECCEA, the simulation is extended for MANET scenarios ranging from 20 to 100 nodes (with different seed values, blackhole nodes and mobile speeds) and evaluate their performance based on different Quality of Service (QoS) parameters. Then, based on the simulation results, the graphs are plotted for each quality of service parameter by varying the number of nodes in MANET scenarios and the mobile speeds of the nodes using the tool called GNUPLOT.