CHAPTER 4

MITIGATING BLACKHOLE ATTACK IN MANET USING TRUST

The goal of this chapter is to mitigate black hole attack using trust mechanism. In this chapter how, particularly blackhole attack can be prevented is discussed in detail. Also the detail of modification of DSR header file is explained.

4.1 Introduction

Wireless communication is gaining popularity in present era because of its use and availability of mobile nodes. The major advantage of wireless communication is the ability to transmit data among users while staying mobile. However the distance between nodes are limited by the signal strength of the transmitter. If signal strength is more the area covered by the network will be more and vice-versa. Mobile Ad-hoc networks mitigate this problem by allowing out of range nodes to access network through intermediate nodes. Ad-hoc networks have many applications in military and commercial and also in civilian use like personal area network such as conferences, classrooms. Ad-hoc network is best in situation where installing infrastructure is not always possible such as in war zone or disaster management like storm, earthquake. Also ad-hoc network can be connected with other fixed network via gateway devices. Ad-hoc network improves the throughput performance by using all the nodes for routing and forwarding data and control. So selecting appropriate routing technique is a difficult task as the conventional routing algorithm cannot be directly applied in ad-hoc network. Since MANET is an open entry and open exit with higher mobility and dynamicity, the network is vulnerable to various security threads. In MANET there are various factors (Zhou & Hass, 1999) responsible for security like access control, authentication, reputation, trust, integrity, availability etc. In real life situation all nodes may not be cooperative, which leads to malicious act. Trusted routing will identify the malicious node and will exclude them from participating in the routing process.

In MANET (Papadimitratos & Haas, 2002) there may be both active and passive attack. Malicious node can absorb data packets without forwarding it to the appropriate node. Malicious node can also misguide the intermediate hop node with false routing information and hence leads to dropping of data packets. In (Hu *et al.*, 2005; Zapata, 2002) proposed a secured encryption and authentication mechanism to maintain integrity and confidentiality during communication, but such mechanism require a third party trusted which is not suitable for MANET(Griffiths *et al.*,2008). Also this mechanism cannot prevent the inside attacker who are authorized participant of the network. In practical in the routing process a node must have to trust some intermediate node to build the communication though the trustor node could not guarantee the trustee nodes behavior (Gambetta, 2000). Trust in MANET is used to measure the expectations about one node to other for doing some action in the network. The concept of trust defined in social science as a subjective belief about an entity.

Trust management is important where several nodes try to create network without having any prior communication. For set up of initial trust (Eschenauer *et al.*, 2002) method like bootstrapping, certificate authentication etc. is used. Trust management also include trust establishment, trust update, trust information gathering, which are very difficult in dynamic topology network like MANET.

In this chapter, a Trust based mechanism is proposed using a mathematical trust function which find the trust value of each node participating in the network, and this trust function is incorporated with the existing standard DSR protocol. The DSR protocol is updated for finding the trusted route between the communicating nodes.

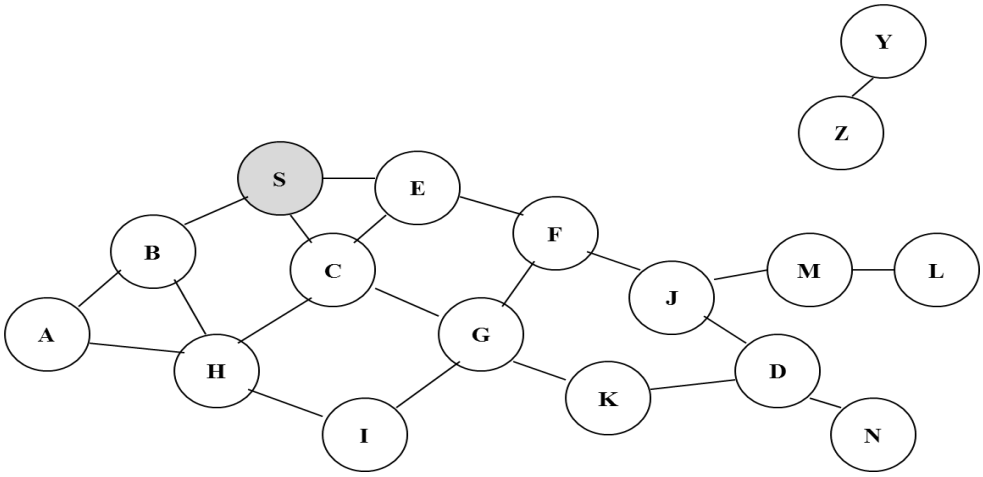
4.2 Dynamic Source Routing (DSR)

The Dynamic Source Routing (DSR) is a reactive unicast routing protocol that utilizes source routing algorithm. In source routing algorithm, each data packet contains complete routing information to reach its dissemination. Additionally, in DSR each node uses caching technology to maintain route information that it has learnt. There are two major phases in DSR, the route discovery phase and the route maintenance phase. When a source node wants to send a packet, it firstly consults its route cache. If the required route is available, the source node includes the routing information inside

the data packet before sending it. Otherwise, the source node initiates a route discovery operation by broadcasting route request packets. A route request packet contains addresses of both the source and the destination and a unique number to identify the request. Receiving a route request packet, a node checks its route cache. If the node doesn't have routing information for the requested destination, it appends its own address to the route record field of the route request packet. Then, the request packet is forwarded to its neighbors. To limit the communication overhead of route request packets, a node processes route request packets that both it has not seen before and its address is not presented in the route record field. If the route request packet reaches the destination or an intermediate node has routing information to the destination, a route reply packet is generated. When the route reply packet is generated by the destination, it comprises addresses of nodes that have been traversed by the route request packet. Otherwise, the route reply packet comprises the addresses of nodes the route request packet has traversed concatenated with the route in the intermediate node's route cache. After being created, either by the destination or an intermediate node, a route reply packet needs a route back to the source. There are three possibilities to get a backward route. The first one is that the node already has a route to the source. The second possibility is that the network has symmetric (bi-directional) links. The route reply packet is sent using the collected routing information in the route record field, but in a reverse order. In the last case, there exists asymmetric (uni-directional) links and a new route discovery procedure is initiated to the source. The discovered route is piggybacked in the route request packet.In DSR, when the data link layer detects a link disconnection, a ROUTE_ERROR packet is sent backward to the source. After receiving the ROUTE_ERROR packet, the source node initiates another route discovery operation. Additionally, all routes containing the broken link should be removed from the route caches of the immediate nodes when the ROUTE_ERROR packet is transmitted to the source. DSR has increased traffic overhead by containing complete routing information into each data packet, which degrades its routing performance. The following example clearly demonstrates the route discovery and route maintenance phase of DSR protocol. In the example we have taken 17 nodes each labeled with A, B, C, etc. Out of which S is considered as sundered node and D as destination node. **[**X, Y] Represents list of identifiers appended to RREQ.

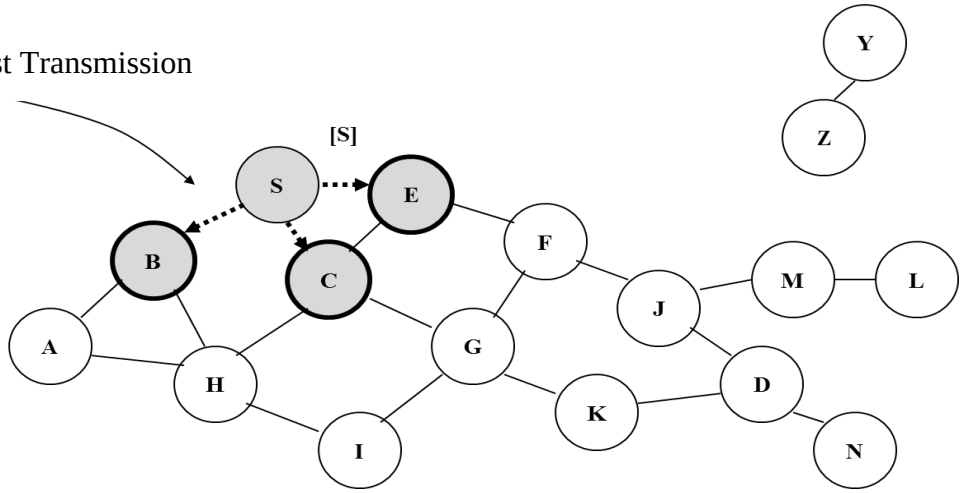
Route Discovery in DSR

- When node S wants to send a packet to node D, but does not know a route to D, node S initiates a route discovery
- Source node S floods Route Request (RREQ)
- Each node appends own identifier when forwarding RREQ



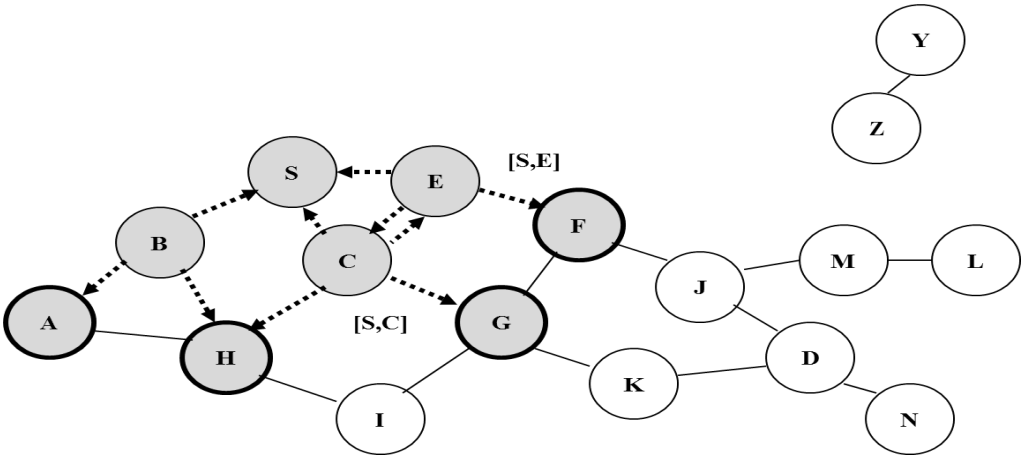
Represents a node that has received RREQ for D.

Broadcast Transmission

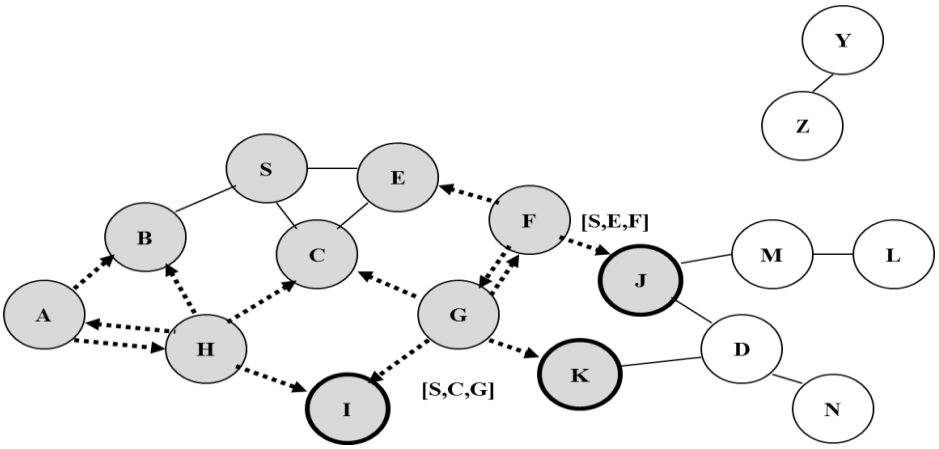


Represents transmission of RREQ

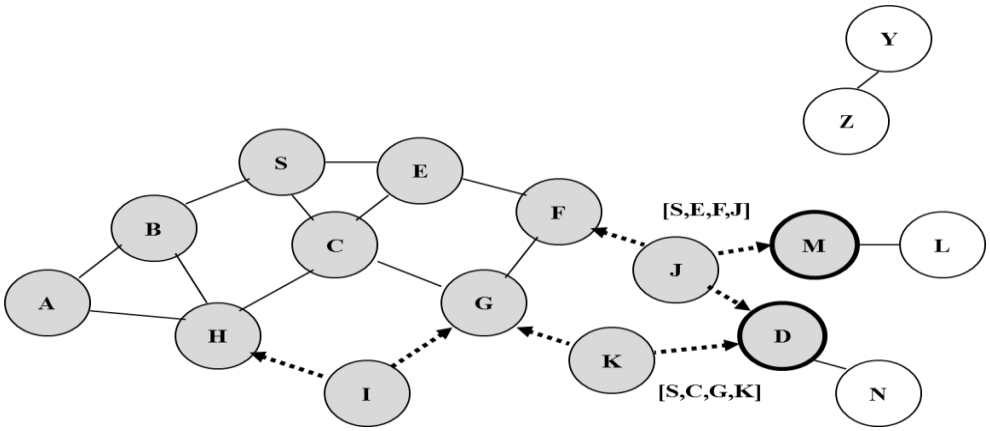
[X, Y] Represents list of identifiers appended to RREQ



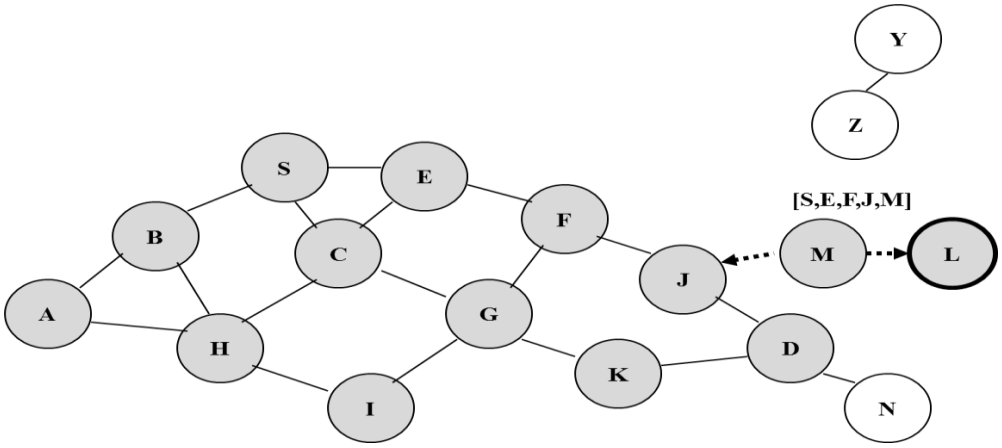
Node H receives packet RREQ from two neighbors: potential for collision



Node C receives RREQ from G and H, but does not forward it again, because node C has already forwarded RREQ once.



Nodes J and K both broadcast RREQ to node D



Node D does not forward RREQ, because node D is the intended target of the route discovery

Figure 4.1: Route Discovery of DSR

Route Reply in DSR

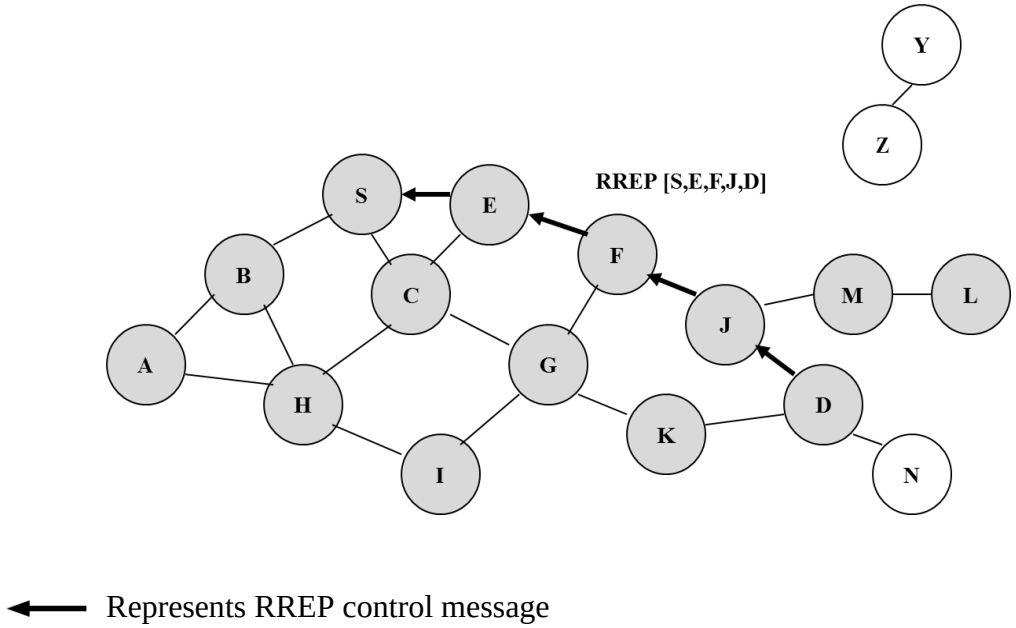


Figure 4.2: Route Reply in DSR

Data Delivery in DSR

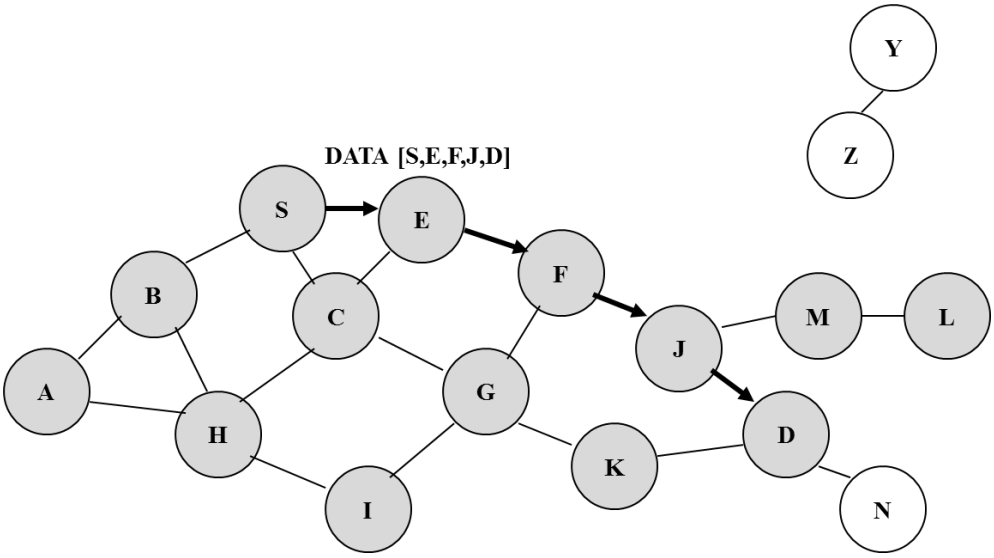


Figure 4.3: Data Delivery in DSR

Packet header size grows with route length as shown in the figure.

4.3 Trust Integrated Dynamic Source Routing

In MANET, as there is no centralized management, most of the protocols are based on cooperation and coordination among the participating nodes in the network. So trust is an important factor for securing a MANET protocol. Since, MANET is dynamic; an attacker can easily exploit the network due. In this trust based approach first, trust value of each node is calculated by the equation used in equation (3.5) using the concept of blind and referential trust. Secondly Trust correlation score is calculated and are integrated in the Dynamic Source Routing protocol. The new modified DSR protocol is named as Trust Integrated DSR (TIDSR). The pictorial representation of the proposed model is given below. Also the trust metrics and the modification performed in DSR are explained below.

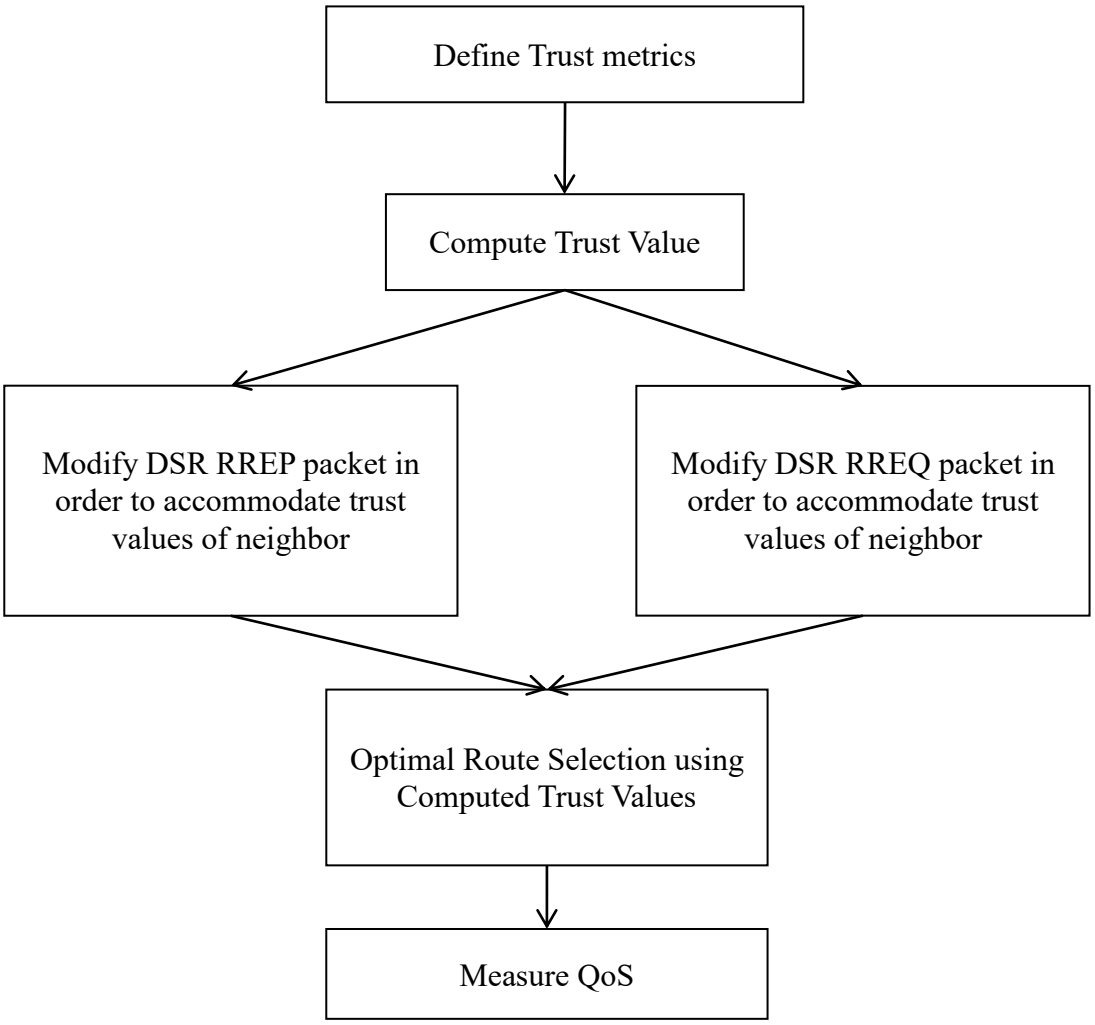


Figure 4.4: Proposed TIDSR

Trust Value Calculation

The Trust Value (TV) of each node is calculated using the following equation a detail of which is explained in chapter 3, of equation 3.5 of the thesis.

$$TV = B_T + (1 - |B_T|) * R_T \quad (-1 \leq B_T \leq 1, -1 \leq R_T \leq 1) \tag{4.1}$$

The above equation satisfies the following properties:

(i) If $|B_T|$ =1, the trust estimator will not consider the referential trust value from a third node.

(ii) If B_T=0, the trust estimator node will completely rely on the referential trust value from third node or nodes.

(iii)The more trust value gets from its direct interaction with a trustee, the less the referential trust will be considered and vice versa.

Trust Correlation Score Matrix: The proposed trust correlation score based on Pearson Product Moment Correlation between any two nodes X and Y is given by the following relation.

$$TCS_{XY} = \propto \cdot \frac{(TV_X - TV_Y)}{\sqrt{(TV_X - TV_Y)^2}} + \frac{P_d}{P_S} \quad (4.2)$$

Where, TV_X and TV_Y is the calculated trust value of any two nodes X and Y. $\propto$ is the threshold value, which lies between -1 and 1. When $\alpha = 0$ the trust value of node is not considered, this may be happen when there is no malicious node in the network. As the value of α increases, the trust correlation score also increases.

The correlation between two nodes means in what degree one node is related to other. Pearson Product Moment Correlation (PPMC) is used for finding the relationship between the nodes, which is a linear relationship function and ranges from -1 to +1.

The DSR's Route Request (RREQ) and Route Reply (RREP) headers are modified to attach the trust values of nodes. The modified RREQ and RREP header of DSR routing protocol are shown in the figure 4.5 and 4.6 respectively.

Table 4.1: Modified DSR RREQ header for blackhole

IP Header	DSR Header	DSR RREQ Header	Intermediate Addresses Address 1, Address 2, ……, Address n.	Trust Score Values

Table 4.2: Modified DRS RREP headers for blackhole

IP Header Reply	DSR Header	DSR RREP Header	Addresses Source Address1, Address2, ……, Address Destination.
Reply Trust Score Values Between source node and Destination node	DSR Source node Route Header	DSR Source Route Address 1… Address N	DSR Source Route Trust Score values

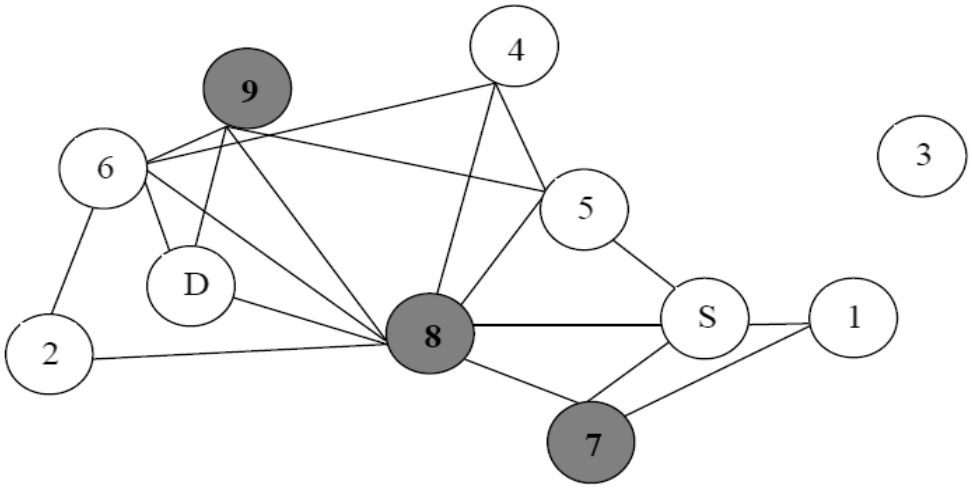


Figure 4.5: A MANET with 3 Malicious Nodes

In the above MANET example, there are total 11 nodes, out of which 3 are considered as malicious, one source node and one destination node. The possible routing path from source to destination is listed in the table 4.3. From the figure it is clear that the shortest path between the source and destination is S - 8 - D. If normal routing technique is considered, since the shortest path is S-8-D, so this will be taken. But node 8 is a malicious one. So some packets may be dropped while passing through node 8. Therefore, secured routing is needed for avoiding malicious behavior.

Table 4.3: Possible Routes between the Source (S) and the Destination (D)

Route	**Path**
R1	S-8-D
R2	S-7-8-D
R3	S-5-9-D
R4	S-8-2-D
R5	S-8-9-D
R6	S-5-4-6-D

Table 4.4: PDR at all Nodes

S	**N1**	**N2**	**N4**	**N5**	**N6**	**N7**	**N8**	**N9**	**D**
0.69	0.87	0.72	0.65	0.76	0.87	0.68	0.85	0.81	079
0.92	0.65	0.98	0.75	0.84	0.76	0.76	0.92	0.72	0.84
0.90	0.91	0.76	0.95	0.64	0.95	0.84	0.71	0.90	0.87
0.86	0.97	0.86	0.97	0.63	0.66	0.81	0.61	0.76	0.78
0.61	0.85	0.95	0.79	0.89	0.65	0.64	0.75	0.94	0.85
0.70	0.63	0.90	0.84	0.80	0.65	0.83	0.85	0.65	0.72

0.95	0.76	0.73	0.80	0.69	0.72	0.94	0.90	0.98	0.68
0.71	0.64	0.89	0.93	0.76	0.82	0.86	0.68	0.95	0.76
0.94	0.97	0.94	0.73	0.85	0.98	0.89	0.77	0.68	0.69
0.66	0.89	0.79	0.76	0.97	0.60	0.61	0.66	0.65	0.79

Table 4.5: Trust Correlation with $\alpha = 1$

S	**N1**	**N2**	**N4**	**N5**	**N6**	**N7**	**N8**	**N9**	**D**
2	0.18	-0.66	0.98	1.3	-0.6	-0.92	1.12	-0.58	-0.78
0.18	2	-0.02	0.04	0.06	0.38	-0.2	-0.08	0.26	-0.7
-0.66	-0.02	2	0.08	-0.48	0.16	-0.28	0.12	0.22	-0.1
0.98	0.04	0.08	2	0.34	0.84	-0.32	1.1	1.02	-0.7
1.3	0.06	-0.48	0.34	2	-0.68	-0.94	-0.38	0.56	-0.72
-0.6	0.38	-0.16	0.84	-0.68	2	1.32	-0.12	0.02	-0.04
-0.92	-0.2	0.28	-0.32	-0.94	1.32	2	0.18	0.36	-0.1
1.12	-0.08	0.12	1.1	0.38	-0.12	0.18	2	-0.58	0.16
-0.58	0.26	0.22	1.02	-0.56	0.02	0.36	-0.58	2	-0.78
-0.78	-0.7	-0.1	-0.7	-0.72	-0.04	-0.1	0.16	-0.78	2

Table 4.6: Trust Correlation with α = 0.5

	S	**N1**	**N2**	**N4**	**N5**	**N6**	**N7**	**N8**	**N9**	**D**
S	1	0.09	-0.33	0.49	0.65	-0.3	-0.46	0.56	-0.29	-0.39
N1	0.09	1	-0.01	0.02	0.03	0.19	-0.1	-0.04	0.13	-0.35
N2	-0.33	-0.01	1	0.04	-0.24	-0.08	0.14	0.06	0.11	-0.05
N4	0.49	0.02	0.04	1	0.17	0.42	-0.16	0.55	0.51	-0.35
N5	0.65	0.03	-0.24	0.17	1	-0.34	-0.47	0.19	-0.28	-0.36
N6	-0.3	0.19	-0.08	0.42	-0.34	1	0.66	-0.06	0.01	-0.02
N7	-0.46	-0.1	0.14	-0.16	-0.47	0.66	1	0.09	0.18	-0.05
N8	0.56	-0.04	0.06	0.55	0.19	-0.06	0.09	1	-0.29	0.08
N9	-0.29	0.13	0.11	0.51	-0.28	0.01	0.18	-0.29	1	-0.39
D	-0.39	-0.35	-0.05	-0.35	-0.36	-0.02	-0.05	0.08	-0.39	1

The PDR between nodes is computed to find the no of packet drops in the network. The Table 4.2 shows the packet delivery ratio between the nodes is approximately 60% to 95%. Table 4.5 shows the trust correlation score values with α =1 and Table 4.6 shows the trust correlation score with α =0.5.

4.4 Results and Discussion

The NS2 simulator is used for network simulation. A network model is designed using NSG2, which comprises of nodes and links, connections and modules. The network model is configured with parameters shown in Table 4.7. For simulation purpose the following scenarios were considered: DSR protocol without blackhole

node, DSR protocol with blackhole node and TIDSR with blackhole node. The experiment is performed by taking 50 of nodes and 4 malicious nodes. In the experiment we have assumed that all nodes have a unique ID and it can be changed at the time of simulation time. Nodes can listen to the packets within its transmission range. The connection between every node is symmetrical.

Table 4.7 Simulation Parameters

Number of Nodes	50
Number of Malicious Nodes	4
Malicious Activity	Blackhole
Routing Protocol Used	DSR
Trajectory of Nodes	Random waypoint
Data Rate of Node	11 Mbps

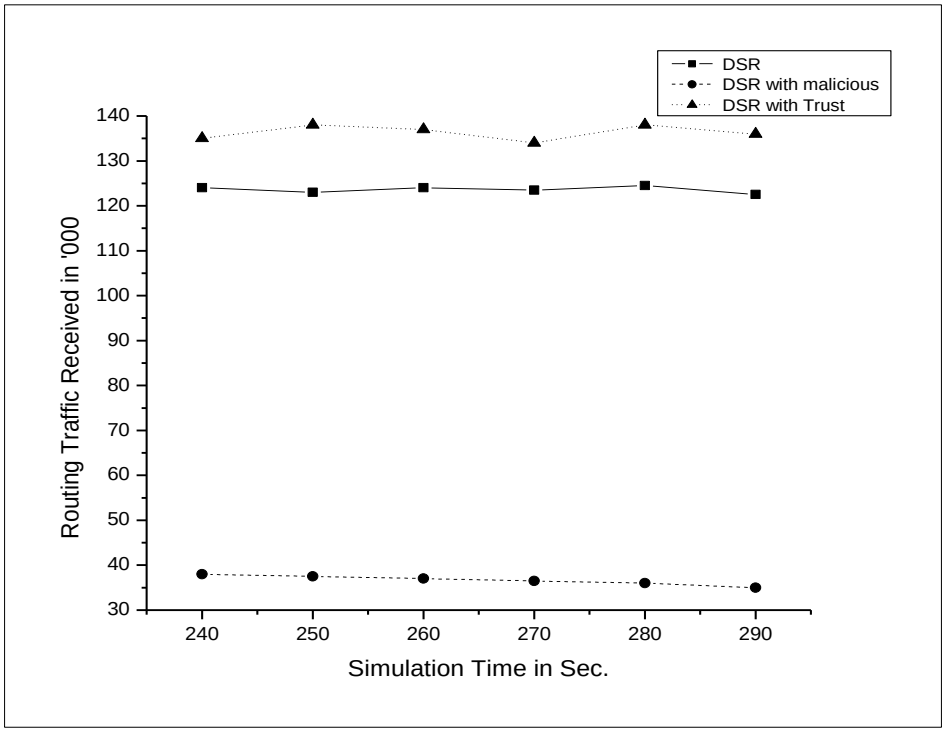


Figure 4.6: Routing Traffic

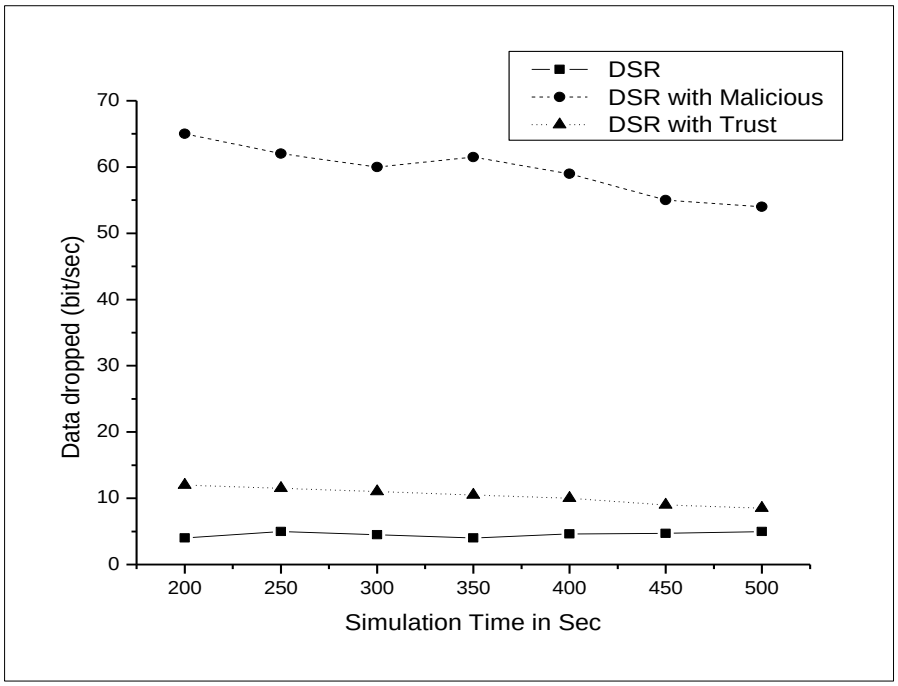


Figure 4.7: Data Dropped due to Threshold Exceeding

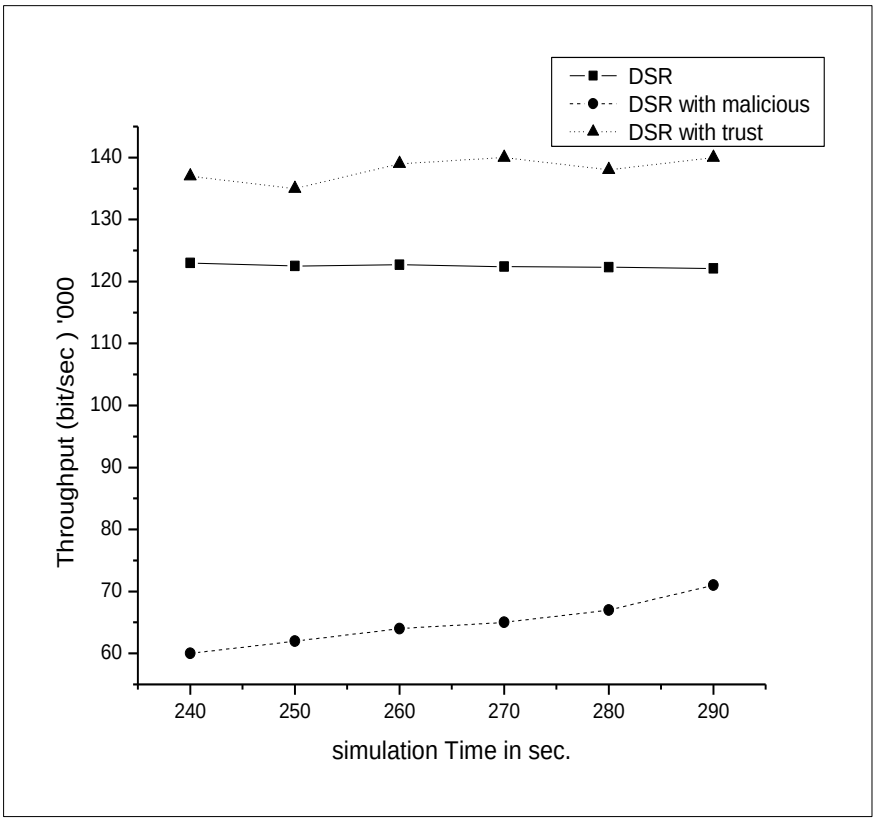


Figure 4.8: Throughput of the Network

The average routing traffic received is shown in the figure 4.6. The proposed TIDSR improves routing traffic by approximately 7.5% because the proposed scheme avoids

malicious node in the network process by selecting the route based on trust values. The figure 4.7 shows the data dropped (bit/sec). When a source node broadcasts RREQ, it waits for a stipulated for reply massage, if it does not arrive within the stipulated time, the nodes again tries by sending another route request. So to avoid the resource constraint, a threshold value is assigned for no of tries. If the no of tries is more than the assigned threshold then the data from the particular node is dropped to avoid congestion. The Throughput of the network is shown in the figure 4.8. It is clear from the figure that although the proposed model takes the long route for rooting, it performs better throughput than the standard DSR. Table 4.8 shows hop count, throughput, end-to-end delay, and data dropped for all the three scenarios. The proposed TIDSR mitigate blackhole attack by identifying and isolating malicious node from routing by increasing approximately 3.5% increase in the no. of hops.

Table 4.8: QoS measured under various experimental setups

Parameters	**Protocol**	**Experimental Result**
Number of intermediate nodes to reach Destination	Standard DSR	2.382145
	DSR with Blackhole	4.8372545
	TIDSR	2.8953434
End-to-End Delay (sec)	Standard DSR	0.000437
	DSR with Blackhole	0.000138
	TIDSR	0.000451
Data Dropped (Bits / sec)	Standard DSR	3.56021
	DSR with Blackhole	62.9777
	TIDSR	7.89762
Throughput (Bits / sec)	Standard DSR	136164.23
	DSR with Blackhole	68256.18
	TIDSR	137293.24

4.5 Chapter Summary

This chapter of the thesis discuss about mitigating blackhole attack using trust function in DSR protocol. Since MANET is based on multiple dynamic nodes with cooperative nature and dynamic topology, so no centralized security measure can be applied directly in MANET. This chapter proposes a trust based mechanism for mitigating blackhole. Here, the DSR header file is modified to measure trust in the network. The proposed TIDSR improves the network performance at approximately 11% without compromising to security although it has increased the intermediate hop count little more. The proposed model can be extended for other protocol as well as for mitigating other malicious attack.