CHAPTER 3

SECURE ROUTING IN MANET USING TRUST ESTIMATION MODEL

This chapter presents a security mechanism using trust model. The trust based security mechanism is attached with the DSR protocol and the performances are compared. Trusts are calculated based on blind trust and referential trust. The new protocol is named as SRUTEM. Then again this model is modified named as TSRM. It uses the similar concept of SRUTEM with some modification. Here we have taken recommendation from different nodes for more justifiable trust. Also while calculating the trust the weights are considered from different factors. The performances were measured with respect to route modification, dropping nodes and flooding of nodes. A reasonable outcome is observed.

3.1 Introduction

Ad-hoc networks are simple, self -configuring, self-structured, dynamic, network with no central infrastructural set up. MANET has many applications in real life situation such as in administrative use, battle field, war zone, meetings etc. Tavli and Bulent, (2006), Boukerche and Azzedine, (2008), Mohammad *et al.* (2003) in their books mentioned various uses of MANET such as conducting meetings among group outside offices, uses in Bluetooth and Wi-Fi protocols etc. Designing an efficient routing algorithm is very challenging because of limited resources such as energy, bandwidth, signal strength, transmission range etc. An efficient and adaptable routing protocol is needed for cope up with the dynamic network condition like network traffic, size, partitioning etc. In the same time the routing protocol should support different type of services to different types of applications. Due to the dynamicity and flexibility in the network topology the MANET is prone to various attacks so security is a major issue in deployment of MANET in large scale. Since in MANET nodes cooperate with each other for transmission of control and data packet, so keeping trust among nodes is very essential for securing the network. Assuring trust is a challenging job among nodes. Also MANET has diverse features than conventional

wireless network, so maintaining of trust of wired network is also not feasible for MANET. In conventional network, a third party may establish a trust among two nodes. This third party may be a central authority for authentication and verification. However in MANET, there does not have any third part. The nodes have to evaluate trust locally by itself. In (Hu *et al.*, 2002), (Papadimitratos and Haas, 2002) authors proposed secure routing protocol to find out secure path among cooperating nodes. Secure routing is achieved by these protocols by confirming the intermediate nodes and authenticating path integrity. The secure routing protocols are vulnerable to flooding and packet dropping attacks as these protocols are not designed to assure the readiness of network. Although a few trust models has been designed for securing routing protocols, till no fully secured trust model has not been developed and still this is an open research topic. This inspired us to propose a Trust Based Security Models for secure routing. MANET network is characterized by the low cost, high performance small and powerful dissimilar devices, communicate effortlessly in highly dynamic, heterogeneous environment. It embraces limited resources, highly dynamic and heterogeneous network, dependence on battery power backup, lack of mechanisms of identity control etc. Evaluating trust within a MANET is a challenging task. MANETs encompasses different network features compared with conventional infrastructure based networks. In MANETs each node must evaluate its trust on other nodes individually. Due to dynamic feature of MANET the trust model designed for static network is not feasible to MANET. Designing an appropriate trust model in MANET is still an open research question and requires further research.

In this chapter, we designed a trust model to estimate trustiness of every node in MANET. In the work, a general trust estimation model has been developed to outfit in real life scenarios. The main contributions of this paper are:

a) Trust model is defined for evaluating trustiness of every node. We calculate the trust using a trust function which comprises of blind trust, referential trust, and a combined function of both blind and referential trust.

b) This trust model is attached with the Dynamic Source Routing (DSR) protocol.

c) The performance of the proposed protocol is evaluated by comparing the simulation results with the DSR in presence of malicious nodes.

The remainder of this chapter is organized as follows. In section 3.2, we discuss some considerations on designing trust evaluation model for MANETs. In section 3.3 we present our new algorithms for secure routing. In section 3.4, the parameters and environment of the simulation were presented, in section 3.5 the result obtained from the simulated experiment has been analysed and finally the chapter is wind up in section 3.6 as chapter summary.

3.2 Evaluating Trust for Secure Routing in MANET

Trust can be defined as an association between two nodes for performing certain activities. The definition of trust is different in different respect. Here we present the definition of trust by (T. Grandison, 2003) as it is a belief that can be quantified with respect to certain attributes such as honesty, competence, security etc. In our trust scheme we used two terms Trustor and Trustee where Trustor is the node that evaluate the trust and Trustee refers to the node that whose trust is been evaluated. Referential node is the node from which recommendation comes. An ad-hoc network is always comprised of many entities, and each entity is an independent node. The trust model can be presented from graph theory as,

$$M = < V, E, f >$$

(1) Trust node set can be defined as$V = \{v1, v2, \ldots, vn\}$, where n is the size of the network;

(2) E is a relation on V, and |E| is the number of edges connected.

(3) $f: f(e_{ij}) \rightarrow R[-1,1]$ Denotes the trust value (a real number between -1 and 1) of each edge e_{ij}.

The trust behavior of an ad-hoc network can be represented as a directed weighted graph as shown in Figure 3.1, this is just an hypothetical example where 1, 2, 3, 4, 5 are the mobile nodes. The circular area is the transmission range of each node and the link value represents the trust value of each node with respect to other.

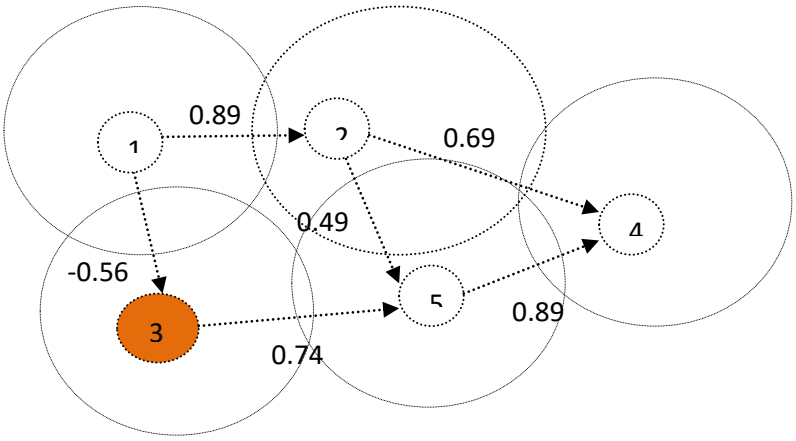

Figure 3.1: Trust Network Graph

System Model: In this chapter we present trusted and secure topology formation using micro devices called nodes to provide nodes communication and information exchange. The network may consists of low cost, high performance, small and powerful dissimilar devices equipped with micro sensors capable of physiological dynamic behaviour monitoring and multimodal biometric continuous authentication in distributed environment. We assume that these devices are equipped with multiple biosensors has continuous authentication which is capable of collecting multiple biometrics, which has the ability to malicious behaviours. The steps for taking routing decisions using trust model are represented in Figure 3.2.

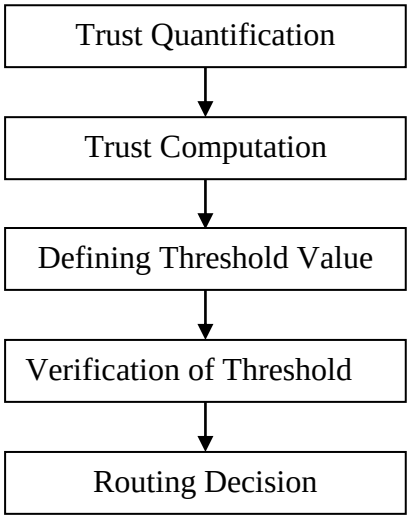

Figure 3.2: Routing steps

A. Trust Quantification: Trust quantification refers to the degrees of trust or distrust that a trust estimator node may have on a trustee node. Here we quantified our trust with continuous real number between -1 and + 1, where -1 is the maximum value that indicates as complete distrust and + 1 is the maximum value that represents as absolute trust. Table 3.1 depicts the trust level we have considered. The number 0 is a natural trust value for a new or unknown node.

Table 3.1: Trust Level

Level	**Trust Value**	**Ranking of Trust**
1	-1	Complete Distrust
2	0	New or Unknown
3	0.2	Very low trust
4	0.4	Low trust
5	0.6	Partially Trusted
6	0.8	Highly Trusted
7	1	Absolute Trust

B. Trust Computation: In our trust model, we evaluate two types of trust between trustor node and a trustee node, Blind Trust and Referential Trust. Blind Trust is the trust that a node has to other directly not taking reference of third nodes. Referential Trust is the trust obtained by a trustor node from a third node or nodes' recommendation on the trustee node.

I. Blind Trust

Blind Trust value is estimated based on the direct experience that a trustor node may have on a trustee node. Direct experiences may be positive or negative. Experiences may include nodes past behavior, performance ratio, packet forwarding, receiving, recommendation to others, dropping packets etc. Positive experience leads to increase

in trust value and negative experience leads to decrease in trust value accordingly. There may be various number of experiences, but in our scheme we have confined it to – 1 and + 1. So to satisfy these here we use hyperbolic tangent function to calculate the trust value of node y.

$$y = \tanh(x) \tag{3.1}$$

A trustor node may have various experiences statistics upon a trustee node and each experience may have different level of importance, for calculating the direct trust value B_T the following function is used.

$$B_T = \tanh \sum_{i=1}^{n} (\mu_i * W_i * P_i) \tag{3.2}$$

Here, Pi indicates the number of experiences of node i on trustee node, n represents the total number of experiences. W_i, is the weight of the experiences of node i and μ is +1 if experience i is positive and -1 if it is negative experience. Here weights are calculated depending on the following factors such as Experience value, Node black list, Reference.

a) **Experience value**: This is the value of prior experience during the communication. Successful communication leads to increase the trust value; unsuccessful communication leads to decrease the trust value.

b) **Node black list:** If the node is black listed or not. If blacklisted in the malicious node list, it will give negative value that is μ will be -1. If it is a good node then μ will be +1.

c) **Reference:** Reference value is based on others recommendation, reputation of evaluated nodes. If it is good μ is +1, otherwise – 1.

II. Referential Trust

If a trust estimator node doesn't have sufficient direct experience on a trustee node, the trust estimator node may enquire to a third node for recommendation. We assume that the third node has some trust value V_i on the trustee node based on its own evaluation. The referential trust R_T value for the trustor node is calculated as:

$$R_T = B_T * V_i \quad (3.3)$$

Where, B_T means direct trust value that the trustor node has on the third node. To ensure the reference is more justifiable, a trustor may collect more than one node for reference. So the referential trust value is calculated as

$$R_T = \frac{1}{n}\sum_1^n (B_T * V_i\ ) \quad (3.4)$$

Combination of Blind Trust and Referential Trust: Finally for finding the ultimate trust, we combined both the Blind Trust and Referential Trust with a relationship function. The amount of recommendation will be taken based on how much blind trust value the trustor nodes have on trustee node. The higher blind trust value that the node has, the smaller value will be taken from referential trust value and vice-versa. If the trustor node does not have any blind trust value, it will completely rely on referential trust and if the trustor has complete blind trust it is not required to collect reference trust value from other nodes. To satisfy these properties, we define a relationship equation to express relationship between Blind Trust and referential trust. By applying this relationship the ultimate trust value is evaluated.

$$V = B_T + (1 - |B_T|) * R_T \quad (-1 \leq B_T \leq 1, -1 \leq R_T \leq 1) \quad (3.5)$$

This relationship equation satisfies the following properties:

(i) If a trustor node has full blind trust, i.e. $|B_T| = 1$, the trustor will not consider the referential trust from a third node.

(ii) If a trustor node does not have any blind trust, it will go for referential trust, i.e. BT=0, the trustor node will completely rely on referential trust.

(iii) The more trust value the trustor gets from its blind trust, the less referential trust will be consider and vice versa,

(iv) The amount of referential trust being considered based on the amount of blind trust, but not vice versa.

C. Making Decision with Trust Value

For taking security decision, a threshold value must be defined. The threshold value may vary based on the security needed by each task. For example, a very important message may be required a high security level where as a less important message may not require a high threshold value. In this implementation we have assumed 0 as the threshold value. By checking the computed trust value with the threshold trust value, the node can easily take the decision whether the evaluated node is trusted or not. The deviational equation for decision taking can be given as

$$D = V - T_{threshold} \tag{3.6}$$

If $D \geq 0$, it means the computed trust value satisfies the threshold limit. If $D < 0$, it means that the trust requirement is not satisfied.

D. Maintaining Trust Information

In our model, each node performs its trust evaluation itself. For maintaining the trust information each node maintain an additional trust information table, which carries trustee node' ID, Blind trust value, numerical value of direct experience, referential trust value and the combined trust value. During the operation of the system, the nodes will update their trust information either periodically or upon request depending upon the protocol it will use.

3.3 Algorithms

Algorithm 3.1: Trust Calculation with Blind trust

Blind Trust (B_T, A, B, PR, PF)

// B_T is the blind trust

// A is an observer node

// B is an neighbor node

// PR is the no. of the packet received

// PF is the no. of packet forwarded {

Step 1: if A finds B is a trustee from the trust table then A will send packet to B

Step 2: PR=PR+1;

Step 3: if node A finds that node B forwards the packet successfully

Then PF=PF+1;

Step 4: Else if B is unable to receive

Then PR=PR-1;

end if

end if

end if

Step 5: Calculate the trust value, B_T, from equation (3.2) and update the old one. }

Algorithm 3.2: Referential Trust Calculation

Referential Trust (R_T, A, B)

// R_T is the referential trust

// A is an observer node

// B is an neighbor node

{

Step1: If node A, has more than one hop neighbors between it and the trustee, node B then calculates the trust value, from equation (3.4)

else

Step 2: set Trust value to 0

end if

}

Algorithm 3.3: Combined trust calculation

Combined Trust (V, B_T, R_T, A,B)

// V= Final trust value

// B_T= Blind Trust

// R_T= Referential Trust {

Step 1: If node A gets both B_T, R_T on a trustee node B then calculates the trust value,

from equation (3.5)

else

Step 2: set Trust value to 0

end if }

Algorithm 3.4: for Secure Routing Using Trust Estimation Model (SRUTEM):

Step 1: Source node broadcasts RERQ for route discovery.

Step 2: The neighbors of the source node first checks its evaluation matrix with the predefined threshold value and if it satisfies the threshold value (assumed as 0 for this algorithm) it sends the RERQ message to their neighbor & so on, until the destination is reached.

Step 3: If some nodes respond that they have fresh route to the destination node and wants to transfer data, the source node checks the trust evaluation matrix and conducts the trust evaluation on the responded nodes. Based on the evaluation result the source node selects one preferred route, when it believes the best.

Step 4: The source node sends data packets to the destination node using the selected route.

Step 5: After receiving the data packets the destination node uses the same method to reply the confirmation message if the source node requests it.

Step 6: If within the stipulated time, the target nodes confirmation arrives and treated as trusted, the source node will continue sending data packets using the route.

Step 7: If the destination's confirmation is not received within the stipulated time, the source node will update its trust evaluation matrix data on the routing nodes by reducing the trust value. If the source node makes sure the response node of underlying route is malicious, it will put the node into the intrusion black list, set that value to -1.

Step 8: The source node selects the second best route and then goes to step 4 and repeat.

Algorithm 3.5: Algorithm for Trusted and Secured Routing in MANET (TSRM)

TSRM (S, T, N_i, TM, α,→)

// S is the source node

// T is the target node

// N_i is the neighboring nodes

// TM is the trust evaluation matrix

// →is sending

// α is the threshold value

{

Step 1: S → RREQ to N_i.

Step 2: N_i checks TM with α.

Step 3: If value of TM of N_i>**α**

N_i→RREQ to its neighbors

Continue until T is reached.

Step 4: If some N_i responds route to T,

Then S checks the TM of some N_i and chooses the best route.

Step 5: S→data packets to T using the route.

T → confirmation message.

Step 6: If T's confirmation arrives within the time slot, then using the root, S will

continue to send data packets.

Else if within the preferred time slot, T's confirmation is not received, by reducing the trust value S will update its trust evaluation matrix.

Else If the source node confirms the malicious behaviour of the response node of underlying route, malicious; it will set the value to -1 and will keep the node in the disturbance black list.

Step 7: The source node selects the second best route and then goes to step 4 and repeat. }

3.4 Simulation Environment

The performances of modified DSR protocols and original DSR are evaluated in the presence of malicious node using NS2 simulator. The simulations have been performed in a mobile traffic scenario. The DSR routing protocol is used for all simulation and the other simulation parameters are shown in the Table 3.2 and Table 3.3. The topology of the MANET depends on the pause time and mobility speed. It changes frequently when pause time is less and mobility speed is more. The performance of SUTEM, TSRM and DSR routing protocol under the presence of

malicious node were evaluated using NS2 simulator. The simulations have been carried out under a wide range of mobility and traffic scenarios.

Table 3.2: Simulation Parameter used for SRUTEM

Parameter	**Value**
Simulator	NS2 (ver 2.34)
Simulation Time	500 sec
Number of Mobile Nodes	50
Transmission Range	250 m
Topology	1000m x 1000m
Routing Protocol	DSR
Maximum Bandwidth	1 Mbps
Traffic	CBR
No. of Malicious node	1 to 5
Packet Size	512

Table 3.3: Simulation Parameter used for TSRM

Parameter	**Value**
Simulator	NS2 (ver. 2.34)
Simulation Time	500 sec
Number of Mobile Nodes	100
Transmission Range	250 m
Simulation Area	$1200 \times 1200 m^2$
Routing Protocol	DSR
Maximum Bandwidth	1 Mbps
Traffic	CBR
Total CBR connections	20
Threshold limit	0.60

3.5 Result and Discussions

The performance of our proposed technique SRUTEM is compared with original DSR protocol in presence of malicious node. The following table and graph shows the recorded simulation results by adding the trust function to the existing DSR protocol. In every communication the modified DSR protocol checks the neighbouring node using the trust estimator function and identifies the malicious node and determines the amount of packets that are dropped by malicious nodes from the total dropped packets. The Packet Delivery Ratio is used to compare the existing DSR protocol and the improved DSR protocol i.e. SRUTEM to determine the impact of the trust based routing to the DSR protocol. The throughput of the SRUTEM is also evaluated.

Table 3.4: Recorded Simulation Data (Avg. of 10 scenarios)

Communication between nodes		**Packet Sent**	**Packet Received**		**Packet Loss (%)**	
Source Node	Next Hop Node		With Existing DSR	With SRUTEM	With Existing DSR	With SRUTEM
N1	N2	500	20.23	112.45	95.95	77.51
	N3	650	178.12	302.62	72.6	53.44
	N4	700	325.35	590.05	53.52	15.71
	N5	740	27.37	137.8	96.3	81.37
	N6	790	201.3	380.1	74.51	51.89
	N7	800	356.44	691.72	55.45	13.54

Table 3.5: Recorded Simulation Data of PDR & Throughput (Avg. of 10 scenarios)

Communication between nodes		**Packet Delivery Ratio (PDR)**		**Throughput**	
Source Node	Next Hop Node	With Existing DSR	With SRUTEM	With Existing DSR	With SRUTEM
N1	N2	4.04	22.49	5.2	5.08
	N3	27.4	46.56	6.78	7.51
	N4	46.48	84.29	4.76	5.36
	N5	3.7	18.62	6.93	7.8
	N6	25.48	48.11	7.74	8.15
	N7	44.56	86.47	4.35	4.9

The tables show the recorded simulation data which is the average of 10 scenarios. Also the performance of our proposed technique (TSRM) and the original DSR protocol is compared in presence of malicious node. We have taken packet dropping of nodes, flooding and route modification of nodes for the performance comparison. Under various proportions of malicious nodes, the nodes of TSRM and DSR are compared. Here PDR is the performance metric. The average ratio of the total number of CBR data packets received by the destinations to the total number of CBR packets sent by the source is defined as the packet delivery ratio.

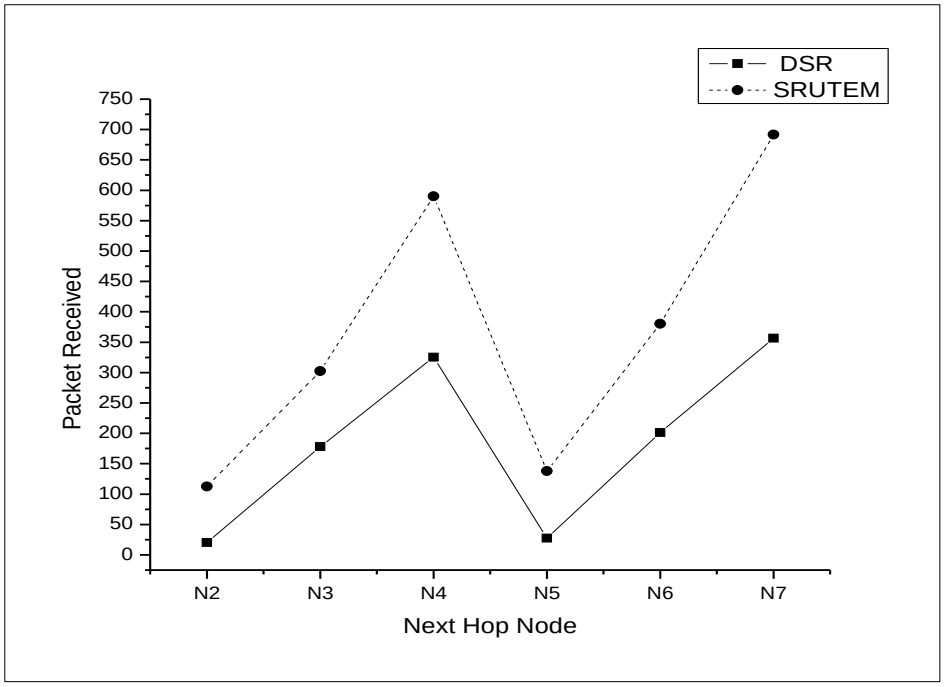

Figure 3.3: Data Analysis of RREQ Packet Sent/ Received

The Figure 3.3 shows the graph of total RREQ sent/received from node N1 versus neighbouring nodes with mobility speed 5 m/s and pause time zero (0). It is clear from the graph that SRUTEM can perform better than DSR.

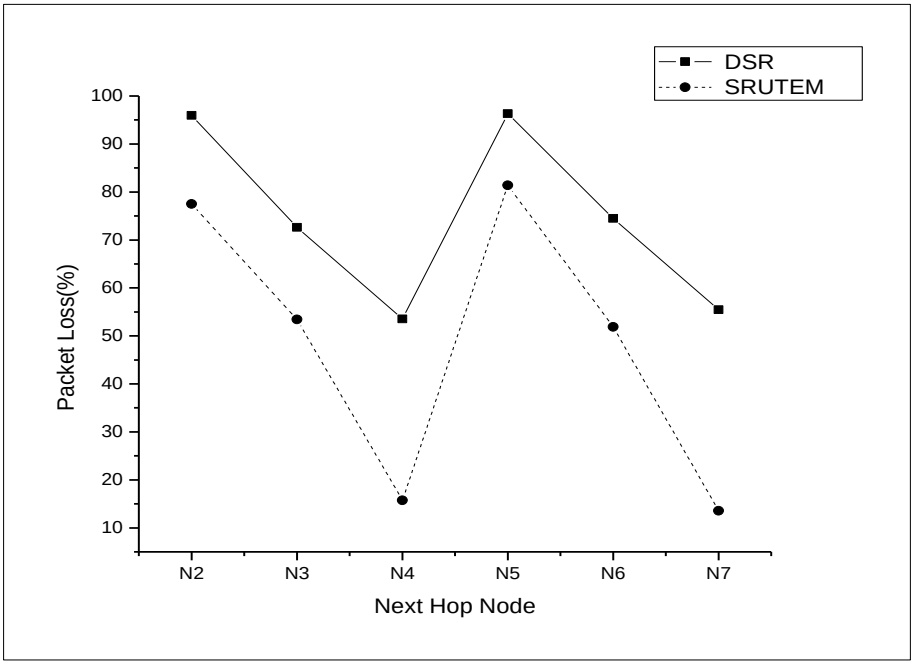

Figure 3.4: Data Analysis of RREQ Packet Loss

From the Figure 3.4, it has been observed that packet loss is less between the source node N1 and the neighbouring nodes in SRUTEM than standard DSR. When the packet passes through trusted node (here N4 and N7) the amount of packet loss is the lowest as we can see in the graph.

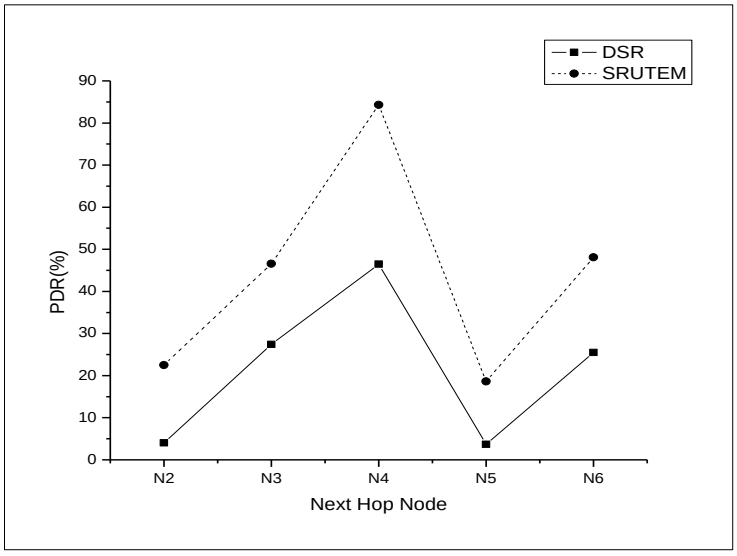

Figure 3.5: Packet Delivery Ratio (with DSR versus SRUTEM)

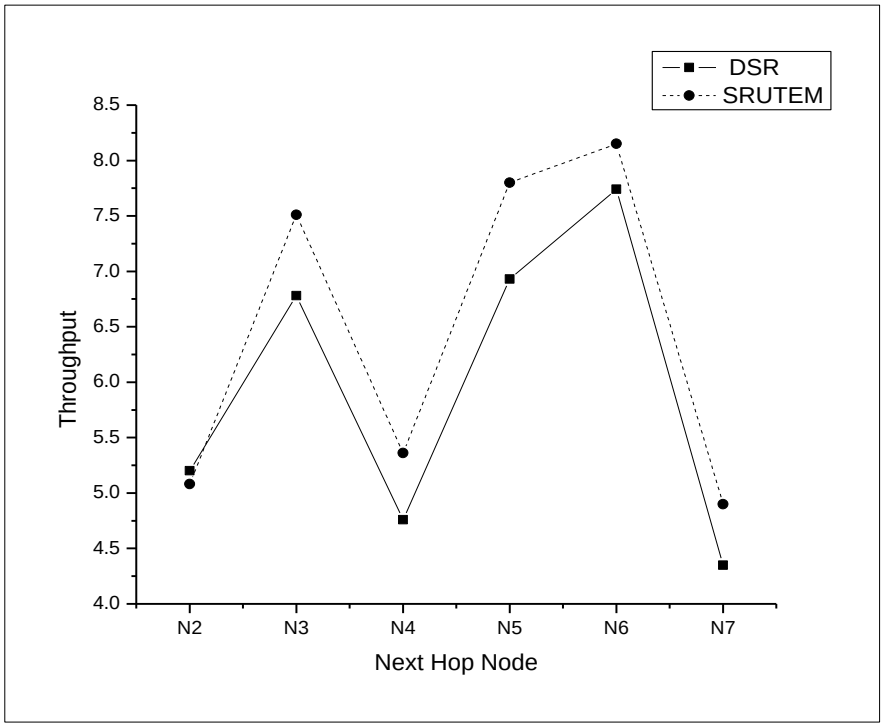

Figure 3.6:Throughput (with DSR versus SRUTEM)

It is observed from Figure 3.5 that packet delivery ratio is less using existing DSR as compared to SRUTEM. Figure 3.6 shows that throughput is more in without flooding environment using SRUTEM than in flooding with existing DSR. From the four figures we have seen that our modified methodology is able to secure the routing behaviour using trust estimation model up to a reasonable extent.

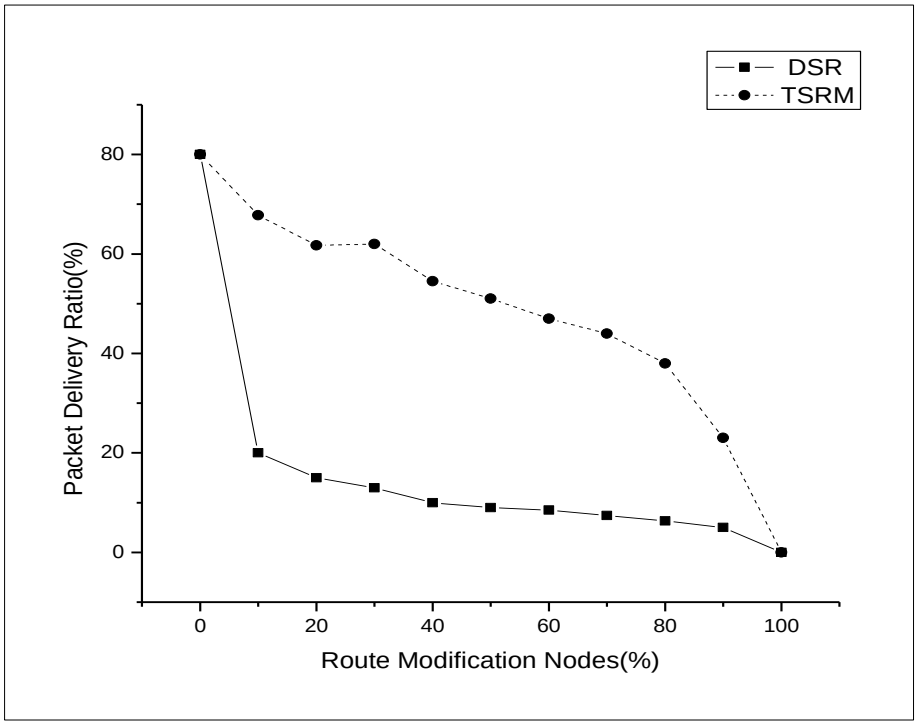

Figure 3.7: PDR against Route Modification

According to figure 3.7, the performance of TSRM nodes is better in terms of route modification nodes (%) as compared to DSR. The possible reasons are - TSRM nodes accept packets from trusted previous nodes. Also they forward packets to the trusted node and the packets are propagated only through trusted packets and trusted routes. From the result it is confirmed that TSRM nodes provides valid routes even with higher amount of malicious nodes. Also figure 3.7 depicts that in the absence of malicious nodes TSRM nodes do not experience extra overhead.

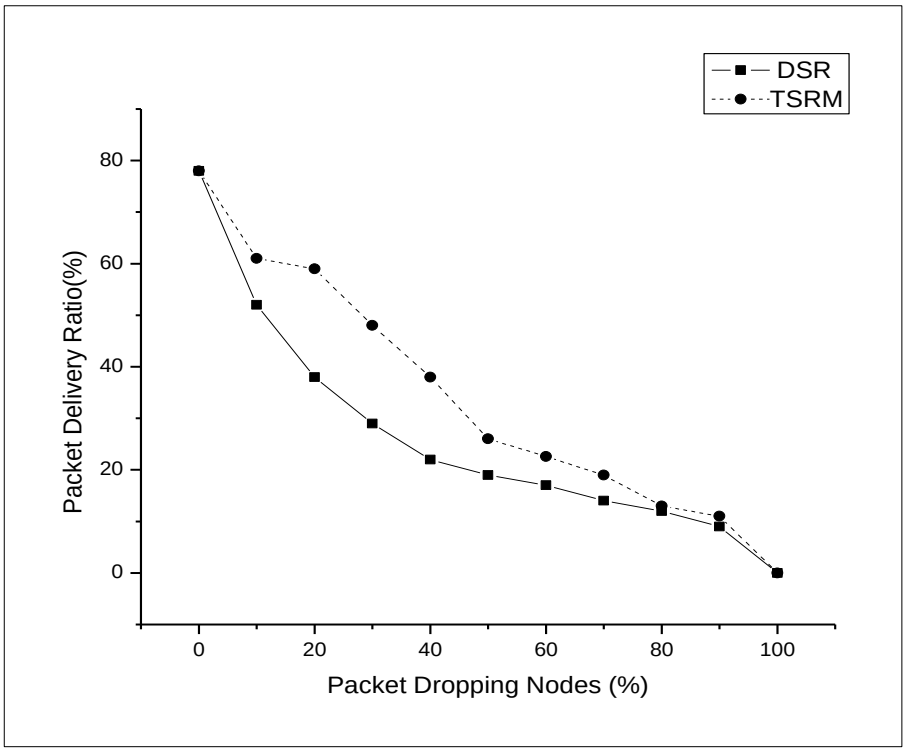

Figure 3.8: PDR against Packet Dropping Nodes

Figure 3.8 shows that TSRM performs better in case of packet dropping nodes as compared to DSR. But the act of TSRM is condensed pointedly as equated to DSR nodes in the presence of 85% of packet dropping nodes.

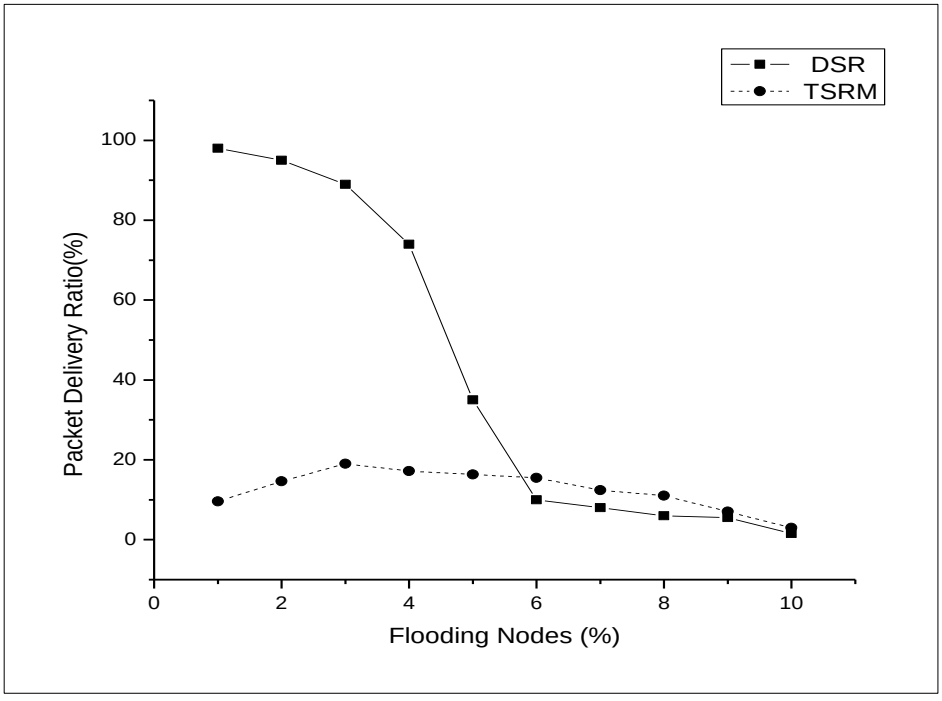

Figure 3.9: PDR against Flooding Nodes

From Figure 3.9, it is obvious that TSMR nodes give better performance when compared with DSR nodes in terms of PDR against flooding nodes. Unlike Figure 3.7 and 3.8, in Figure 3.9 we can see the performance of TSRM and DSR nodes, when the flooding nodes are considered. The figures 3.7, 3.8, and 3.9 show the Packet Delivery Ratio (PDR) in TSRM against malicious node as compared to DSR.

3.6 Chapter Summary

In this chapter a trust model is presented for securing MANET. Here a trust based scheme is defined using trust relationship function. Trusts are calculated using both the blind trust and referential trust. This trust relationship function is then integrated with the DSR protocol. The new modified protocol is named as SRUTEM. Then the performance of modified protocol and DSR protocol is studied with performance matrices such as packet sent, received, loss, PDR, throughput etc. A reasonable outcome is observed. Also in this chapter an improved trust establishment scheme is used to detect and prevent routing attacks. The trust function is used in DSR protocol. The chapter also presents simulation results to prove the efficacy and efficiency of the proposed model. In future, a more improved trust model can be developed for better security solution.