CHAPTER 5

TRUST BASED ROUTING FOR MITIGATING GRAYHOLE ATTACK IN MANET

The aim of this chapter is to design a security model which can resist grayhole attack, which is a special type of blackhole attack. This chapter presents details of how attack model is implemented in NS2 and how the original protocols are modified. Finally it shows how the grayhole attack is prevented in MANET.

5.1 Introduction

MANET is a temporary network created and operated by the nodes themselves without having any centralized infrastructure. Nodes cooperate with each other by passing data and packets from one hop to another. Every nodes act as a router itself for communication. MANET is a multihop wireless network with dynamic topology, low battery power and limited bandwidth. Due to dynamic nature of nodes (Kannan and Mohapatra, 2012) topology changes frequently at any time. So it is very difficult to find an optimal route for communication. The routing algorithm must act quickly as the topology changes. Different protocols (Elizabeth *et. al.*, 1999) have been developed for such type of network. Since the network is dynamic in nature, the topology changes frequently and the network is open to attack and unreliability. Nodes misbehavior due to malicious intention could significantly degrade the performance of MANET. In MANET the nodes act both as host and router and act as a communicating device in a wireless environment, so trust is a major factor in MANET because ad-hoc network communicate depending upon the cooperative and trusting nature of nodes. Since the nodes changes frequently, so the number of nodes participating in the route selection is always changing, thus the degree of trust also changes. Trust is a relationship between two nodes. Trust value can be stated as the degree that one node expects another node to offer certain services. Trust can be calculated directly or by recommendation by other nodes. Grayhole attack (Xiao *et al.*, 2006), a different form of blackhole attack (Mohammad *et al.*, 2004) is an active attack type which drop packets. In grayhole attack the attacker node accepts the packets for forwarding, but without doing so it just drops it. In grayhole attack the malicious node initially behave correctly and reply true RREP messages to that forwards RREQ messages. This way it takes the packets and later just drops the packets. The sender nodes thus loose the connection and again try to establish a new route, broadcasting RREQ messages. Attacker node again do the same things thus consume battery power and other network resources. This study reveals with a new Dynamic Source Routing Protocol for MANET based on trust model to mitigate grayhole attack. Trust is calculated based on trust function. Nodes are selected based on the values of trust function and threshold value. The modified DSR protocol can effectively detect the grayhole nodes and isolate them from taking part on routing. This paper tries to mitigate the grayhole attack using trust based routing. In this paper the original DSR protocol has been modified along with trust estimation model. The communication between the nodes in the MANET is based on the trust value of a node to its neighbors**.** Trust value is calculated based on the experiences of node. Grayhole attack, a type of blackhole attack (Bhalaji and Shanmugam, 2009) is an active attack type which drop packets. In grayhole attack the attacker node accepts the packets for forwarding, but without doing so it just drops it. In such attack the malicious node initially behave correctly and reply true RREP messages to nodes that forward RREQ messages. This way it takes the packets and later just drops the packets. The sender nodes thus loose the connection and again try to establish a new route, broadcasting RREQ messages. Attacker node again do the same things thus consume battery power and other network resources. Trust is a critical factor based on uncertainty conditions and is used for decision making on cooperating with unknown participants (Solhaug, 2008). It includes establishment and updating of trust. In Golbeck (2006) explain the features of trust as trust may not be transitive, symmetric. That means if node A trust node B, and node B trust node C that does not necessarily imply A trust C. Also symmetric means if node A trust node B that does not guarantee that B will trust A. In Yunfang (2007) elaborates logic and reputation based trust. Logical policy based mechanism takes binary decision depending upon which a node is certified as trusted or not. In (Xiaopeng and Wei, 2007) the authors proposed an aggregate signature algorithm for grayhole nodes. In that mechanism aggregate signature algorithm, DSR protocol and network model were incorporated. Aggregate signature algorithm was used to trace grayhole nodes. In this paper, we present a Trust Based DSR (TBDSR) to mitigate packet dropping that is grayhole attack. In the process first the nodes trust value is calculated using the trust calculating function, then the DSR RREQ header and RREP header were updated. Based on trust value and threshold value the optimal route has been selected for routing. Finally the performance were measured based on various performance parameters. The remainder of this paper is structured like this. In section 5.2 the proposed trust model is discussed including the algorithm. In section 5.3, the experimental setup was presented. In section 5.4, The Result and Discussion were discussed. Finally the paper is wind up with chapter summary in section 5.5.

5.2 Proposed Trust Based Model (Trust Based DSR)

The proposed Trust Based DSR (TBDSR) improves the DSR protocol (Johnson *et al.,* 1996) fortified with trust based route selection. In this model the trust values will be adjusted based on the experiences that the node has with its neighbor nodes. In the proposed work the DSR routing protocol is embedded along with the trust estimation function. The communication among the nodes in the MANET depends on the coordination and the trust value with its neighbors.

.

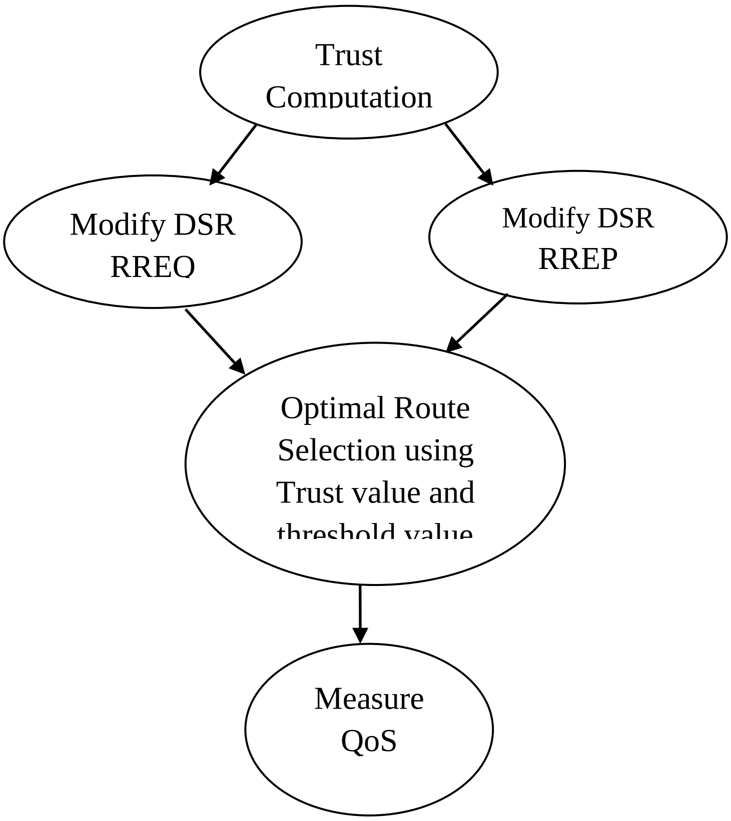
Trust Computation
Modify DSR RREQ
Modify DSR RREP
Optimal Route Selection using Trust value and threshold value
Measure QoS

Figure 5.1: Proposed Trust Model

5.2.1 Trust Computation

We propose a very simple equation for the calculation of trust value.

$$V = tanh\,(r1 + r2 + A), \tag{5.1}$$

Where,

V = Trust value

$$r1 = \frac{\text{number of packets sent}}{\text{number of packets to be sent}}$$

$$r2 = \frac{\text{total no. of packets received from a node but not originated from that node}}{\text{total number of packets received from it}}$$

A = Acknowledgement bit (0 or 1)

Here, we use hyperbolic tangent function (Kannan, 2012)) to limit the computational trust value within the range -1 and +1.

5.2.2 Maintaining Trust Information

In this scheme the trust of each node is calculated locally. To store the trust information, 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 table 5.1 and Table 5.2 respectively.

Table 5.1: Modified DRS RREQ Header for grayhole

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

Table 5.2: Modified DRS RREP Header for grayhole

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 values

5.2.3 Decision Making using Threshold Value

To make a security decision with the computed trust value, we need to approximate the level of risk that can be affordable by each task. In other words, a threshold trust value has to be fixed for each task. Such threshold value may be varied depending on the security requirement of each ongoing task for example a very important message may have threshold value as 0.8 where as a less important one may have threshold value as 0.2. By comparing the computed trust value and the threshold trust value, it is easy to see whether the trustor node can trust the trustee. A simple equation for making decision is defined as follows:

$$D = V - treshold\ value \qquad (5.2)$$

If D ≥ α , it means the computed trust value satisfies the trust requirement of the ongoing task and is trusted as per the degree of trust. If D < α , it means that the trust requirement is not satisfied.

5.3 Algorithm for Routing

Notations:

SN: Source Node

```
IN: Intermediate Node

DN: Destination Node

    Step 1: SN broadcasts RREQ

    Step 2: SN receives RREP {

        IF (RREP is from trusted node)

            {

            Route data packets (Secure Route)

            }

        ELSE

            RREP is from Unknown node

      Insecure Route

      IN can be a grayhole node

     } While (IN is NOT a reliable node)
```

5.4 Simulation Environment

The proposed model is implemented using network simulator 2. Here the original DSR protocol is modified with calculated trust value. The DSR’s Route Request (RREQ) and Route Reply (RREP) headers are modified to attach the trust values of nodes. Here calculated trust is used to identify and handle grayhole attack in the routing process which drops the packets. For simulation random waypoint model is used that is in random waypoint any node can start at random position, waits for pause time and then moves any other random position. The simulation parameters used is tabulated below.

Table 5.3: Simulation Parameters

Parameter	**Value**
Simulator	NS2 (ver 2.34)
Simulation Time	800 sec
Number of Mobile Nodes	100
Transmission Range	250 m
Topology	1000 m × 1000m
Routing Protocol	DSR
Maximum Bandwidth	1 Mbps
Traffic	CBR
No. of Malicious node	9
Packet Size	512

5.5 Results and Conclusion

In this simulation experiment we have used various parameters for performance analysis of the Trust based DSR protocol. Here we have calculated Packet Delivery Ratio, throughput of the network, routing overhead and dropped data packets. The experimental values and their respective graphical representation are given below.

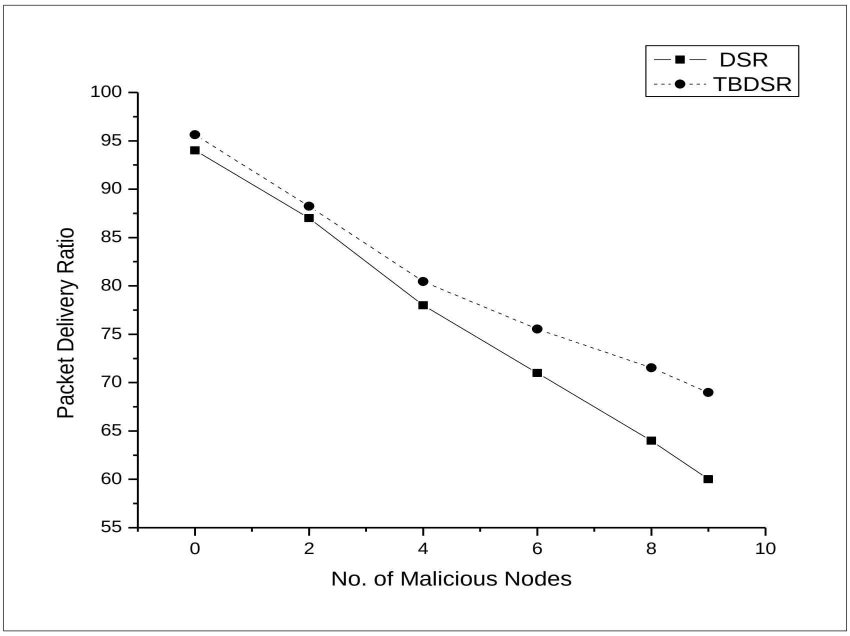

Figure 5.2: Packet Delivery Ratio

Here we have calculated the Packet Delivery Ratio of both DSR and TBDSR for measuring the performance of trust based DSR. It is been observed that when there is no grayhole malicious node both DSR and TBDSR's Packet delivery Ratio is more than 90%, but as the no of malicious node increases the PDR decreases. It is estimated that with approximately 20% of grayhole node the PDR for TBDSR is approximately 70% which is a 10% improvement over DSR.

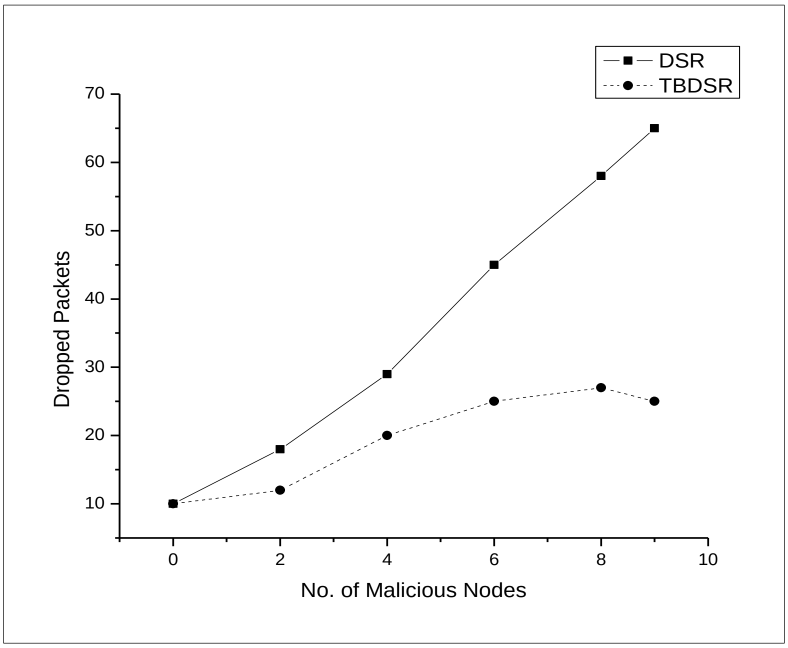

Figure 5.3: Packet Dropped

In this simulation packet dropped by grayhole node is calculated. Here also when there is no grayhole node packets dropped were very few, but as the malicious node increases, percentage of packet drop is very high in DSR as compared to TBDSR. The simulation result shows that the proposed TBDSR can prevent packet dropping at a great since the routing take place via secured and trusted node.

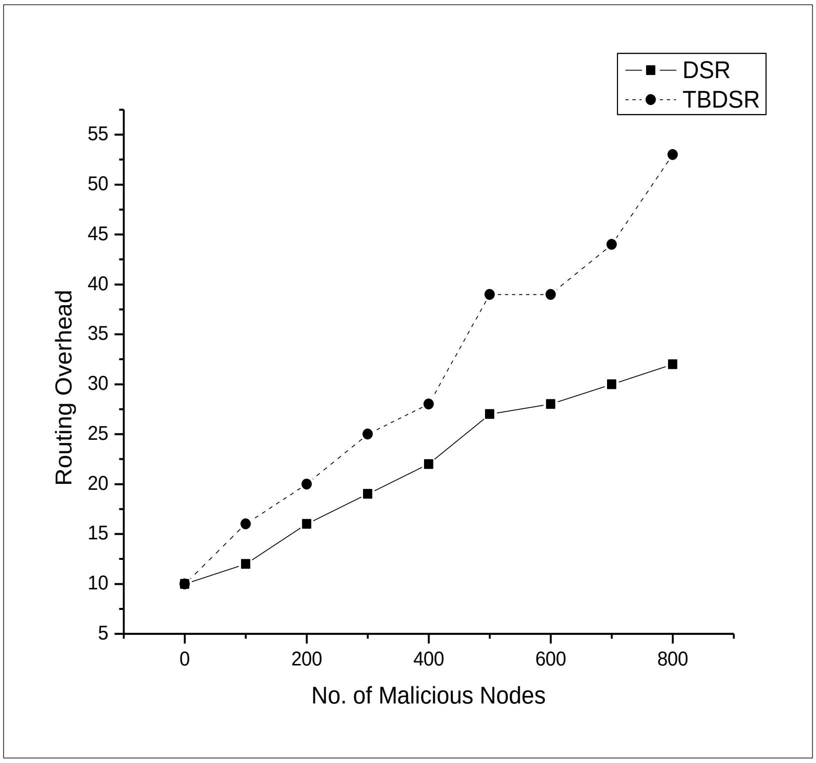

Figure 5.4: Routing Overhead

In this simulation experiment routing overhead is measured for both DSR and TBDSR. When grayhole node presents in the network all the attacking nodes participate in the routing process and forward some packets. Since in TBDSR routing is done through trusted node, routing overhead is higher than DSR.

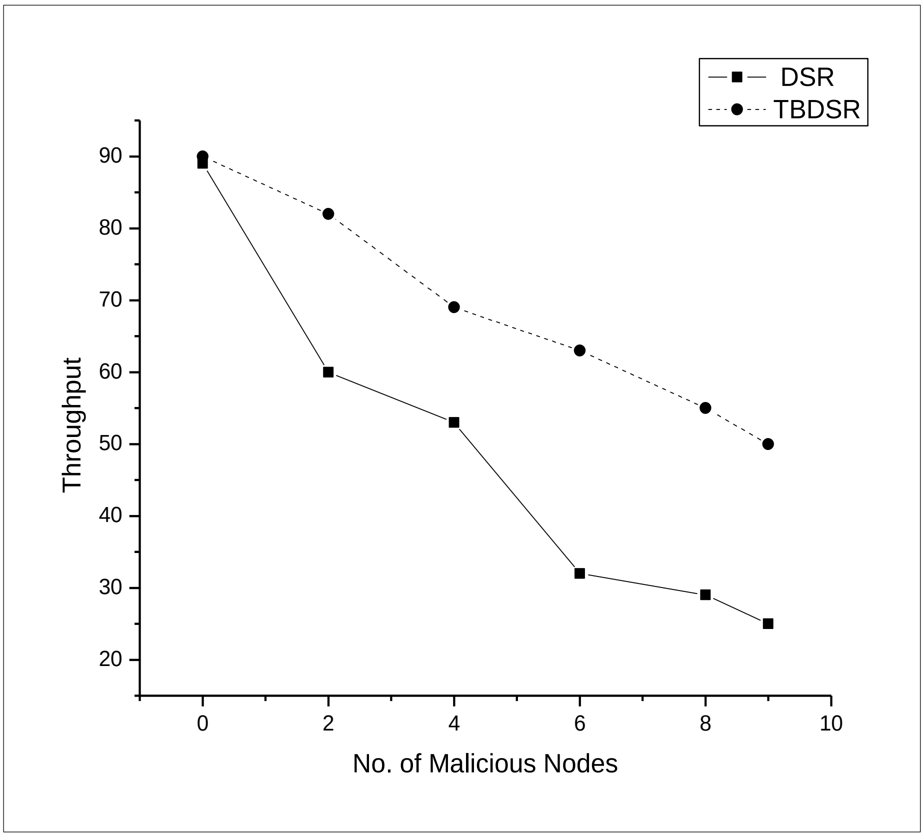

Figure 5.5: Throughput

Finally the simulation result shows the throughput of the DSR and TBDSR protocol in presence of the grayhole malicious node. The simulation result shows that when there is no malicious node the throughput were more than 90% both for DSR and TBDSR. But at 20 % of grayhole node the throughput for TBDSR is 80% while for DSR it is 60%. When grayhole node is 60%, the throughput for DSR is only 25% and for TBDSR is 62%, which is 37% improvement over DSR.

5.6 Chapter Summary

This chapter discussed about a security solution of grayhole attack in mobile environment. The performance of the proposed technique is evaluated with respect to routing overhead, PDR, dropping nodes and throughput. The performance matrix shows a reasonable outcome. In future more improved trust based security protocol may be designed to secure the network from various kind of attack and same can be implemented for other protocol also. Also the work can be tested using test bed.