ISSN:0975-9646

TRAODV: Trusted and Robust Adhoc On demand Distance Vector Routing in MANET

Ravindra J. Mandale[#1], Dadaso T. Mane[*2]

[#1]*Computer Science & Engineering Department, RIT, Islampur Maharashtra, India*

[*2]*Information Technology Department, RIT, Islampur Maharashtra, India*

***Abstract*— Mobile Ad hoc Network (MANET) is a collection of wireless mobile nodes forming temporary network without having central authority. As there is no central administrator for monitoring the network, every node should collaborate with each other to provide the services of the network to users. Unfortunately this assumption is not always true because of resource constraints to nodes. Hence this results in misbehaviour and selfish behaviour from nodes in MANET. Therefore there is important need of trust among the nodes participating in the network activity. We used Trust Based Malicious Node Detection (TBMND) model for evaluating trust of all nodes in MANET. We presented simulation results in terms of comparison which shows Ad hoc On Demand distance Vector routing (AODV) protocol with and without TBMND trust model. TBMND is able to detect and subsequently isolate the untrustworthy nodes from the network which leads to better packet delivery ratio and throughput.**

***Keywords*— MANET, Routing Security, Trust model, AODV.**

I. INTRODUCTION

In the current age of research, mobile computing is increasingly in popular today. Now a day everywhere we found applications of MANET such as for search and rescue operations, conference meetings, disaster recoveries, wireless sensor networks, etc. MANET comprising different wireless mobile nodes which are communicating with each other to form network. MANET does not have permanent infrastructure therefore it is called as infrastructure-less network [1]. Infrastructure less networks has no fixed routers; all nodes are capable of movement and can be connected dynamically in an arbitrary manner. Nodes of these networks function as routers which discover and maintain routes to other nodes in the network.

In MANET, the goal of routing protocols is to find stable and valid route to the destination. To perform route discovery, the routing algorithm must obey QoS requirements while optimizing the network performance. Even though nodes do not have prior knowledge about network topology, they need to find routes between source and destination. Mobile nodes doing communication in MANET face many attacks which include denial of service, packet delay, packet modification, packet dropping, and spoofing, etc. In order to combat such attacks, MANET protocols must meet necessary security goals. The goal of the security solutions for MANET is to provide security requirements such as Data confidentiality, data integrity, authentication, availability, non-repudiation and access control [2].

The rest part of the paper is planned as follows: Section II discusses about existing trust management frameworks proposed by various researchers in the area of MANET security. The TBMND trust model is given in section III. Section IV presents modification done on top of AODV. Section V presents simulation results and analysis of proposed model. Finally, conclusion and future work is given in section VI.

II. RELATED WORK AND MOTIVATION

Now a day, trust management is one of popular concept in the era of MANET. Trust and belief are social concepts and they are interchangeably used in the MANET. This section discusses about different frameworks proposed by various researcher in the field of trust management in MANET.

Hui Xia et al. [3] proposed novel trust model called trusted source routing (TSR) which uses nodes historical trust and logic rules prediction method. This model penalizes malicious nodes which are present in the black list by isolating or denying the network services.

Akshai et al. [4] presented Trust Based Secure (TSDRP) model by modifying AODV routing protocol. This model helps to provide security from Blackhole and DoS attacks based on the trust value computed by each node. TSDRP has three modules Direct which are Observation, Promiscuous Mode Observation and Trust Module for Secure Route Discovery Establishment, its Maintenance and Attack Prevention.

Kung Wang et al. [5] proposed Secure Trust-based Location Aided Routing (ST-LAR) algorithm which uses direct and recommendation trust to isolate malicious nodes or untrustworthy nodes. They compared ST-LAR with Distance-Based LAR (DB-LAR) model and received satisfactory PDR and delay. Here, in ST-LAR model, each node maintains LIT (Location Information Table), including an *IC* (Index Counter) item to record the various number of location information This *IC* item can verify the real-time performance of location information.

Antesar M. Shabut et al. [6] proposed friendship based trust model which introduces the concept of degrees of trustworthiness or friendship eg. Stranger, Acquain, friend, misbehave and redemp. The proposed model is divided in four parts such as evidence manager, trust manager, policy and evaluation manager.

Many researchers proposed different frameworks to maintain trust among the nodes present in the network. Despite of this, there are some pitfalls in each framework. The model from this paper concentrates on node and route trust calculation and based on trust value computed by source, it will choose trustworthy route and subsequently avoid untrustworthy nodes.

III. TRUST BASED MALICIOUS NODE DETECTION IN MANET

We used trust model from [7] which is normalized to compute trust value of each node participating in network activity.

Trust vector computation:

Following formula calculates final trust value of node based on evaluated experience, knowledge and recommendation. This trust value ranges from 0 to 1.

$$_AT_B = W1 *\ _AEXP_B + W2 *\ _AKNW_B + W3 *\ _AREC_B$$

```
void  normalize(double w1,double w2,double w3)

 {
   for ( int i = 0; i < count; i++)
     {
      trust_vector[i] = w1 * exp[i] + w2 * knwl [i] + w3 *
recom [i];
     }
}
```

Where W1=0.4, W2=0.2 and W3=0.4 are weightages assigned for experience, knowledge and recommendation respectively.

Experience:

The experience is calculated directly by observing the data packet forwarding behaviour of a node by other node. This experience value ranges between 0 and 1.

Experience is calculated is as follows:

$$_AEXP_B = \frac{\bar{P}_B}{P_B}$$

Where $_AEXP_B$ is node A's experience about node B. $\bar{P}_B$ is the number of data packets successfully forwarded to all nodes except node A and P_B is the number of packets received from all nodes for forwarding purpose except from node A.

```
double  exp = double (pkts_out_[index] - node_pkts_out
[nb -> nb_addr]) / double (pkts_in_[index] - node_pkts_in
[nb->nb_addr]);
```

Knowledge:

The knowledge is MAC layer's link quality between node A and B on physical layer. This knowledge value ranges from 0 to 1.

Knowledge is calculated is as follows:

$$_AKNW_B = (1 - P_{A,B}) * (1 - P_{B,A})$$

Where $_AKNW_B$ is node A's knowledge about node B.

```
MobileNode* n_ = (MobileNode*)
Node::get_node_by_address(nb->nb_addr);
double p_a_b = absol((node_pkts_out[nb->nb_addr] - n_-
>pkts_out[nb->nb_addr]));
double p_b_a = absol((node_pkts_in[nb->nb_addr] - n_-
>pkts_in[nb->nb_addr]));

        double  knwl = (1 - p_a_b) * (1 - p_b_a);
```

Recommendation:

The recommendation means the opinion about a particular node by other node. Recommendation is not only associated with the neighbour node but also non-neighbour node. Consider there are three nodes A, B and C. Here, node B and node C are neighbours of node A. Recommendation is calculated is as follows:

$$_AEXP_B = \frac{\sum_0^n {}_AT_B * {}_BT_C}{\sum_0^n {}_AT_C}$$

Where $_AREC_B$ is node A's evaluation of recommendation to node B by collecting opinion from other nodes. Where n is the number of neighbour nodes. This recommendation value ranges from 0 to 1.

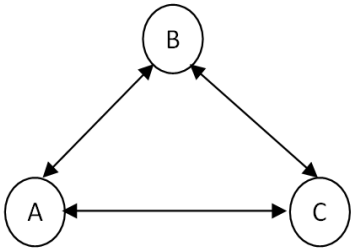

Fig.1 Recommendation trust

Suppose node A calculates direct trust value of node B, node B calculates direct trust value of node C. If node A want to evaluate recommendation of node B then A ask node C to give calculated trust of node B to him. Also collect trust value from other node which are neighbour of node A as well as node A. By using equation 4, node A calculates recommendation of node B.

Trust robustness:

As the trust value is dynamic it is not constant. It changes over time, so we need to update trust value of node at a regular interval so that we can get fresh trust values of the nodes in the network and we can perform the actions accordingly. Otherwise because of stale trust values there are many chances of misbehaviour.

IV. TRADITIONAL AODV AND MODIFICATION IN AODV

This section covers traditional AODV and modification which have been done in AODV.

Traditional AODV:

In traditional AODV [8], two phases are involved: route discovery and route maintenance. Route discovery phase is initiated only when source node wants to send data packets to the destination and at the same time it does not

have valid route to the destination. At first, Source broadcasts Route Request (RREQ) packet to their neighbours. If neighbour is having route to destination then it replies Route Reply (RREP) packet to source otherwise rebroadcasts RREQ packet to their neighbours. This process continues till it reaches to the desired destination or the intermediate node having fresh route to the destination. If destination arrives RREQ packet, it send RREP packet back to source in the reverse path. Based on minimum hop count between source and destination, source selects a route among the routes available to destination. Finally, source uses this route for future data delivery. If there is any link failure between two nodes then corresponding node sends RERR packets to source node and that route entry is deleted from routing table. Sometimes if link failure closer to destination is happen then local repair is attempted otherwise source perform new route discovery.

Modification in AODV:

Data structures of node:

i) Node trust table: This table is maintained by each node in the network. This comprises node id, experience, knowledge, recommendation and trust vector values of all nodes in the network. This trust value will be useful in future for selecting trustworthy nodes that is source will decide to whom he should forward packets and from whom he should accept packets. It is shown in figure 2.

Node id	*Experience*	*Knowledge*	*Recommendation*	*Trust vector*
1	*0.4*	*0.5*	*0.3*	*0.38*
..	..	..	..	..

Fig.2 Fields in a Node trust table

ii) Modified Routing table: This table is maintained by all nodes in the network based on their participation in the route discovery activity. This table comprises destination IP, sequence number, hop count, next hop, lifetime value and route trust. This route trust value ranges between 0 to 1 and it is useful while selecting trustworthy route from available routes in the routing table. It is shown in figure 3.

Destination IP address	*Current sequence number*	*Hop count to the destination*	*Next hop towards the destination*	*lifetime value*	*Route Trust*
--	--	--	--	--	--

Fig.3 Fields in a Routing table

V. SIMULATION RESULTS AND DISCUSSION

i) Simulation environment

We formed simulation environment using popular discrete event simulator NS2.35.The simulation parameters are listed in Table 1. Also some of the node attributes are presented in Table 2. We used Random waypoint mobility (RWPM) model to determine the node mobility and its related attributes. In RWPM model, each node selects random destination and travels towards that destination with some uniform speed. Once it reaches to selected destination it waits for defined pause time. When this pause time finished, again it selects next random destination. This procedure is repeated until it reaches the desired destination specified by user [8].

Table 1 Simulation parameters

Name	Values
Simulation area	1000m x 1000m
Simulation time	200 seconds
Mobility model	Random Waypoint
Number of nodes	50
Transmission range	250m
Traffic type	CBR
Transport agent	UDP
Packet size	512 bytes
Packet Interval	0.1 second
Pause time	10 seconds

Table 2 Node attributes

Name	Values
Link layer protocol	LL
MAC layer protocol	802.11
Interface queue type	DropTail/PriQueue
Buffer length	50 packets
Antenna type	Omni directional
Radio propagation model	Two Ray Ground
Channel type	Wireless
Initial energy	200 joules
Transmission power	0.02 watts
Receiving power	0.01 watts
agentTrace	ON
routerTrace	ON
macTrace	OFF

ii) Simulation results and analysis

Figure 4. indicates scenario using NAM tool of NS2 in which source and destination node colored in blue, malicious nodes colored in Red and link failure between corresponding nodes colored in black.

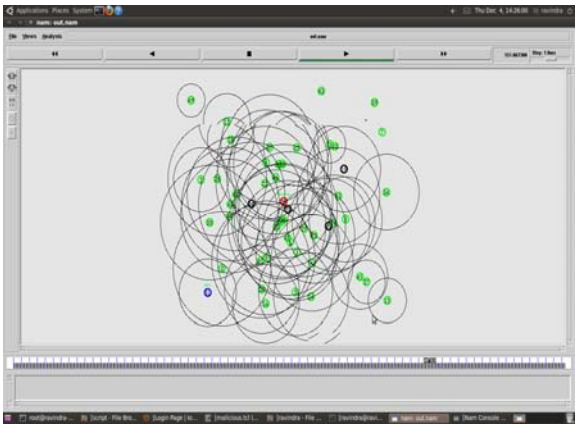

Fig. 4. Scenario with 50 nodes and showing malicious node detection coloring in RED

Here in following part of this section, we presented our simulation results with TRAODV and without TBMND algorithm. We used following four metrics to test the performance of TBMND model for MANET.

- **Performance metrics [8]:**
- **Packet Delivery Ratio (PDR):**

It is the ratio of number of data packets successfully reached to the destination and the number of packets sent by source node.

- **End to end delay:**

The average time taken by data packets to reach the destination after it leaves from the source node.

- **Network Throughput :**

The average number of bits transmitted per second from source to destination in the network.

- **Routing overhead:**

It is the total numbers of routing packets generated in the network during simulation time.

- **Performance tests:**

We tested the performance of TBMND by following two tests.

Varying node speeds: We did different tests by varying node mobility for all nodes from 10 m/s to 30m/s.

Figure 5 depicts packet delivery ratio comparison with node mobility. Here TRAODV with detection received better packet delivery ratio as we increase speed of nodes against TRAODV without malicious node detection. We conclude that TRAODV detects malicious nodes successfully and takes subsequent action on them. Simply it penalizes these malicious nodes by isolating and does not allow nodes in participating to the network in near future.

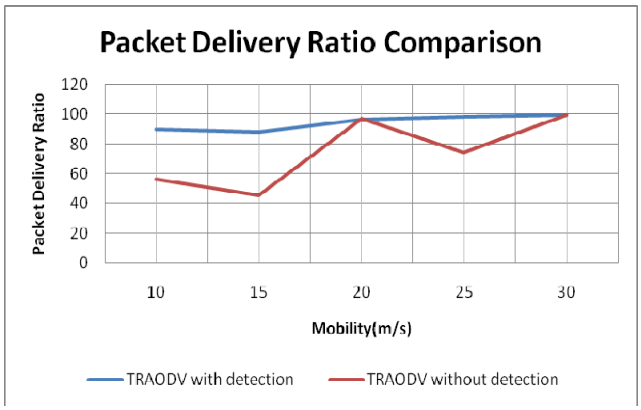

Fig. 5 PDR versus Node Mobility

Figure 6 shows the comparison of end to end delay taken by TRAODV while and without detection of malicious nodes by varying node mobility. Here, TRAODV with detection takes less delay to reach the data packets to the destination than TRAODV without detection of malicious nodes. We observed that by embedding some techniques in protocol, it does take more delay. However, this is not the case with our model.

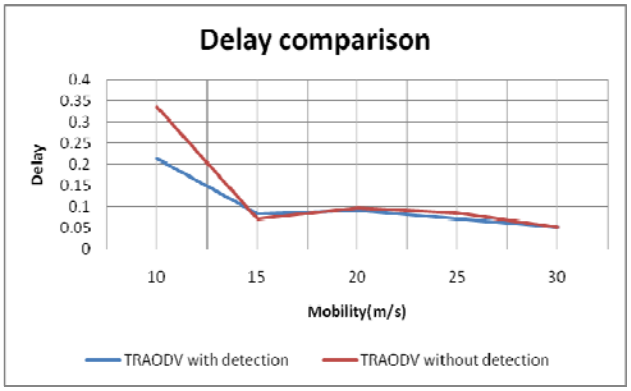

Fig. 6 End to End delay versus Node Mobility

Figure 7 indicates the throughput comparison with node mobility. As we received good packet delivery ratio, we received same kind of results with throughput because packet delivery ratio is directly proportional to throughput of the network.

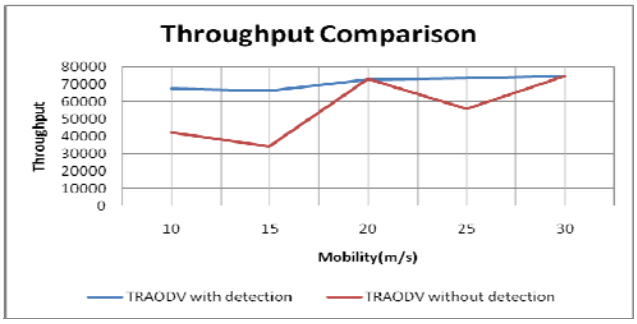

Fig. 7 Throughput versus Node Mobility

Figure 8. Shows routing overhead comparison with node mobility. Here total number of routing packets generated in the network with detection mechanism is more than without detection for TRAODV.

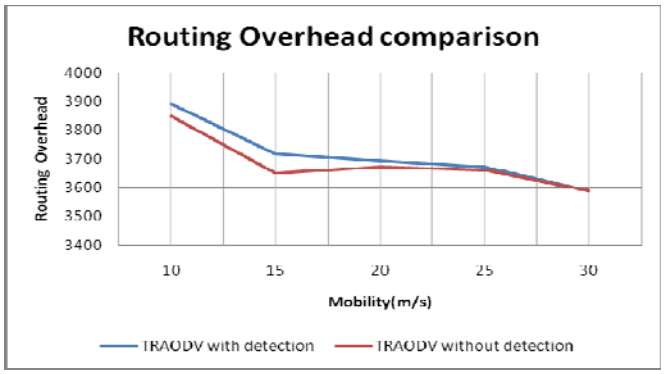

Fig. 8 Routing overhead versus Node Mobility

i) Varying number of malicious nodes:

We did different tests by varying count of malicious nodes in the network with an increment of one node from 0 to 5 nodes. Figure 9 depicts the comparison of packet delivery ratio and number of malicious nodes. Even in the presence of malicious nodes TRAODV with detection gives good packet delivery ratio as compare to TRAODV without detection of malicious

nodes. When we increase the number of malicious nodes in the network, our model first detects those nodes and does not allow such nodes for any kind of network services eg. Forwarding, receiving packets, etc.

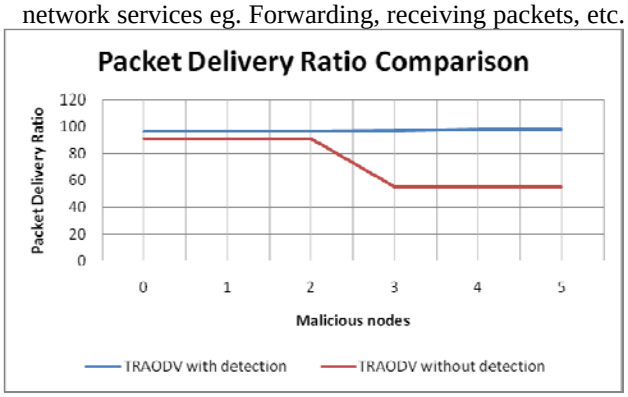

Fig. 9 PDR versus Number of malicious nodes

Figure 10 depicts the delay and number of malicious nodes comparison for TRAODV with and without detection. Here TRAODV with detection takes somewhat more delay for taking action on malicious nodes. Hence there is more delay for TRAODV with detection than without detection.

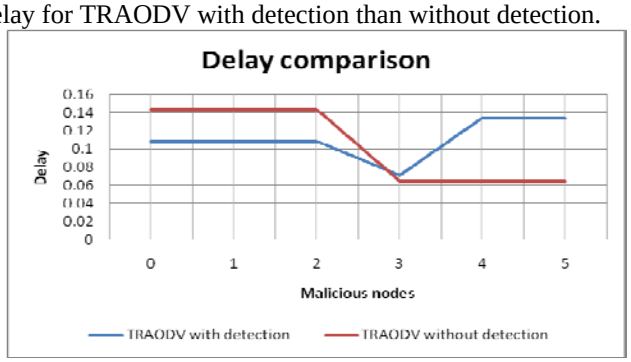

Fig. 10 End to End delay versus Number of malicious nodes

Figure 11 shows the throughput comparison for TRAODV with and without detection by varying number of malicious nodes. We received high throughput for TRAODV while detecting the malicious nodes in the network. For any network, reliability is depends on throughput achieved.

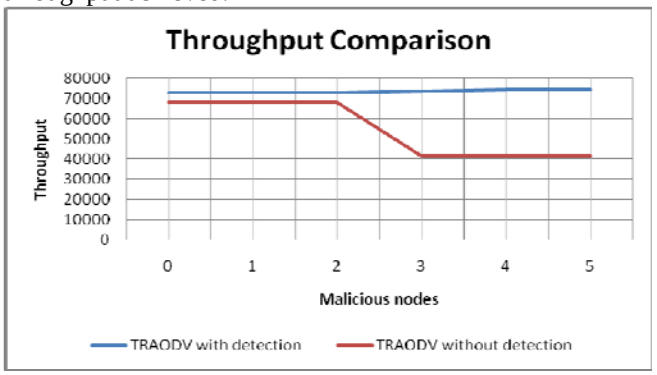

Fig. 11 Throughput versus Number of malicious nodes

Figure 12 depicts the number of routing packets generated in the network by varying number of malicious nodes in the network. Although the routing packets generated are more for TRAODV with detection than without detection, we received positive PDR, throughput and delay.

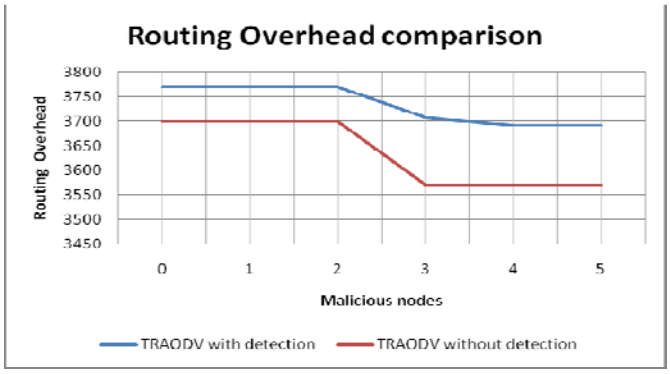

Fig. 12 Routing overhead versus Number of malicious nodes

VI. CONCLUSIONS

Trust is now became an important concept in the security of MANET. The implemented trust model is able to detect malicious nodes based on trust value and takes actions on them. This reduces packet dropping ratio and improves throughput of the network. Also because of trust decay function robust trust value of each node is maintained with source node so that it will not face the problem of distrust after some interval. Also we successfully detected packet dropping attack and analyse the performance of model. In future work, we will concentrate on overhead issue of nodes for calculating trust value in the trust management frameworks. With this minimal overhead, we can get trust value of all nodes participating in the route and we can perform the task with trustworthy nodes only.

REFERENCES

[1]. Asma Adnane, Christophe Bidan, Rafael Timóteo de Sousa Júnior, Trust-based security for the OLSR routing protocol, Computer Communications, Volume 36, Issues 10–11, June 2013.

[2]. BY XU LI, AMIYA NAYAK, ISABELLE RYL, DAVID SIMPLOT AND IVAN STOJMENOVIC , “SECURE MOBILE AD HOC ROUTING ”, IEEE 2007.

[3]. Hui Xia, Zhiping Jia, Xin Li, Lei Ju, Edwin H.-M. Sha, Trust prediction and trust-based source routing in mobile ad hoc networks, Ad Hoc Networks, Volume 11, Issue 7, September 2013.

[4]. Aggarwal, A.; Gandhi, S.; Chaubey, N.; Jani, K.A., "Trust Based Secure on Demand Routing Protocol (TSDRP) for MANETs," *Advanced Computing & Communication Technologies (ACCT), 2014 Fourth International Conference on* , vol., no., pp.432,438, 8-9 Feb. 2014.

[5]. Kun Wang; Meng Wu; Pengrui Xia; Subin Shen, "A Secure Trust-based Location-Aided Routing for Ad Hoc networks," *Communications and Networking in China, 2008. ChinaCom 2008. Third International Conference on* , vol., no., pp.835,839, 25-27 Aug. 2008.

[6]. Shabut, A.M.; Dahal, K.; Awan, I., "Friendship Based Trust Model to Secure Routing Protocols in Mobile Ad Hoc Networks," *Future Internet of Things and Cloud (FiCloud), 2014 International Conference on* , vol., no., pp.280,287, 27-29 Aug. 2014.

[7]. Wei Gong;Zhiyang You; Danning Chen; Xibin Zhao; Ming Gu; wok-Yan Lam; ,"Trust Based Malicious Nodes Detection in MANET," E-Business and Information System Security, 2009. EBISS ’09. International Conference on , vol., no., pp.1-4, 23-24 May 2009.

[8]. Ravindra J. Mandale, Sandeep A.Thorat, “A Novel Trust Model with Reduced Computation and Communication Overhead in MANET, 2013 Advanced Research in Engineering and Technology, Vol. 7, pp. 260 – 266, Elsevier 2013.