Journal of Theoretical and Applied Information Technology
10th November 2014. Vol. 69 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

TRUST MODEL BASED ON BAYESIAN STATISTICAL METHOD FOR AOMDV IN MANET

[1]Mrs.S.GEETHA, [2]Dr.G.GEETHA RAMANI
[1]Asst. Prof., Department of Computer Applications, Tiruchirappalli, India
[2]Asst. Prof(SG)., Department of Mathematics, Tiruchirappalli, India
E-mail: [1]kasagee1971@yahoo.co.in, [2]geeramdgl@rediffmail.com

ABSTRACT

Mobile Ad Hoc Networks (MANETs) present a dynamic environment in which data can exchange without help of a centralized server , provided that nodes cooperate with neighbor nodes for routing. In this environment, the security of data established route to its destination is a challenging issue in the existence of malevolent nodes. This paper proposes a data security approach in MANETs that uses a trust based multipath AOMDV routing combined with Bayesian statistical method called Trust based adhoc multipath distance vector (TB-AOMDV) protocol. This protocol is also capable to discover multiple loop-free paths in route discovery. These routes are evaluated by three aspects: hop counts and route trust and node trust values. Furthermore, the routing protocol describe the procedures for identification of the trusted routes and. Simulation results show that TB-AOMDV improves packet delivery ratio, end-to-end delay, packet overhead when compared to the AOMDV.

Keywords: MANETs, Data Security, TB-AOMDV, *Packet Delivery Ratio, End-To-End Delay, Packet Overhead*

1. INTRODUCTION

The past decade has witnessed the emergence of mobile ad hoc network (MANET). Routing security problems in MANETs have hindered the development and deployment of these networks. It is a set of limited range wireless nodes, which works well only if those mobile nodes are trusty and behave cooperatively. However, MANETs are subjected to a variety of attacks by malicious nodes and selfish nodes. Selfish nodes deny relaying the attacks of other nodes, and malicious nodes disturb the network. Several attacks, such as man-in-the-middle, black hole, and DoS, may target a MANET. MANETs often suffer from attacks by malicious nodes. These attacks range from naive passive eavesdropping to vicious battery draining attacks. MANETs can be characterized by the types of attackers. External attackers attempt to disrupt the network by injecting erroneous routing information. They create routing loops or other non-functional routes, or attempt to partition the network by creating a wormhole. External attackers may also replay old routing information or modify route information being transmitted between nodes. Internal attackers are nodes that have been compromised by malicious parties. Trust has been recently introduced in solving this problem and is used in existing protocols for ad hoc networks to improve security. There is a common assumption among routing protocols and applications for ad hoc networks that all nodes are trustworthy and cooperative and all nodes behave in accordance with the defined specifications of such protocols and applications.

The proposed trust model calculates the trust value for the nodes in the network based on the packet forwarding ratio and gives incentives and penalties for the nodes based on their past history in the network. Weights are assigned for each method and the trust value is computed for each node. The link between two trusted nodes is established based on the Bayesian network mathematical formula.

The remaining paper is organized as follows. Section 2discusses the literature work. In Section 3, we describe our trust model based on the Bayesian network in detail. Based on the trust model, in Section 4, we propose a novel on-demand routing protocol, the Trust with Bayesian based AOMDV (TB-AOMDV). Section 5 presents the experiments and analysis on the performance of the protocol. Finally, Section6 gives the concluding remarks

2. LITERATURE SURVEY

Diego Gambetta [1] states that trust is a level of likelihood that an agent will perform a certain action before the action can be monitored. It takes trust as a function of uncertainty over a relationship between two entities for certain action according to the previous information. A trust based cooperation model is used to prevent false trust fluctuation and balance the network load result in successful transmission rate.

From the evolutionism and sociology point of view, Mui[2]et al. firstly introduced a trust and reputation computation model for generalized networks. In the indirect trust evaluation process, they proposed a graph parallelization algorithm, which is intuitive and easy to understand. Based on the work of Mui, Durad et al . introduced a new term: trust of scaling factor (TSF2) [3], emphasizing the contribution of direct interactions and the rationality of recommendation. They also proposed a modified transformation algorithm (MTA) for TSF2 calculation.

In the model established by Sun et al. [4,5], trust is measured by entropy. They introduced an entropy function to represent the trust value between two nodes, which really captured the dynamic nature of trust evidence. To compute the indirect trust value, Sun's model used trust value iteration techniques considering multilevel directed graph. When more nodes involved, the convergence speed of this method is exponentially slow, and its scalability becomes an issue.

Luo and Fan [6,7] proposed a subjective trust management model based on certainty-factor for MANETs (CFStrust) after considering fuzzy set theory and reputation model, which can be used to quantify and evaluate the nodes' credibility. In this model, the problem of trust management is modeled by fuzzy likelihood estimation and confidence estimation. The trust evaluation mechanism and the derivation rules of recommendation trust relationship are given in this model.

Liu et al. proposed a trust model for mobile ad hoc networks which uses both cryptography and trust [8]. In this model, each node is initially assigned a trust level. The concepts discussed in this paper are generic and do not rely on centralized control, key distribution protocols, or any particular routing protocol. They can therefore be easily integrated into the current routing protocols used in mobile adhoc networks.

In the opinion of Pirzada and McDonald [9,10], the reliance on a central entity is against the very nature of mobile adhoc networks, which are supposed to be improvised and spontaneous. They presented a trust-based model for communication in pure mobile ad hoc networks that is based on individual experience rather than on a third party advocating trust levels. The model introduces the notion of belief and provides a dynamic measure of reliability and trustworthiness in this network. They also proposed an aggregation mechanism, where nodes calculate trust according to multiple observed events including acknowledgments ,packet precision, gratuitous route replies, and blacklists.

In the TDSR [11] model, trust among nodes is calculated as a combination of direct trust and indirect trust. The direct trust score is modified when misbehavior has occurred by a number of times exceeding a threshold. The indirect trust score is modified when a node receives a message reported by neighbor nodes. If the trust score of a node in the table has deteriorated so much as to fall out of a tolerable range. Such nodes are added to the blacklist. In the route Discovery phase, when node A sends a RREQ packet to node B, B looks up its blacklist to find whether the node A is in it. If not, it forwards the packet.

Wang et al. [12] have also proposed a Routing Algorithm based on Trust. The trust value of a node is computed and updated by trust agents that reside on network nodes [13]. They have assumed that the trust values of all nodes are stored at each node in advance. Trust for the route is calculated at the source node based on the weight and trust values are assigned to the nodes involved in the route at the source node. Weights are assigned by the source node as 0 or 1. The node having the minimum trust in the route is assigned weight as 1 and all the other nodes as 0.

P. Narula et al. [14] proposed a novel method for message security using trust-based multi-path routing. The Pizarda model [15,16] is used for assigning trust levels to the nodes in the network.

The trust level is assigned in discrete form, from -1 to 4, which signify complete distrust to complete trust. The paths between the source and destination are found using DSR. The trust levels assigned to the nodes are used to define the maximum number of packets which can be routed via these nodes. Nodes having lower trust values are given lesser number of encrypted parts of a message, making it difficult for malicious nodes to access the information in the message. A node with trust level 0 is not given any message and all the packets received from a node having trust level as -1 are dropped. A node with trust level 4 can read the message.

3. TRUST MODEL BASED ON BAYESIAN STATISTICAL METHOD

The trust model calculates the trust value of a node based on their history of behaviors. The factors used to calculate the trust values are

1.Forwarding Ratio
2. Incentives and Penalties

3.1 Forwarding Ratio

It is the ratio of number of packets forwarded correctly, to the number of packets to be forwarded. If a malicious node forwards a data packet after tampering with data. It will not be considered as correct forwarding. The forwarding ratio of this neighbor node decreases when this illegal modification is monitored by the sender.

$$F(t) = \frac{N_{cor}(t)}{N_{all}(t)}$$

When $N_{cor}(t)$ means the cumulative count of correct forwarding packets and $N_{all}(t)$ means the total count of all requesting packets from time 0 to t. Based on the above formula all packets may be divided into two types namely control packets and data packets. Forwarding Ratio is again divided into two parts CFR and DFR. CFR means count the number of forwarding control packets and DFR computes data forwarding ratio. The trust information of CFR and DFR is given by the trust record list whichcontains monitored node ID,node's trust value, two integer counters of $N_{cor}$and$N_{all}$for control packets and data packets and a packet buffer. The packet buffer is used to record all packets sent recently.

By this method a node can identify whether the packet has been sent to its neighbor is forwarded or not. Using this method, before sending a packet a sender increases N_{all} by 1 for data or control packets. For a broadcast packet including a route request packet or a route update packet, the sender increases N_{all} for control packets of all records in its trust record list except N_{all} for control packets of the node where the packet comes from. To detect whether a packet is successfully forwarded, the sender will not delete the packet immediately after sent out. The packet will be stored in the packet buffer and wait for acknowledgement.

At time t, the trust value of node v_J evaluated by node v_i is calculated by this formula

$$X = w1 \text{ x } CFR_{ij}(t) + w2 \text{ x } DFR_{ij}(t)$$

Where $CFR_{ij}(t)$ and $DFR_{ij}(t)$ represent control packet forwarding ratio and data packet forwarding ratio respectively. using the timestamp mechanism to analyze each interval t=30 milliseconds data to be sent is forwarded.

3.2. Incentives And Penalties

3.2.1 Incentive:

Incentives for the nodes are given based on their capability to transmit packets within the stipulated time. The nodes should forward packets within 30 milliseconds or else there will not be any incentive for the nodes. If the given packets are sent within 15 milliseconds the incentive is .2 otherwise .1

The incentives are as follows

$0<=t<=15$, i=.2
$15<t<=30$, i=.1 $t>30$,
there will not be any incentive .

These incentives are proportional to the nodes distance from the destination, incentives are given to the successive node by their neighbors .The incentives will be calculated by

$I= r \text{ x } {}^{i}\!/\!_{H}$ H is the distance of the node from destination node in terms of number of hops.

3.2.2. Penalties

When the packet is not forwarded within 30 milliseconds then gives penalty. The penalty factor(P) is determined in 2 ways i) if data is not sent with in 60 milliseconds the penalty P=.1 ii) If

data is not sent within 90 milliseconds P=.2 .These penalties are proportional to the nodes distance from the destination.
The Penalties will be calculated by

P=r x $^{p}/_{H}$ H is the distance of the node from the destination node interms of number of hops.

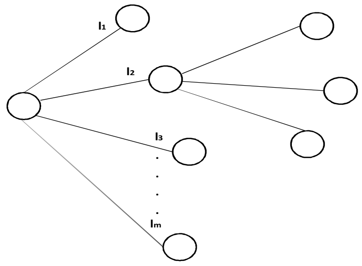
Then to find the trust value

$$\text{IP(t)} = \frac{X[i]+X[p]}{2}$$

3.3.Bayesian Statistical Method

3.3.1. Bayesian statistical method for linking two trusted nodes

For the v_j node contains m links to the neighboring nodes, to establish the link between two trusted nodes.



l_j - linksbetween two trusted nodes

E_{Vj} theevent , E_{Vj} node is trusted among the neighbor nodes.

E_{li}^{Vj} the node has V_i^{th} link of the j^{th}trusted node.

p_i^j = p(E_{li}^{Vj}), p_j = p(E_{Vj}) are the probabilities of E_{li}^{Vj} and event E_{Vj}

f_i^j the probability density of the random variable L_i^j which represents the p_i^j ’s variations

f_B and H_B the probability density and distribution function of the random variable B_j which represents the p_j variations

$f_{1,2,........bj}$ the probability density of the l_j tuples (L_1^j , L_2^j , ... L_{lj}^j)

The j^{th}trusted nodes if and only if atleast one link is operational, so

p_j = p(E_{Vj})

=p(atleast one of links constituting the link is operational)

=1-p(none of the links constituting link is operational)

$$=1-\prod_{i=1}^{lm} (1\text{-p}(V_i^{th} \text{ link of the } j^{th} \text{ trusted node})$$

$$=1-\prod_{i=1}^{lm} (1-p_i^j)$$

So we have

$$B_j = 1-\prod_{i=1}^{lm} (1-L_i^j)$$

H $_{\text{Bj}}$ (z) = p(Bj$\leq$ z)

$$=\text{p}(1-\prod_{i=1}^{lm} (1-L_i^j) \leq z)$$

$$=\text{p}(-\prod_{i=1}^{lm} (1-L_i^j) \leq z\text{-}1)$$

$$=\text{p}(\prod_{i=1}^{lm} (1-L_i^j) \geq 1\text{-}z)$$

$$=\text{p}((1-L_1^j) \,.\,.\,.\,.\,.\,.\,.\,.\, (1-L_{lm}^j) \geq 1\text{-}z)$$

To find the neighboring nodes using $f_{1-L_i^j}$ we obtain

$$\int_{\{(x1,xlj)/(1-x1)\ldots(1-xlj)\geq 1-z} \text{f}\, L_i^j \; (1\text{-x}_1) \,.\,.\, (1\text{-}_{\text{xlj}}) \; \text{dx}_1 \,.\,.\,.\text{dx}_{\text{lj}}$$

and distribute to the trusted nodes,

$\text{f}_{\text{lj}} = \text{H}_{\text{lj}}$ (z)

3.3.2. Bayesian statistical model for Routetrust

A route noted is composing of trusted nodes. If n_r is the trusted node number.

p(Route) = p(the n_r trusted nodes are moving)

$$\text{p}_r = \prod_{i=1}^{nr+1} \text{p}(i^{th} \text{ link of } j^{th} \text{ trust neighbor}) \,.\, (1\text{-p}_1)^{\text{nr}}$$

p_r means probability of the route and p_1 means probability of the trusted node

The trusted notations are

f_{Cr} and H_{Cr} the probability density function and distributed function of the random variable C_r it represents the p_r’s variations.

B_i is the random variable it represents the p(i^{th} link of j^{th} trust neighbor)’s variations

M_1 is the random variable it represents the p_1’s variations.

Then

$$\text{C}_r = \prod_{i=1}^{nr+1} \text{B}_i \,.\, (1\text{-M}_1)^{\text{nr}}$$

And

$= \text{p}(\text{C}_r \leq \text{z})$

$$= \text{p}(\prod_{i=1}^{nr+1} \text{B}_i \,.\, (1\text{-M}_1)^{\text{nr}} \leq \text{z})$$

$$=\int \text{f}_{\text{M1}}(1\text{-y}_1) \,.\,.\,.\; \text{f}_{\text{Mnr}}(1\text{-y}_{\text{nr}}) \; \text{dy}_1 \,.\,.\,.\, \text{dy}_{\text{nr}}$$

$\text{f}_{\text{Cr}} = \text{H}_{\text{Cr}}$

4. PROPOSED TB-AOMDV ROUTING PROTOCOL

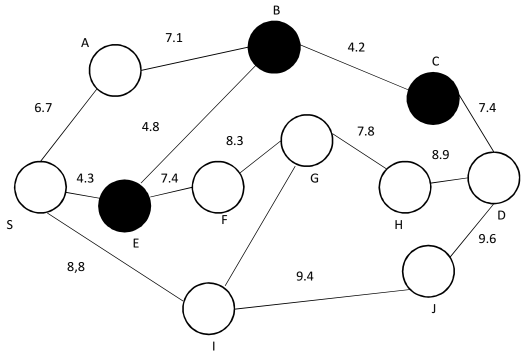


Fig1:TB-AOMDV with Malicious Nodes (E,B,C)

TB-AOMDV protocol is proposed to modify the AOMDV routing protocol with node trust and route trust value. The existing-AODV has two new control packets, namely TREQ (Trust Request) and TREP (Trust Reply). The Modified extended routing table has seven fields namely Destination IP, Destination Sequence Number, Monitored Node ID, Hop count, Next hop, Packet Buffer and Node trust.

Using this proposed method the route can be established by trust value of each node involved the route establishment process from source to destination. It is completely based on trust value of nodes. This proposed method concentrates more on the route trust value based on Bayesian approach. This route trust mechanism is used for secure and reliable route establishment. TB-AOMDV routing protocols use shortest route towards the destination to compute the best route. Which is not congested and not affected malicious or selfishness and also it is not affected physical or network layer. This method gives equal priority for both route trust and node trust for the route selection process. It requires acceptable level of changes in existing functionality of TB-AOMDV protocol to obtain secure and reliable routes and then no additional overhead in other layers.

Dest_IP	Dest_Seq_No	Monitor_Node_ID	Hop Count	Next Hop	Packet buffer	Node Trust

4.1Node Trust

Neighbor_ID	Monitor_Node_ID	Packet Buffer	Trust Value
. . . .			

Table 1: Neighbor Table

Several methods have been proposed for calculating node's trustworthiness. Different trust metrics have been evaluated to identify the node trust. In this paper, a new data structure neighbor table is introduced in each node of the MANET. All the nodes in the network environment maintain routing table before transmission of the packets. Additionally added Neighbor Table should be maintained for all the nodes for tracking the dynamically changing neighbor list and compute its corresponding node trust value. Neighbor table should maintain the fields NeighborID, Monitored Node ID, Packet buffer and Trust value. To compute Trust value based on forwarding ratio, correct packets are sent within the time interval (30 milliseconds) then given incentives otherwise penalties. The trust values for all the nodes can be combined using the determined trust level of another node.

To find the trust value of a node, weights are assigned to the trust values as given in the equation 1.

$$TV = w1\ F(t) + w2\ (IP(t)) \text{ --------------- } (1)$$

F(t) is a trust value to compute forwarding ratio method and IP(t) computes incentives and penalties method.

4.2 Route Trust

Table 2: TB-AOMDV Routing Table

The existing routing table is used to computed route trust by every node for each route. The extended routing table supports route trust calculation process.The TB-AOMDV routing table extended with two more fields namely monitored Node ID and Node trust. In this method, source node selects the route which have been highest route trust value based on Bayesian approach. In this route trust field is updated every 30 milli seconds of intervals. Destination node in each entry maintaining R-ACK message packet which have been entered into the routing table. The best route having the entry for number of packets sent to the corresponding destination. This packet moves backward direction from the destination and if create a new entry in the routing table then entered node trust value is 0. It may be changed based on the route conditions.

ORIGNATOR_ID
MONITOR_NODE_ID
DESTINATION_ID
PACKET BUFFER
NEXT HOP
HOP COUNT
TIMESTAMP

Table 3: R_ACK Message Packet

In this section, described an on-demand routing mechanism for ad hoc network based on the proposed trust model. At first, the structures of routing table and trust record list are depicted. Then, the procedures of route discovery and routing maintain are discussed. Finally a sequence number method is presented to avoid the routing loop.

4.3 Routing Table

Routing table stores the routes to various nodes in an ad hoc network. Each trusted node maintains a route trust table composed of multiple routing entries. AOMDV adopts hop-by-hop routing mechanism, in which the source should know how to get to the next hop. So when a data packet is going to a particular neighboring node, it then refers to local routing table to find the address of next hop with trust value (named node j) to the destination. Once it reaches the node j, it again refers to the j's routing table for the address of next hop which has the higher trust value and so on, until it reaches the final destination.

Destination
Sequence Number
Expiration Time
RouteList{(NextHOPtv1,Hopcount1,Routetrust1), (Nexthoptv2,Hopcount2,Routetrust2) …….}

Table4. Structure of TB-AOMDV Routing Table.

Table4. shows the structure of the routing table entry for TB-AOMDV. The routing entry consists of the following fields:

(1) Destination: the identifier of destination node.
(2) Sequence number: Packet number the greatest known sequence numbers for destination denotes freshness of routing information. It is used to avoid routing loop.
(3) Expiration Time: the time after which the route is considered to be invalid. Each time a route entry is used to transmit data from a source toward a destination, the Expiration Time for the entry is reset to the current time plus a constant (active route timeout).
(4) Next hop: The next hop, or gateway, is the address of the next station with high trust value to which the packet is to be sent on the way to the final destination.
(5) Hop Count and Route Trust: Number of hops needed to transmit the packet to the destination and route trust is the trust value of the route. Trust values of the node, hop count and route trust constitute the cost vector.

Multiple routes leading to the same destination arrange in descending order of the sumof the node's trust value and the route trust. If two routes have same value, the one with lesser hop count precedes.

4.4 Trust Record List

Table 4. Structure of a trust record Node ID, N_{cor} and N_{all} for control packets N_{cor} and N_{all} for data packets Packet Buffer to remember trust information, we introduce a trust record list. Each node will also maintain a trust record for every neighbor which has been sent packets to for forwarding. A trust record listed in Table 4 comprises a node ID, two integer counters of N_{cor} and N_{all} for control packets, two integer counters of N_{cor} and N_{all} for data packets, and a packet buffer. The packet buffer is used to record all packets sent recently. It is a circular buffer, which means that the buffer will cycle and overwrite the oldest packet if it is not removed in time. Before sending a packet to a neighbor, the sender looks up the trust record corresponding to the neighbor and increases N_{cor} of CFR (the packet is a unicast control packet) or N_{all} of DFR (the packet is a data packet) by 1. To detect whether a packet is successfully forwarded, the packet will not delete immediately after being sent. Then it will be stored in the packet buffer and wait for acknowledgment. If the packet is forwarded

correctly, it will be removed from the packet buffer and the corresponding counter of correct forwarding increases 1. If the packet is send at the time of 30 milliseconds then calculated incentive value otherwise to calculated penalty value.

4.5 Route Discovery and Route Selection

The route discovery process is initiated whenever a source node s needs to communicate with another node d for which node s has no routing information in its routing table. Every node maintains two independent counters: a node sequence number and a broadcast ID. The source node initiates a network-wide flood by broadcasting a route request (TREQ) packet and waits for a route reply (TREP) packet.

4.6. Trust Route Request

A TREQ packet contains the following fields: <BroadcastID, SourceAddr, SourceSequenceNo, DestAddr, DestSequenceNo, HopCounter, RouteTrust, NodeTrust>.

The first 6 fields including BroadcastID, SourceAddr, SourceSequenceNo, DestAddr, DestSequenceNo, and HopCounter are similar to the corresponding ones in AOMDV[14]. The major difference is two additional fields for route trust value, i.e. RouteTrust (PT) and Node Trust (NT). The PT represents the route trust value required by the data packet and is set by the source. During the flood, RT remains unchanged. The NT denotes average trust values of nodes using forwarding ratio and incentive and penalties that the TREQ has passed by during route discovery. And it is initialized to 1 by the source. During the flood, NT varies with the transmission of TREQ packet.

4.7. Route Reply

The intermediate node can reply only when it has a route with a sequence number that is greater than or equal to that contained in the TREQ. If it does have a fresh route to the destination, and if the TREQ has not been processed previously, the node unicast a route reply (TREP) packet back to its neighbor from which it received the TREQ. A TREP packet contains the following information:

<SourceAddr, SourceSequenceNo, DestAddr, DestSequenceNo, HopCounter, Timestamp, RouteTrust, NodeTrust>

The first 6 fields including SourceAddr, SourceSequenceNo, DestAddr, DestSequenceNo, HopCounter, and Timestamp are also similar to the corresponding ones in AOMDV [14]. The Route Trust (PT) and Node Trust (NT) have same meaning to the ones in TREQ. The NT in TREP denotes the minimal one of trust values of nodes that the TREP passed by during route reply. And it is initialized to 1 by the destination. If an intermediate node receives a TREQ from a neighbor, and if it has multiple routes to the destination, it will reply two copy of TREP, in which one has the smallest hop count and the other has the greatest trust value. If the destination receives multiple copies of TREQ, it will reply the first k trusted routes at most, whose route values are greater than the RouteTrust of the TREQ. After a TREQ packet arrives at a node, a reverse route is established to the source of the TREQ.

As the TREP travels back to the source, each node along the route sets up a forwarding route to the destination from which the TREP came, updates its timeout information for route entries to the source and destination, and records the latest destination sequence number for the requested destination.

4.8 Route Maintenance and Loop Freedom

The route maintenance in TB- AOMDV is similar to that in AOMDV, i.e., nodes maintain and update route table when receiving a TREQ, TREP or route error (RERR) packet. When a link failure is detected (by a link layer feedback, for example), a RERR is send back to all sources using that failed link via separately maintained predecessor links. Routes are erased by the REER along its way. When a node receives a RERR, it initiates a new route discovery to fix the link if the route is still needed. Unused routes in the routing table are expired using a timestamp technique.

When receiving a control packet such as a TREQ or TREP packet, a node may create a reverse route to the source or forward route to the destination. However a node should create or update a route on a fresh control packet not on an old control packet. The proposed protocol only allows accepting alternate routes with higher node trust and route trust with a lower hop count.

5. SIMULATION AND RESULTS

Performance of proposed trust based TB-AOMDV routing protocol is analyzed by the MATLAB. MANET environment (Table 1) is fully formed using this MATLAB. Maximum number of node is 50 and node's mobility characteristic is random movement. Routing decision in this environment is carried out by both AOMDV and Modified TB-AOMDV protocols. Finally, they are presented in the form graph for the comparison of these protocols likely end-to-end delay, throughput and packet overhead.

5.1.Simulation Parameter Value

Parameter	Setting
Terrain dimension	1000m x 1000m
Number of nodes	50~100
MAC protocol	IEEE 802.11
Mobility model	Random way point
Radio range of a node	250m
Traffic Type	CBR
Packet size	512 bytes
Data rate	10(packets/s)
Node's speed	10(m/s), 20(m/s)
Simulation Time	100 (s)
Percentage of malicious nodes	10~40% of total nodes

Table 5:Simulation Setup parameters

The performance of the TB_ AOMDV is evaluated comparing with the traditional AOMDV based on the following metrics

1. Throughput
2. End- to end delay
3. Packet Overhead.

5.2 Performance Metrics

The proposed protocols use three metrics to evaluate the performance of the routing protocols, in which the first two metrics are the most important for best trust route and transmit protocols.

5.2.1 Test 1: varying node speeds

In the first test, compare TB-AOMDV with AOMDV as the maximum speed of nodes varies from 0 to30m/s. As shown in Fig. 2, the delivery ratios of TB-AOMDV has more apparent at higher speeds compared to AOMDV. This advancement of TB-AOMDV can attribute to the improved probability of node behavior detection because of more interactions. This elevates the probability of successful delivery to a trustworthy node. It has more attention to control packets and alleviates the impacts of malicious nodes in route discoveries.

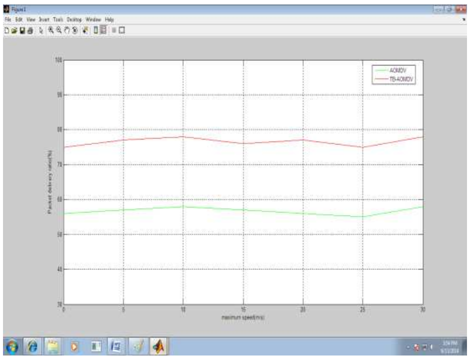


Fig 2. Packet Delivery Ratio

Fig.3 and Fig.4 illustrate that the average end-to-end latency and routing packet overhead in these protocols rise with the increase of maximum speed. At higher speeds, route entries become invalid more quickly and thus source nodes initiate more route rediscoveries before sending data. At the highest speed of 30 m/s, the average latency and routing packet overhead reach their peaks, respectively. TB-AOMDV has a little lower average end to end latency (2–6 ms) than AOMDV when the speed is greater than 5 m/s. The routing packet overhead in TB- AOMDV remains comparatively lower than that in AOMDV. Because multiple routes are found in one trusted route discovery, the frequency of route discovery is smaller in TB-AOMDV than in AOMDV and also the routing overhead in TB-AOMDV is smaller than that in AOMDV.

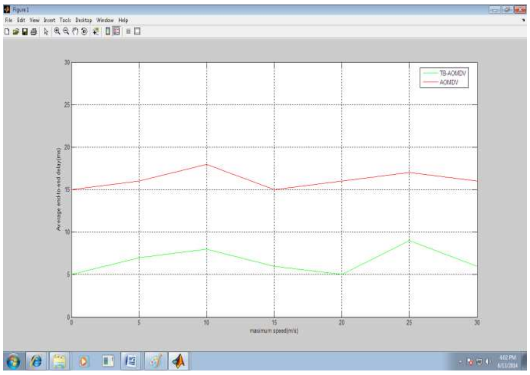


Fig 3: Average End-To-End Delay

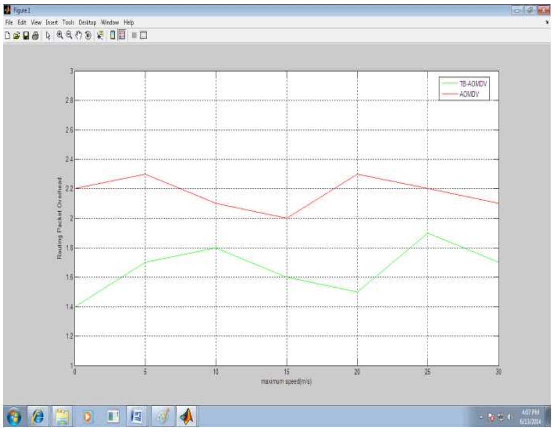


Fig 4: Routing Packet Overhead

5.2.2 Test 2: varying black-list trust threshold

In the next test, compared the two protocols TB-AOMDV and AOMDV with different trust threshold for local black lists. The number of malicious nodes is set to 20 and the trust threshold ranges from 0.1 to 0.5.As shown in Fig. 5, on the whole, the delivery ratios are not as high as expected. In fact, they are smaller than 55%. This is because the proportion of malicious nodes is 40% and a lot of packets are not forwarded devotedly by the intermediate nodes. The delivery ratios of TB-AOMDV increases lowly from 50 to 55% as the black-list trust threshold increases from 0.1 to 0.5. A smaller trust threshold means that more packets could be dropped by a node before it is regarded as a malicious node. When the threshold is equal to 0.4.

Fig. 6 shows the average end-to-end latency of TB- AOMDV as black-list trust threshold varies. The results indicate that the average end-to-end latency increases gradually from 10.2 to 15.5 ms as the trust threshold ranges from 0.1 to 0.5. As the trust threshold is set to a smaller value, fewer nodes will be added to black lists. This leads to lower average latency at the smaller threshold.

The effects on the routing packet overhead are shown in Fig.7 respectively. The routing packet overhead is about 3.4 f the trust threshold is assigned to a small value (h,0.3), the malicious nodes launching grey hole attacks will not be detected and the count of route discoveries for avoiding malicious nodes is small. As the trust threshold increases, more nodes are detected as malicious nodes and more routing packets are forwarded along trustworthy routes. Accordingly, the routing packet overhead tends to rise with the increase in the trust threshold.

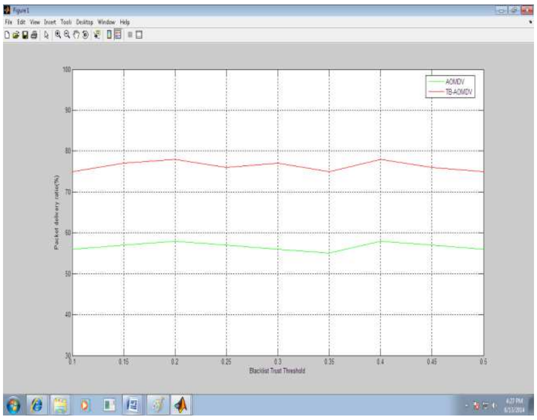


Fig 5. Packet Delivery Ratio

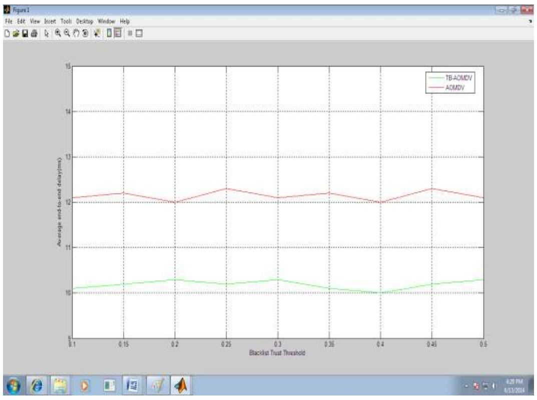


Fig 6: Average End-To-End Delay

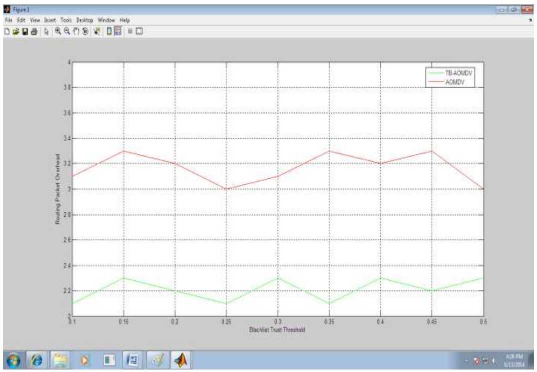


Fig 7: Routing Packet Overhead

6. CONCLUSION

In this paper, the average of the packet forward ratio and the incentive and penalty calculated is taken as the trust value. To estimate a route trust, Bayesian statistical method is used. Combined with the simple model, a novel Trust based with Bayesian statistical method in AOMDV (TB-AOMDV) is proposed to discover trustworthy forward routes and alleviate the attacks from malicious nodes. In this protocol, a source establishes multiple trustworthy routes as candidate to a destination, to identify the route using route trust value in a single route discovery. This protocol provides a flexible and feasible approach to choose a route with higher route trust values in all route candidates Performance comparison of TB-AOMDV and AOMDV and the results show that TB-AOMDV is able to achieve a remarkable improvement in the packet delivery ratio, end-to-end delay and detect malicious attacks effectively.

REFERENCES:

[1] D. Gambetta, *"Can we trust trust?," Trust: Making and breaking cooperative relations, electronic edition,* Department of Sociology, pp. 213- 237,2000.

[2] L. Mui, *Computational models of trust and reputation: agents, evolutionary games, and social networks,* Ph.D. Thesis., MIT, Massachusetts, 2003.

[3] M.H. Durad, Yuanda Cao, Liehuang Zhu, *Two novel trust evaluation algorithms, in: Proc. of the Communications Circuits and Systems,* June 2006, vol. 3, pp. 1641–1646.

[4] Y.L. Sun, W. Yu, Z. Han, K.J. Ray Liu, *Information theoretic framework of trust modeling evaluation for ad hoc networks, IEEE Journal on Selected Areas in Communications* (2006) 305–319.

[5] Y.L. Sun, W. Yu, Z. Han, K.J. Ray Liu, *Trust modeling and evaluation in ad hoc networks, in: Proc. of the Global Telecommunications,* IEEE Computer Society Press, 2005, pp. 1–10.

[6] J. Luo, M. Fan, *A subjective trust management model based on certainty-factor for MANETs,* Chinese Journal of Computer Research and Development 47 (3)
(2010) 515–523.

[7]Hui Xia a, ZhipingJiaa,⥣, Lei Jua, Xin Li a, Edwin H.-M. Shab *Impact of trust model on on-demand multi-route routing in mobilead hoc networks Computer Communications* (2013) 1078–1093(Elsevier)

[8] Z. Liu, A.W. Joy, R.A. Thompson, *A dynamic trust model for mobile ad hoc networks, in: Proceedings of the 10th IEEE International Workshop on Future Trends of Distributed Computing Systems* (FTDCS'04), 2004, pp. 80–85.

[9] A.A. Pirzada, C. McDonald, *Trust establishment in pure ad-hoc networks, Wireless Personal Communications* 37 (1) (2006) 39–168.

[10]Hui Xia a, ZhipingJiaa,, Xin Li a, Lei Jua, Edwin H.-M. Shab *Trust prediction and trust-based source routing in mobile ad hoc networks,* Ad Hoc Networks (2013) 2096–2114 (Elsevier).

[11] C. Yong, H. Chuanhe, S. Wenming, *"Trusted Dynamic Source Routing Protocol," IEEE International Conference on Wireless Communications, Networking and Mobile Computing,* 2007(WiCom 2007), pp.1632-1636, 2007.

[12] C. Wang, X. Yang, and Y. Gao, *"A Routing Protocol Based on Trust for MANETs,"* Lecture notes in computer science, vol. 3795, p. 959-964, 2005.

[13] Pirzada, A.A., McDonald,C.: *Establishing Trust in Pure Ad-Hoc Networks.* Proceeding of 27th Australasian