A Light-Weight Trust based Mobility Aware Routing Algorithm for Mobile Ad Hoc Networks

Saurin J. Choksi
Student
G.H.Patel college of Engineering and Technology
V.V.Nagar, Anand Gujarat, India

Nikhil N. Gondaliya
Head of Information Technology Department
G.H.Patel college of Engineering and Technology
V.V.Nagar, Anand Gujarat, India

ABSTRACT
Security and mobility is always a wide research area of the mobile ad hoc network. In this paper a new technique is proposed to apply secure as well as mobility aware routing in mobile ad hoc networks. For applying security the packet forwarding behaviour of the nodes is used and for mobility speed and the relative direction of the node is taken. The algorithm is implemented on AODV protocol and checked the final simulation results against the normal AODV and trust based AODV (that uses only forwarding behaviour of the nodes) using NS2. The simulations results show that proposed technique can prevents attacks from the malicious nodes and also improves the performance by using mobility aware routing.

Keywords
MANETs, trust, AODV,QOS

1. INTRODUCTION
The mobile ad hoc networks (MANETs) are infrastructure less and nodes moves randomly in the network and communicate using wireless links. So the bandwidth, topology of the mobile ad hoc networks also changes by time. Due t these characteristics mobile ad hoc network is used in different application likes in military services, emergency operation, in disaster relief and many more [1]. But because of these characteristics there are many issues in MANET like mobility, security, limited resources, routing and many more [2]. There is lots of research work done to improve the performance of the network by using different techniques. Our focus is on the security and the mobility of the mobile ad hoc networks.

There are different kinds of attack possible in the mobile ad hoc network and to provide security against them various techniques developed like by using secure keys and many more[3]. Proposed algorithm used trust based scheme to provide a security against the malicious nodes. But there are also others issues in MANET which should be considered while applying routing. As per our knowledge there is few research work is done that incorporates both security and mobility. So trust based technique uses forwarding behaviour to apply security in the network and by using the mobility metrics speed and relative direction of the node the proposed method provides the better routing with security.

The rest of the paper is as follows. In section 2 an over view of the related research is described. In section 3 how trust value is calculated is described. In section 4 the trust based routing is described and simulation results are described in section 5 and finally section 6 describes the conclusion and future work of this research work

2. RELETAED RESEARCH
In recent years there has been much work done in trust establishment in mobile ad hoc networks that are described by authors in [4] and [5]. We also have described recent work done in trust based routing in [6]. The recent work done in trust based architecture is described below.

In [7] Bo Wang *et al* has proposed trust based framework in which packet forwarding ratio is taken to establish trust and by using ETX metrics they have insured less link delay. So their proposed technique ensures both security with QOS routing.

In [8] R. Datta *et al* has proposed a light-weight trust-based trust based scheme which uses packet forwarding behaviour of the network and can eliminate the black-hole and gray-hole attack from the mobile ad hoc network. The authors says it is light-weight because it only uses information from neighbour nodes and no need to have information about whole network.

In [9] Pedro B. Velloso *et al* has proposed the new recommendation exchange protocol in which nodes can exchange the recommendation of other nodes and based on that trust value is calculated by adding some extra information like time duration in which node is in a radio range.

In [10] authors have proposed a method in which with security the energy issue is also considered. The path is established by using two metrics. One is packet forwarding ratio and second is residual energy. So the routing is secure and also energy aware.

In [11] Hui Xia *et al* has proposed a trust based framework in which two techniques is involved. In first the historical behaviour of node is calculated using packet forwarding ratio and future behaviour of the node is estimated using the fuzzy logic by using different parameters like processing power, routing load of the node etc. based on that routing is done.

In [12] the authors have proposed the security over opportunistic routing. The opportunistic routing uses minimum cost to establish a route in the network. So the authors applied forwarding on the minimum cost opportunistic routing and make the routing secure using trust value.

In [13] Zhi Li *et al* has proposed the trust based architecture using autoregression functions. This mechanism they have used 2 models, Autoregressive model in which only direct observation are taken in to account to calculate the trust value of the node. While in ARX (Autoregressive with exogenous inputs) model with direct observation recommendation of the other neighbours is also used. In this method the packet forwarding behaviour is used to calculate the trust value.

In [14] authors have proposed routing by using the probability of the different QOS parameters like transit time variation, deleted,

multiplied and inserted packets, processing delays are used to estimate and update trust value. With using the probability of these parameters the trust value is calculated and used in the routing scheme.

In next section how the proposed technique will calculate the trust value and how routing is done based on that is described.

3. TRUST COMPUTATION

In this work three trust metrics are considered that are packet forwarding ratio as a security metrics for considering secure routing and speed and relative direction as a mobility metrics for mobility awareness. So in below section we will see how each trust metrics is calculated for selecting reliable path.

The packet forwarding behaviour is used to calculate the node trust and after sensing this behaviour of the neighbouring nodes based on how packet forwarding is done by each neighbour. It is the ratio of how many packets the node has received and forwarded successfully.

Suppose node i is sensing the behaviour of node j the trust value using packet forwarding ratio can be calculated using below equation.

$$T_{i,j}(t) = \frac{F_{i,j}(t)}{R_{i,j}(t)} \ldots\ldots (1)$$

$F_{i,j}(t)$ represents the number of packets forwarded by node j at time t, $R_{i,j}(t)$ represents the number of packets successfully received by node j at time t. So we can say that if there is a malicious node in the route and it is not forwarding the packets to its next node its packet forwarding ratio will decrease and it will be detected successfully and can be removed from the route.

In this method all nodes are placed in the promiscuous mode. Whenever it finds that its neighbour nodes have received a packet to forward ahead, it increments receive count by one. Whenever it finds that its neighbour nodes have forwarded a packet it has to forward, it increases the forward count by one and based on this the packet forwarding ratio is calculated for every neighbour nodes.

The trust value of a node is between 0 and 1 and a threshold value is defined to check if trust value of node is less than threshold the node consider as a malicious. After each interval the node get the value of no of packets received and forwarded by each neighbour node and update the trust value based on that. The equation for updating the trust value is as below.

$$T_{PFR} = a * T(old) + (1 - a) * T(new) \ldots. (2)$$

Where a is a weighting factor used to balance current measurement and previous estimation.So in this way the packet forwarding ratio is calculated for each n every neighbour node and stored in the trust table. So if any of malicious node in the network is not forwarding the packet correctly packet forwarding ratio of it will decrease and if the ratio goes below threshold value it is considered as a malicious node.

In the mobile ad hoc network each node can have random speed. The node that is moving fast can go out of range of other nodes. So speed is considered for calculating trust. The equation for calculating trust based on speed is as below.

$$T_{speed(j)}(t) = \left(1 - \frac{Current\ Speed}{Maximum\ Speed}\right) \ldots\ldots (3)$$

So from the equation we can see that the node with more speed can be untrustworthy and node with less speed is more trustworthy as it moves slowly and it will take time to go out of range .

In a MANET, nodes can move from one place to another randomly with random speed and random direction that is called random waypoint model The direction of the node always lies between 0 to 360 degree (with respect to x axes). So the relative direction is the difference of the direction in degree with respect to x axes.

For example we can say that if one node is moving at 30 degree related to x axes and another node is moving 210 degree with respect to x axes so the relative direction will be 180 degree so we can say that both nodes are moving opposite direction.

Suppose node i is calculating its relative direction with node j the equation for calculating relative direction is as below

$$\theta(i,j,t) = |\theta(i,t) - \theta(j,t)| \ldots. (4)$$

Now after getting relative direction the trustworthiness is calculated based on below table which is taken from [15].

Table 1. Relative Direction

Relative Direction	$T_{Direction}$
0<=Θ<60 & 300<= Θ<360	1.0
60<=Θ<90 & 270<= Θ<300	0.8
90<=Θ<120 & 240<= Θ<270	0.6
120<=Θ<150 & 210<= Θ<240	0.4
150<=Θ<180 & 180< Θ<210	0.2
Θ=180	0

So after getting the relative direction the value is inserted in the above table and get the trust value between 0 and 1. We can say that if two nodes are moving in opposite direction the trust value using relative direction will be less and if in same direction the trust value will be high.

Now there are two metrics based on mobility so the final trust metrics based on the mobility is as below.

$$T_M = b * T_{Speed} + (1 - b) * T_{Direction} \ldots. (5)$$

Where b is the weighting factor between 0 and 1 to balance the both trust metrics.

Now there are two trust values one is T_{PFR} which is based on packet forwarding ratio and other one is T_M which is based on the mobility metrics and using both metrics the routing is done by checking the trust value against the threshold value of the particular mobile node. If the trust value of the node is below threshold value it will be considered as an untrustworthy node and the more trust value of a node, the more it is trust worthy.

4. TRUST BASED ROUTING

In this section we will see how routing is done based on trust. There are many routing protocols for MANET but Ad hoc on demand distance vector routing protocol is used as it use only local information for routing and its is suited for proposed technique. So modification is done on in AODV so that instead of shortest route trusted route is selected for reliable routing

For calculating the packet forwarding ratio all the nodes are put in promiscuous mode. So that each node can monitor the traffic and can calculate the packet forwarding ratio of each neighbour

nodes. Suppose node i is watching the behaviour of node j than it will get the number of packets received by that node j and number of packets sent by node j and store in the trust table and can calculate the packet forwarding ratio.

Now for calculating the mobility metrics of neighbours speed and relative direction each node puts its current speed and direction in the Hello packets and when a node receive the hello packets it will calculate the mobility trust based for that particular node and store in the trust table and by using the trust table the trust value calculated for each neighbour node. The trust table have values of node id, number of packets received, no of packet forwarded, T_{PFR} ,T_{speed} , $T_{Direction}$ and T_M.

For updating the trust value a Trust update Timer is defined so that after each duration the all the values are calculated and stored again in the trust table. The trust table is as below.

Table 2. Trust Table

Node id	**No of packets received**	**No of packets sent**	**T_{PFR}**	**T_{speed}**	**$T_{Direction}$**	**T_M**

Now the modification done in the AODV in the routing procedure is as below.

- Route Request:

Before the source node S wants to send a data packet to a destination node D, node S will check in the route table that if the route is available or not. If route is available it will send the data and if not it will proceed to send a REQ packet.

Before sending the REQ packet the source node will check its neighbour nodes' both trust value in its trust table. Then, source node will broadcasts route request packets REQ to its neighbour nodes if their trust degree is greater than the defined threshold value. At first it checks the T_{PFR} value against the threshold value. If it above threshold value it checks the T_M value and if both are above threshold value the REQ packet is sent otherwise not.

When the intermediate node in the network receives the REQ packet sent by the source node S, it first checks whether it received the REQ packet before. if so, it drops the REQ packet, otherwise it will update the packet and broadcast the REQ packet to trusted neighbour nodes whose both trust value is also greater than threshold value. When destination node receives the REQ packet, it will generate the reply packet and send it to the reverse direction.

- Route Reply:

When intermediate node receives the REP packet it will look up the next node in reverse path and send the updated REP packet to next node.

When source node receives the REP packet the REP delivery procedure finished and the source node will start sending the data.

- Route Maintenance:

Each node updates the trust value of its neighbour nodes during each interval and also get the updated information of its neighbours using hello packets.

The node notifies to all the neighbouring nodes about the link broken state by sending RERR packets if the next node in route is lost or if the one of the trust value of the next node in the route will become less than threshold value.

If the intermediate nodes receive the RERR packet they will update it and broadcast it again. If the source node receives the RERR packet, it will rebroadcast the REQ packet to its trusted neighbour nodes and the route will be again established bypassing the broken link or untrustworthy nodes.

Now suppose node k is malicious and its packet forwarding ratio calculated by node i is 0.2 and its speed is 7 m/s so the if the max speed is 10 than the T_{SPEED} will become 0.3 and if relative direction is 96 degree than the mobility trust will become 0.27 and we can say that it is untrustworthy node. So the node will not send the request to node k.

So, in this way we a trusted route is established in the network between sender node and receiver node. In the next section the simulation parameters and results of the proposed algorithm and comparison with normal AODV is described.

5. SIMULATION AND PERFORMANCE EVALUATION

The simulation is done with network simulator 2.35[16] and used random way point model [17] to apply mobility on the nodes. The simulation parameters are shown in table 2. Packet dropping attack is used for attacking scenario and compared the result with normal AODV, TAODV which uses only packet forwarding ratio and TMAODV which is our proposed technique.

Table 3. Simulation Parameters

Parameters	**Value**
Simulation Time	150s
Number of nodes	10 to 60
Routing Protocol	AODV
Traffic Model	CBR
Packet size	512 bytes
Terrain	200 x 200m
Speed	0 to 20 m/s
Transmission Range	50m
No. of malicious node	1
Name of Attack	Packet Dropping Attack

The other trust parameters are described in below table.

Table 4. Trust Parameters

Trust Parameters	**Value**
Threshold	0.4
Trust update timer	1s
Weighting factor b	0.5
Timer to check trust value	0.5s

Now the simulation results are described as below.

5.1 Packet Delivery Ratio: The Packet Delivery Ratio is the ratio of the number of packets received by the destination to the number of packets generated by the source node. The packet delivery ratio of malicious AODV, TAODV and TMAODV is shown in figure 1. The figure 1 shows that malicious node can significantly decrease the performance of the AODV. TAODV can increase the performance by eliminating it and applying TMAODV the PDR is also improved as applying mobility awareness also.

5.2 Average End to End Delay: The Average End to End Delay is the average difference of time between sending of the data packets and its receipt at the destination. This includes all possible delays caused by route discovery latency, propagation and retransmission delays in the routing layer and physical layer. The figure 2 shows that TAODV and TMAODV has more Average End to End Delay because of trusted route in place of shortest route and also applying routing procedure and routing maintenance will take some time.

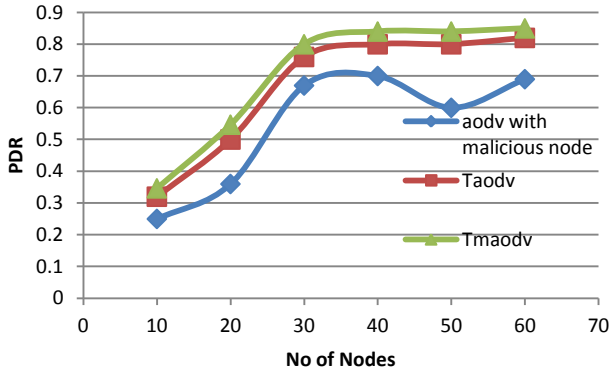

Figure 1. Packet Delivery Ratio vs no of nodes

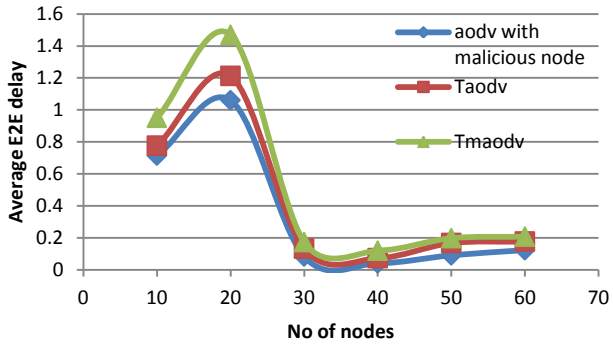

Figure 2. Average End to End Delay vs no of nodes.

5.3 No of malicious: If the number of malicious nodes in the network increases the packet delivery ratio also decreases. For that no of nodes is taken 40 and increase the no of malicious nodes. Fig 3 shows the comparison of the malicious AODV and TMAODV by increasing the malicious node from 1 to 5. It shows that TMAODV gives the better performance to eliminate the malicious node against malicious AODV.

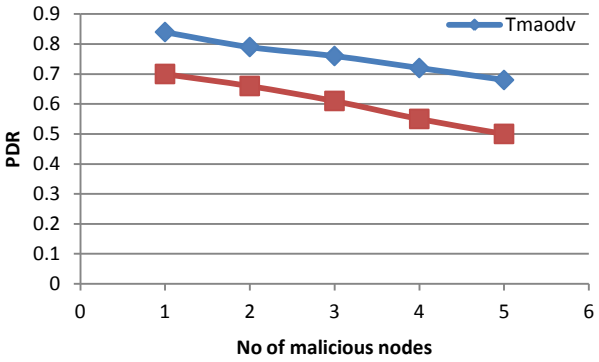

Figure 3. Packet Delivery Ratio vs no of malicious nodes

5.4 Trust Update Time Interval: Trust update time interval also plays important part in out algorithm. If the update interval is high so it will take more time to update the trust value of the particular node so there will be more time to detect the malicious node and to remove it from network. Figure 4 shows that the packet delivery ratio significantly decreases as the trust update time interval increases.

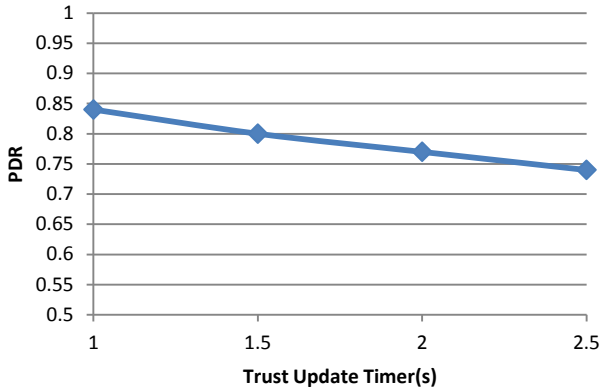

Figure 4. PDR against trust update time interval

5.5 Changing the attacking scenario: Up till now the Packet dropping attack in the attacking scenario is used. Now by changing the attacking scenario to black-hole attack to check the feasibility of the algorithm. Figure 5 shows the comparison of normal AODV and TMAODV in the black-hole attack. The figure shows that TMAODV can successfully eliminate the malicious node from the network and improves the packet delivery ratio of the network.

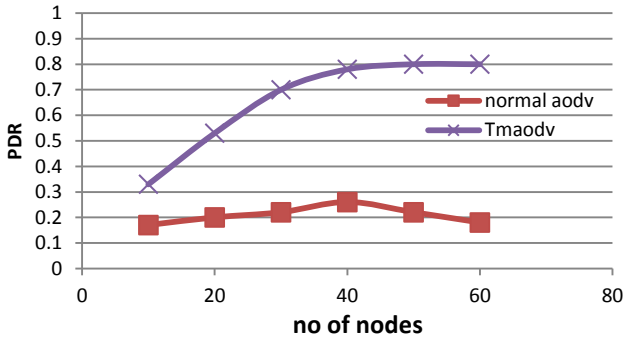

Figure 5.Packet Delivery Ratio vs no of nodes under the black-hole attacking scenario

6. CONCLUSION AND FUTUREWORK

The method describes how mobility metrics is used with secure routing and improve the efficiency of the network. So the proposed technique provides both secure routing as well as mobility aware routing. The algorithm is light weight as only local data is used in the computation and it ensures lower processing time for each node. The simulation results show that the malicious nodes can successfully removed and we can get better performance of the network by using proposed technique. In future work more security parameters can be added to calculate the trust for example using control packet forwarding ratio with packet forwarding ratio. Other mobility metrics can be added like pause time of neighbour nodes or relative velocity to further improvement of the efficiency of the network.

7. ACKNOWLEDGEMENT

My Sincere thanks to my guide Prof. Nikhil N Gondaliya, for providing me an opportunity to do my research work. I also express my thanks to my Institution, my family, friends and colleagues who have helped me for the completion of this work.

8. REFERENCES

[1] Haas J.D.Z., Liang B., P. Papadimitatos and S. Sajama, "Wireless ad hoc networks," in Encyclopedia of Telecommunications J. W. John Proakis, Ed., 2002

[2] Carlos de Morais Cordeiro and Dharma P. Agrawal , " Mobile ad hoc networking", OBR Research Center for Distributed and Mobile Computing, ECECS

[3] Djmel djenouri and lyes khelladi, "A survey of security issues in mobile ad hoc and sensor networks", IEEE communications surveys & tutorials , fourth quarter 2005

[4] Jin-Hee Cho, Ananthram Swami, Ing-Ray Chen, "A survey on trust management for mobile ad hoc networks", IEEE Communications Surveys and Tutorials 13 (4) (2011) 562–583. Fourth Quarter.

[5] Kannan Govindan, Prasant Mohapatra," Trust computations and trust dynamics in mobile ad hoc networks: a survey", IEEE Communications Surveys and Tutorials 14 (2) (2012) 279–298.

[6] Saurin Choksi, Nikhil Gondaliya, "Trust Based Routing Protocols For Mobile Ad hoc Networks : A Survey", International Journal of Research in Advent Technology,2014

[7] Bo Wang, Xunxun Chen, Weiling Chang,"A light-weight trust-based QoS routing algorithm for ad hoc networks" , Elsevier,2013

[8] N. Marchang, R. Datta,"Light-weight trust-based routing protocol for mobile ad hoc networks", IET Information Security 6 (2) (2012) 77–83.

[9] Pedro B. Velloso, Rafael P. Laufer, Daniel de O. Cunha, et al., "Trust management in mobile ad hoc networks using a scalable maturity-based model", IEEE Transactions on Network and Service Management 7 (3) (2010) 172–185.

[10] M. Pushpalatha, Revathi Venkataraman, and T. Ramarao, "Trust Based Energy Aware Reliable Reactive Protocol in Mobile Ad Hoc Networks"World Academy of Science, Engineering and Technology, Vol: 32 2009-08-27

[11] Hui Xia, Zhiping Jia , Xin Li, Lei Ju, Edwin H.-M. Sha,"Trust prediction and trust-based source routing in mobile ad hoc networks", Elsevier,2012

[12] Bo Wang, Chuanhe Huang, Layuan Li, et al., "Trust-based minimum cost opportunistic routing for Ad hoc networks", Journal of Systems and Software 84 (12) (2011) 2107–2122

[13] Zhi Li, Xu Li, V. Narasimhan, "Autoregression models for trust management in wireless ad hoc networks", in: IEEE Globecom, 2011, Kathmandu, Nepal.

[14] D. Umuhoza, J.I. Agbinya, C.W. Omlin ,"Estimation of Trust Metrics for MANET Using QoS Parameter and Source Routing Algorithms", AusWireless 2007, IEEE

[15] Sajal Sarkar , Raja Datta , "A Mobility factor based path selection scheme for mobile ad hoc networks" , IEEE , 2012

[16] Teerawat Issariyakul, Ekram Hossain, "Introduction to Network Simulator NS2", Springer 2008.

[17] Nils Aschenbruk, Raphael Emst and et. al., "BonnMotion: a mobility scenario generation and analysis tool", SIMUTools '10 Proceedings of the 3rd International ICST Conference on Simulation Tools and Techniques, 2010