Multiple Trust in Trust-Based on-Demand Routing in Mobile ad hoc Networks

P. Rama Kishore[1], O. SrinivasaRao[2] & MHM Krishna Prasad[3]

[1&3] Dept. of IT, JNTUK UCEV, Vizianagaram, A.P., 535 003, India
[2] Dept. of CSE, JNTUK UCEV, Vizianagaram, AP, 535 003, India
E-mail : p2rams0@gmail.com[1], osr_phd@yahoo.com[2], krishnaprasad.mhm@gmail.com[3]

***Abstract* – Mobile Ad-hoc networking is concept of communication, which means a communication temporary network without any form of centralized administration. Every node in this network acts both as host and a router to forward packets for other node. Due to the absence of the centralized administration, MANETs are easily attacked by malicious nodes. To decrease the attacks from malicious nodes, a concept is introduced is Trust in MANETs to calculate the trust of neighbors nodes to find a trusted path to send data between source and destination nodes. To maintain the MANETs some protocols are developed AODV, AOMDV by introducing the Trust concept the new protocol developed is AOTDV. By using AOTDV protocol, before sending the data we calculate the trust of the neighboring node by control packet forwarding. After finding the trusted path the data will be sent to destination. Even we find the trusted path there is a chance that the trusted node may turns in to the malicious node. So to avoid this problem we proposing a concept that multiple times trust calculation using time windows in network when we are sending data packets. To compare the AOTDV and Multi Trust calculation in MANETs several experiments have been conducted. And the results show that multiple time trust calculation gives more trusted path and provide more security than previous protocol.**

Keywords – AOTDV, Trust, Node Trust, Path Trust, Time window.

I. INTRODUCTION

A mobile ad hoc network is an autonomous system of mobile nodes connected by wireless links to form a temporary network. MANETs need not require any static infrastructure like base station. The nodes in MANETs communicate and cooperate with each other to achieve its goal. These nodes are dynamically move one place to other so they form a self organized multi agent system and all nodes work as both host and routers. This is MANET concept is open working environment and is depends on the nodes exist in network. So MANET can work well when nodes in the network behave cooperate with each other. Because of open environment property the MANETs are suffering with malicious nodes. Some attacks are Black hole attack, Wormhole attack, Spoofing attack, Denial of service attack, Non repudiation attack, Ignorance attack.

To avoid the attacks and provide security in MANETs we may use the traditional security mechanisms like authentication techniques, key concept that uses public and private keys. But The MANETs don't have the infrastructure so these traditional security concepts do not fit to MANETs, because they need some underlying infrastructures. To provide authentication and encryption concepts, secure touting protocols [1] have been developed to ensure confidentiality and integrity. But these protocols are not possible in MANETs due to lake of centralized trusted third party [2]. So similar to humans the concept trust is introduced to carry an action securely [3] in MANETs to calculate the trust of the node. The truth is the trust concept is not absolutely secure but it provides reliability in the network [4].

The motivation to introduce trust in MANETs is to find the malicious nodes in network. Every node maintains the behaviors of the other's through the trust evolution history. So we can improve the network performance by this history.

In this paper, we introduced a simple trust model and calculate the trust of nodes multiple times using packet forwarding ratio to evaluate the neighbor's behaviors. In MANETs we have two types of packets are control packets and data packets. To evaluate trust frequently we are going to observe the both control and data packets. We propose a novel multipath reactive routing protocol for MANETs that is 'multiple ad hoc

on-demand trusted path distance vector' (MAOTDV). Already some routing protocols were introduced in MANETs are ad-hoc on demand distance vector (AODV), ad-hoc on demand multipath distance vector (AOMDV), and Trust introduced AODV is ad-hoc on demand trusted path distance vector (AOTDV), so we are going to compare our MAOTDV protocol with the AOTDV protocol which was gives the best results in providing the more reliability in MANETs [base paper].

II. Related Work

There is several research works are done on trust concept in MANETs. They are concentrated in two areas are Trust management in network and Trust including in touting protocols of MANETs.

Routing Protocols

In ad hoc networks there are two types of protocols are developed, they are proactive and reactive [5]. The nodes in MANETs have limited resources therefore reactive protocols are more suitable for MANETs. The reactive routing protocol AODV is based on a hop-by-hop routing mechanism [6] and it is a single path routing protocol. AODV is extended with multiple loop free and link disjoint method and a new protocol is developed named as AOMDV [7]. The AOMDV proves that good improvement in the end-to-end delay and these assume that all nodes are honest and cooperative.

To provide security in MANETs some cryptographic methods are introduced in AODV protocol, newly generated protocol is SAODV [1], but these protocols need centralized administration or trusted third party to manage network. So it is expensive and more resources are required.

Recently, a new class of routing protocols in MANETs has been proposed, called trusted routing protocols, which consist of two parts: a routing strategy and a trust model [2]. The node trust is calculated through an acknowledged mechanism from destination to source. Every acknowledged packet will increase the sender node's trusts in all the intermediate nodes along the path to the destination, whereas every retransmission decreases the trusts. It is impossible for senders to know which nodes discard packets. Pirzada et al. [8] evaluated the performance of three trust-based reactive routing protocols (trusted AODV, DSR and TORA) by varying the number of malicious nodes and other experiment settings. The results indicate that each trust-based routing protocol has its own advantage. Specifically, trust-based AODV routing maintains a stable throughput and surpasses TORA and DSR at higher traffic loads [8]. AOTDV is a multipath protocol and AOTDV considers the trust values of paths as well as the number of hops. It provides that more reliability in MANETs but there is a problem in it. That is it only calculates trust of nodes only before data send through control packets, so there is chance that the trusted nodes will turns into the malicious nodes while transferring data in network. Therefore we are providing multiple trust calculation in the AOTDV using both the control packet forwarding and data packet forwarding also.

Trust Model

During trust computation, a linear aggregation is used to estimate the overall trust in a node, and a continued product is used to compute the trust of a path. Trust applications including trust-based route discovery and route selection will be discussed in the next section.

We assume that after one node broadcasts a packet all neighbors will receive the packet correctly. However, if the distance between source and destination is beyond one hop, packets might be dropped by intermediate nodes because of unexpected causes (such as heavy traffic) or malicious attacks (such as black-hold or grey-hold attacks). Trust evaluation in a routing procedure is an assessment of forwarding behaviors of neighbors by a sender. More specifically, a node j will give its neighbor k a trust score after the node k transmits a packet sent by node j. Thus, we use packet forwarding ratio to evaluate the quality of forwarding.

Forwarding ratio:

Forwarding ratio is the proportion of the number of packets forwarded correctly to the number of those supposed to be forwarded.

Window forwarding ratio:

The window forwarding ratio FR (t) is the packet forwarding ratio in a recent window. FR (t) is computed as follows

$$FR(t) = \frac{N_C(t) - N_C(t-W)}{N_A(t) - N_A(t-W)}, \qquad t > W$$

$$FR(t) = \frac{N_C(t)}{N_A(t)}, \quad t \le W \qquad (1)$$

Where $N_C(t)$ represents the cumulative count of correct forwarding and $N_A(t)$ signifies the total count of all requesting before time t. The count of correct forwarding in a time window (from time t-W to t) is equal to$N_C(t) - N_C(t-W)$, where W represents the width of the time window. We compute $FR(t)$ only using the forwarding count and requesting count in the recent W time units. The history records out of the recent window are discarded.

The packets in MANETs classified into two types control packets and data packets. Control packets play an important role in establishing of routing in network. So $FR(t)$ is divided into control packet forwarding ratio

CFR (t) and data packet forwarding ratio DFR (t). They are computed using forwarding count of control packets and data packets according to formula (1) respectively.

Computation of node trust:

The trust of a node j in another node k (node trust for short) is a measure to ensure that packets sent by node j have actually been forwarded by node k. Two trust factors [CFR (t) and DFR (t)] are assigned weights in order to determine the overall trust value of a node. The direct trust in node k by node j is represented as T_{jk} and is given by the following formula

$$T_{jk}(t) = w_1 \times \mathrm{CFR}_{jk}(t) + w_2 \times \mathrm{DFR}_{jk}(t) \qquad (2)$$

Where $\mathrm{CFR}_{jk}(t)$ and $\mathrm{DFR}_{jk}(t)$ represent control packet forwarding ratio and data packet forwarding ratio observed by node j for forwarding node k at time t, respectively. The weights w_1 and w_2 ($w_1, w_2 \geq 0$ and $w_1 + w_2 = 1$) are assigned to CFR and DFR, respectively.

Node j checks whether the neighbor k forwards the packet correctly. If so, the trust value T_{jk} increases. Otherwise, T_{jk} decreases. In our trust model, trust values are limited in a continuous range from 0 to 1 (i.e. $0 \leq T_{jk} \leq 1$). The trust value of 0 signifies complete distrust whereas the value of 1 implies absolute trust. If there is no interaction between two nodes, the initial trust value is set to 0.75 which is minimum trust. A threshold η, termed as the black-list trust threshold, is used to detect malicious nodes. In other words, if the trust value of a node is smaller than η, it will be regarded as a malicious node. An example of trust levels of nodes are listed in Table1.

Level	Trust value	Meaning
1	[0, η)	Malicious node
2	[η, 0.75)	Suspect node
3	[0.75, 0.9)	Less trustworthy node
4	[0.9, 1]	Trustworthy node

Table1 Trust levels of nodes

Computation of path trust:

To send the data from source to destination we need to find the trusted path. So to find the trusted path we use the trust values of the nodes to find the most trustworthy path in the network. Considering the axiom [9] path trust should not be more than the trust values of intermediate nodes. So at a time the trust of a path is equal to the continued product of node trust values in the path, that is

$$T_p(t) = \prod \left(\{ T_{jk}(t) \mid n_j, n_k \in P \text{ and } n_j \rightarrow n_k \text{ and } n_k \neq N_d \} \right)$$

Where t is time, $T_p(t)$ is path trust n_j and n_k are any adjacent nodes in path P, N_d is destination node, $n_j \rightarrow n_j$ represents that the next hop node of n_j is n_k.

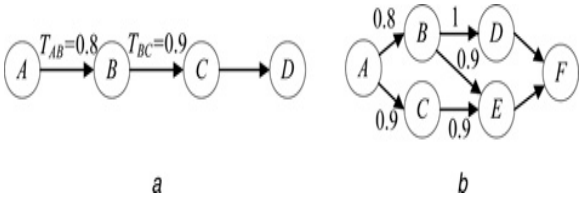

Fig.1 : Path Trust Computation

Observe the figure1, there we can observe two figures a and b, a is an example of a single path and b is an example of a multiple path. In a, the node trust of AB is 0.8 and denoted as (T_{AB}=0.8). The path trust of AB is 1 and it denoted as ($T_{P(A,B)}$=1). Trust of path A to D is calculated as $T_{P(A,B,C,D)} = T_{AB} \times T_{BC}$=0.8×0.9=0.72.

The fig b shows a complex graph, if A is the source node and F is the destination node. So we can send the data in 3 possible ways A,B,D,F is first path A,B,E,F is second possible path and A,C,E,F is the third possible path. The three possible paths have the path trusts are 0.8, 0.72 and 0.81 respectively.

P (A, C, E, F) = $T_{AC} \times T_{CE}$= 0.9 × 0.9 = 0.81

So A to F the path P (A, C, E, F) is the most trustworthy path when compare with remaining two possible paths.

Proposed system:

In this paper consider the concept of adaptive trust model, which depends on the time line. Most of the existing trust models consider a node has normal or malicious till end of the protocol that decision can't change. This will lead to some problems if the existing node's behavior changed. In the adaptive based trust model time is divided into multiple windows, in every window the trust will be recalculated by giving less priority to the past windows. Every window has specific time period and in that time period every node's behavior will be monitored by a thread in simulation, it periodically monitors the nodes behavior and update the trust level of the nodes within that time window.

In this paper, the trust is calculated based on the both control packets and data packets transmission. Initially to find the routes to the nodes, we have to flood the control packets and verify the no. of control packets dispatched to the intermediate nodes. So trust value

calculation involves both no. of control packets transmission and data packets transmissions in this case, but always it is not necessary to flood the control packets. In that case we should not consider the participation of control packet delivery ratio in the trust value calculation. So in every time window initially we consider the no. of control packets are greater than 0 or not. If the control packet ratio is 0 it continue the calculation with by considering with packet delivery ratio. After the completion of one time window, reset the values of trust of every node and recalculate the trust from recent window.

III. Experimental Results

We have conducted a comprehensive test using Java interpreter of TCL is JACAL version 1.4.1. And all experiments are done on a PC with a Pentium4 processor (4 GHz) and 2 GB main memory.

Network Animator (NAM) simulator is used to show how the network performing it activities like path finding, packet dropping, and so on graphically. Within a rectangular field of 1000*1000m, we dispersed 100 nodes randomly.

In order to evaluate this approach simulated a mobile ad hoc network (MANET). Assumptions included that the network has no preexisting infrastructure and that the employed ad hoc routing protocol is the Ad hoc On Demand Trusted path Distance Vector (AOTDV).

Time window	Max trust obtained
T0	0.75
T1	0.805
T2	0.829
T3	0.856
T4	0.895
T5	0.901
T6	0.925
T7	0.95
T8	0.985
T9	1

Table 2 : Trust values in time window

Based on the time window, the level of the trust is increased gradually by isolating the no of malicious nodes from the network.

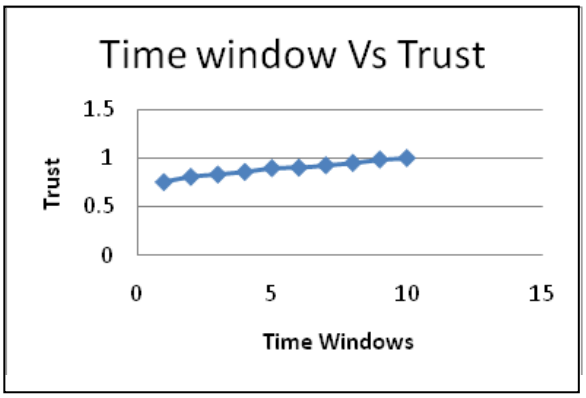

Fig. 2

No. of Nodes	Malicious Nodes
10	5
20	4
30	3
40	8
50	9
60	4
70	7
80	9
90	10
100	15

Table 3 : Table for malicious nodes:

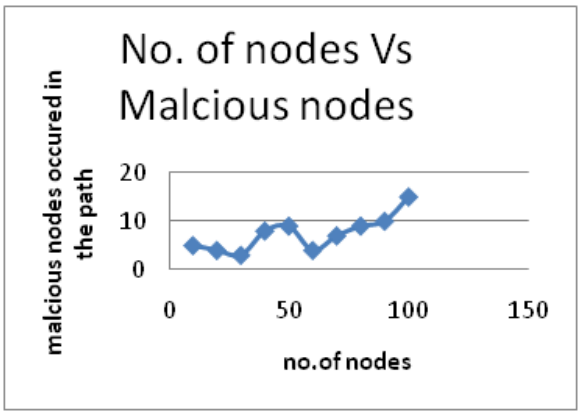

Fig. 3

Based on the no. of nodes and the transmissions from one node to another node, the trust values can be deviated in every transmission. Based on these values no. of malicious nodes can be identified.

No. of Nodes	Min Trust	Max Trust
10	0.816	0.975
20	0.819	0.982
30	0.809	0.984
40	0.914	0.983
50	0.928	0.984
60	0.845	0.984
70	0.739	0.983
80	0.78	0.982
90	0.801	0.983
100	0.907	0.987

Table 4 : Max and Min trust values:

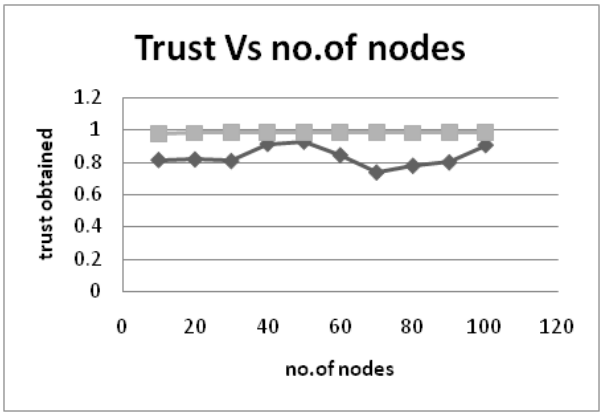

Fig. 4

Above graph (fig4) specifying minimum and maximum trust obtained by varying the no. of nodes in every ideal case.

IV. CONCLUSION

Thus this paper considering the evolution of trust based on-demand adaptive trust window model to increase the delectability of no. of malicious nodes. Later on those nodes will be isolated in every stage to increase the trust model.

V. FUTURE WORK

In future work can be extended by the introducing the multicast groups and applying the same trust model with small modifications suitable to multicast groups and there is a need to find an unique solution for the group trust.

VI. REFERENCES

[1] ZAPATA M.G., ASOKAN N.: 'Secure ad hoc on-demand distance vector routing', ACM Mob. Comput. Commun. Rev., 2002, 3, (6), pp. 106–107

[2] GRIFFITHS N., JHUMKA A., DAWSON A., MYERS R.: 'A simple trust model for on-demand routing in mobile ad-hoc networks'. Proc. Int. Symp. on Intelligent Distributed Computing (IDC 2008), 2008, pp. 105–114

[3] GAMBETTA D.: 'Can we?', in GAMBETTA D. (ED.): 'Trust: making and breaking cooperative relations' (Oxford Press, 2000, 1st edn.), pp. 213–237

[4] PIRZADA A.A., MCDONALD C.: 'Trust establishment in pure ad hoc networks', Wirel. Pers. Commun., 2006, 37, (1), pp. 39–168

[5] ROYER E.M., TOH C.K.: 'A review of current routing protocols for ad hoc mobile wireless networks', IEEE Pers. Commun. Mag., 1999, 6, (2), pp. 46–55

[6] PERKINS C.E., ROYER E.M., DAS S.R.: 'Ad-hoc on demand distance vector routing'. Proc. Int. Workshop on Mobile Computing Systems and Applications (WMCSA), New Orleans, LA, USA., February 1999, pp. 90–100

[7] MARINAM.K., DAS S.R.: 'On-demandmultipath distance vector routing for ad hoc networks'. Proc. Int. Conf. on Network Protocols, Riverside, CA, USA., November 2001, pp. 11–14

[8] PIRZADA A.A., MCDONALD C., DATTA A.: 'Performance comparison of trust-based reactive routing protocols', IEEE Trans. Mob. Comput., 2006, 5, (6), pp. 695–710

[9] SUN Y., YU W., HAN Z., LIU K.J.R.: 'Information theoretic framework of trust modeling and evaluation for ad hoc networks', IEEE J. Sel. Areas Commun., 2006, 24, (2), pp. 305–317

[10] X.Li, Z.Jia, P.Zhang, R.Jhang, H.Wang: 'Trusted-based on-demand multipath routing in mobile ad hoc networks', IET Inf. Secur., 2010, Vol. 4, Iss. 4, pp. 212–232

◈◈◈