IJCTA, 9(21), 2016, pp. 105-110
© International Science Press

Trust Based Routing to avoid malicious nodes in MANET

Kajal Patel*

Abstract : Mobile ad hoc network is network constructed using mobile nodes like laptop, tablet, etc mobile devices which can be used to send and receive data using wireless communications. No pre existing infrastructure is required for ad hoc network setup. Each node of network act as sender, receiver and intermediate node while communication happens. Each node act as a router for packet transfer. Such network is useful for military and disaster management where infrastructure may damaged or not existed. Absence of central authority and specialized routers make such network vulnerable to various packet drop and delay attacks where intermediate nodes act maliciously and disturb network by dropping/delaying packets coming to them. Solution used for wired network can not be applied in wireless network as it is due to resource constraint of nodes in MANET. Cryptographic approaches introduce unnecessary computing complexity which is not appropriate for battery operated and resource constraint nodes. Trust based routing can be used to avoid such selfish/malicious node in network. This paper presents effect of such selfish/malicious nodes in MANET. Also we have proposed a trust based solution to avoid selfish/malicious node in active route and thus improve route discovery time and throughput of the network.

Keywords : Ad hoc Network, selfish node, malicious node, route discovery time, throughput, trust based routing.

1. INTRODUCTION

MANET is a multi hop infrastructure less network with dynamically changing topology due to mobility of participant nodes in network. No pre existing infrastructure is required to set up ad hoc network. Node has to depend on other nodes for data transfer toward destination node[14]. Each node act as a router and responsible for routing packet toward destination. Thus node has to depend on intermediate nodes. The existing routing protocol used for mobile ad hoc network concentrate only on dynamic topology of node. They are not considering various attacks which intermediate node can do on packets[14]. Intermediate nodes act selfishly or maliciously ie they may drop packet instead of forwarding them further or intentionally delay them before forwarding. To detect such malicious activities one may use widely used cryptography based solutions. We can not use such heavy weight complex algorithm in mobile ad hoc network as nodes in mobile ad hoc network are having limited processing power and memory constraint. Researchers come up with many approaches for detecting selfish and malicious activities. These approaches are classified in to three categories. They use cryptographic approach to avoid attacks. They may use IDS to detect attacks and They may use trust based approach to detect and avoid attacks. The first two approaches are heavy weight and use more processing and memory so not widely used for wireless ad hoc network. The trust based approach is getting popular among researcher as it is light weight and simple. Researchers associate trust value with each node[2]. This trust value can be calculated using various parameters observed for that specific node. Also based on past interaction node will compute the future trust value of a node using probabilistic approach, Hidden Markov model, weighted sum model, fuzzy model, symbolic logic etc[3]. Nodes may also broadcast the trust value observed by them as a recommendation. Thus trust value can be calculated directly by

* Department of Computer Engineering Government Engineering College, Rajkot, Gujarat, India Email- kspldce@gmail.com

observing traffic of neighbors and by collecting recommendation from others[1]. Any node's trustworthiness can be decided using trust value calculated for it. Again this trust value changes dynamically with time and behavior of node. Threshold values are used to decide the nodes trustworthiness. In this paper we are using total number of packet drop by node , total number of packets delayed by node, total number of packet modified by node before forwarding, total number of REER packet initiated by node and remaining energy of node to calculate trust value of a node. This trust value is used to calculate trust of the route which is established while routing and avoid less trustworthy node in route. Thus our approach not only detects malicious activities but also gives stable route as I have consider battery life and REER at node for calculating trust value. The route with less malicious nodes and more stable nodes are added in route[16].

The rest of the paper is organized as follows. We discuss the current state of art in section II. Proposed Trust based Routing algorithm used for mobile ad hoc network is explained in section III. Experimental results are presented in section III. Concluding remarks are given in section IV.

2. STATE OF ART

MANET are deployed in controlled environment so the probability of attacks and malfunctioning increase as there is no controlling entity here to monitor the activities of nodes. There are numerous approaches proposed by researchers to implement trust based routing which identify malicious nodes of network.

In [17] authors proposed trust management protocol for MANET which addresses two important area: Trust bias minimization and application performance maximization. They integrate social as well as QoS parameters to calculate trust. Trust will be calculated as social trust and Qos trust. Social trust is calculated using social ties measured by intimacy and honesty by healthiness. QoS trust uses energy of node and cooperativeness (successful packet forwarded).

In [11] authors proposed a secure routing scheme for MANET routing which is based on AODV. They concentrate on packet drop and packet delay attack. They used trust based approach in which trust is calculated using various network parameters and weight is also assigned to them. The parameters they used are data packet dropped, data packet forwarded, number of packets delayed, control packets dropped and remaining energy of a node. Trust is calculated using weighted sum model.

In [18] authors present a light weight trust based routing which consumes less computational resources. It will used locally available information on each node. Their protocol will detect black hole and grey hole attack. On each node trust value of all neighbour nodes will be calculated.

In ARMAN scheme [19] authors have seen trust a subjective probability by which it has no dependency on any third party. It uses direct information coming from personal observation of agents and indirect information coming from other agents. Trust computation is performed in three parts. 1) obtains direct observation between truster and trustee. 2)collects second hand information provided by set of neighbours 3) integrate first hand and second hand information using Dempster Shafer theory. To avoid malicious second hand information it uses Similarity view it is based on an assumption that if two agents observe an event in the same way, they have similar views.

3. TRUST BASED ROUTING ALGORITHM

In our trust model each node which is a part of the network maintains a trust table in which it records values obtain by observing behaviour of each of its neighbours. These values are used to measure the level of trust a node has on its neighbours. For reducing extra overhead we only considered the values locally observed at a node. Let our ad hoc network has N number of nodes. Any random node *i* of a network has M numbers of neighbour. The trust table at node *i* hase total M entries in it. One for each neighbour. Node *i*'s trust on node *j* can be calculated using values stored in a trust table at node *i* for neighbour *j*.

Let Ti(j) is trust of node i on node j(j is neighbour of i).

$Ti(j) = = - W1*(Poj - PFj) - W2 * Pej - W3 * PERj + W4*REj$

Poj : number of packet observed for a neighbour node *j*,

PFj : number of packet successfully forwarded by neighbour node *j*,

Pej : number of packets delayed at neighbour node *j*,

PERj : number of error packets initiated by neighbour node *j*,

REj : remaining energy of node *j*.

Here W1, W2, W3 and W4 are the weight factors. W1 + W2 + W3 + W4 = 1 and 0 < = W1,W2,W3,W4 < = 1. W1 is the weight for detected packet drop and packet modification at node which must be more as packet drop and modification at an intermediate node is serious issue. W2 is weight related to packet delay detected at node which is less serious comparing previous attack. W3 is weight related to mobility of a node. W4 is weight associated with Energy of neighbour node. Initial value of W1 = 0.5, W2 = 0.3, W3 = 0.1 and W4 = 0.1. We are giving more importance to packet drop/modification attack compare to delay attack and route stability due to mobility of nodes and energy of node. With time activities are detected and values of weights changes based on the observed values of each neighbour using following calculation.

$$\begin{aligned} X &= (Poj–PFj) \\ Y &= Pej \\ Z &= REj \\ W1 &= (X/(X + Y + Z)) \\ W2 &= (Y/(X + Y + Z)) \\ W3 &= W4 = (1–(W1 + W2))/2 \end{aligned}$$

In our algorithm weight values are updated when trust value of any node is calculated on node.

The trust model which we design observes the behaviour of their neighbours and calculates the trust value. To reduce complexity and overhead we use passive monitoring of traffic to evaluate the node.

Trust based routing

Route is a sequence of nodes from source to destination. The trust of route depends on the trust value of all intermediate nodes. Let a route r consists of l intermediate nodes.

*x*1, *x*2, *x*3—*x*l where xi is ith intermediate node of route r

Trust value of route *r* is Tr,

$$\begin{aligned} Tr &= T_{x1} + T_{x2} +.....+ T_{xl} \\ Tr &= \sum_{i=1}^{1} Txi \end{aligned}$$

On each node trust table is maintained storing observed values for each neighbour.

4. EXPERIMENT SETUP

In OPNET 11, We have updated a node model wlan_wkstn_adv which comes with standard wireless lan package as Drop_wlan_wkstn_adv and Dly_ wlan_wkstn_adv for implementing periodic packet drop and packet delay attacks respectively.

After creating the malicious node models, We have compare the route discovery time of AODV routing protocol and throughput of Wireless LAN by creating two scenario one is without the malicious node (reliable_aodv) and other is with malicious nodes (unreliable_aodv) as shown in figure 1 (*a*) and (*b*). In fig (*b*) encircled nodes are malicious. Node 2 is a node with packet drop attack and node 4 is a node with packet delay attack. Each scenario has 6 nodes. The traffic used for simulation is UDP traffic which flows from source node to destination node. The simulation runs for 20 minutes and traffic starts at 100 seconds. Traffic is generated by sending 5060 request packets from the source to the destination with a inter request time 3 seconds. Each request packet consists of 1470 bytes, with each request sending 5 packets (Anipakala Suresh, 2000). Response from the destination is disabled in order to make unidirectional traffic. All the nodes in the wireless LAN are stationary nodes. We implemented a proposed routing scheme by incorporating above algorithms with existing AODV as TRST_AODV. We have created third scenario same as second scenario(unreliable_Myaodv) with TRST_AODV as routing protocol with malicious nodes (encircled) and compare the route discovery time and throughput of all three scenarios[14][15].

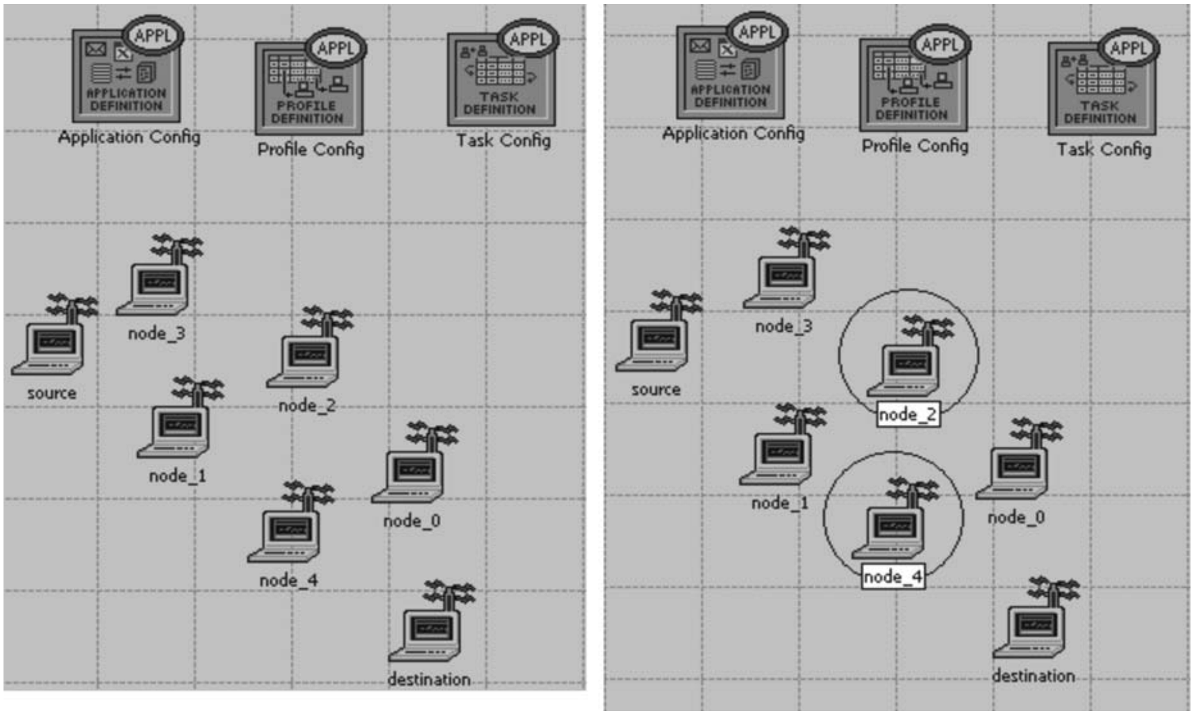

Fig. 1. (*a*) Network without malicious node (*b*) network with drop attacker(node2) and delay attacker(node4)

4. RESULTANALYSIS

In proposed trust based AODV destination node will send RREP packet (includes trust value) for each RREQ it receives. Thus source node has multiple routes from source to destination. Each route has a trust value associated with it, that is the trust value of that route. Based on this trust value route will be chosen for sending data packets. Again load of data packet transferring is distributed among n number of routes. With time the malicious nodes exhibit their behavior and neighbor nodes would notice and record it in their trust table. Thus the malicious node's trust value will be degraded with time and presence of such node in route will also degrade trust value of the whole route. We have considered two performance measurement parameters route discovery time and throughput. Table 1 shows the comparison of route discovery time and throughput of simulated network with AODV in absence of any attacker node and in presence of two attacker nodes. The third column of table shows the recorded values of the parameters in presence of attack but trust based AODV routing protocol.

The values in table shows that the route discovery time of AODV routing is increased and throughput is decreased in presence of attacker nodes. If we use our proposed Trust based AODV with attacker nodes, the route discovery time and throughput will be improved which is almost equal to normal AODV routing. This happens due to searching and using multiple route simultaneously for sending data packets. You can see that the result we get for Trust based AODV with attacker nodes are better than AODV without attackers. This is because in Trust based AODV we have searched multiple routes from source to destination and use them simultaneously to send data packets. The same results are also compared using graphs shown in figure2 and figure3.

Table 1.

	AODV with attack			*AODV without attack*			*TRU_AODV with attack*		
	Max	***Avg***	***Min***	***Max***	***Avg***	***Min***	***Max***	***Avg***	***Min***
Route Discovery ime(sec)	0.659011	0.13516	0.081265	0.254358	0.064676	0.030336	0.254358	0.044947	0.031967
Throughput (bits/sec)	10029.82	8440.343	420.7407	44522.72	36310.39	1214.37	39593.96	33172.15	1214.37

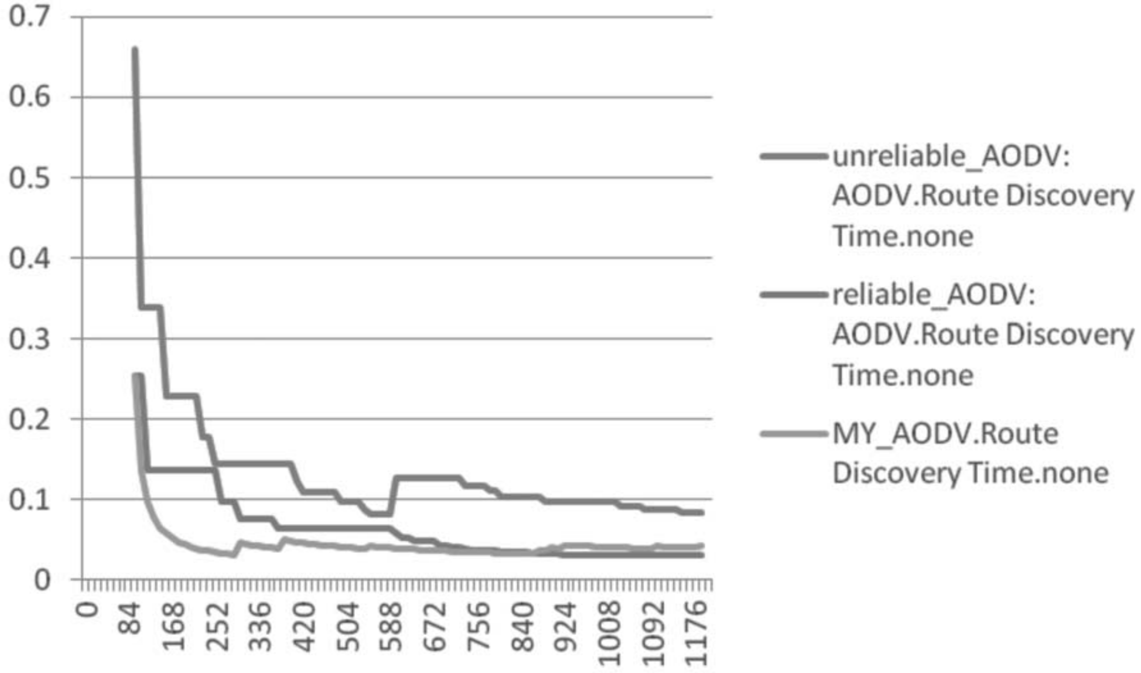

Fig. 2. Comparision of route discovery time

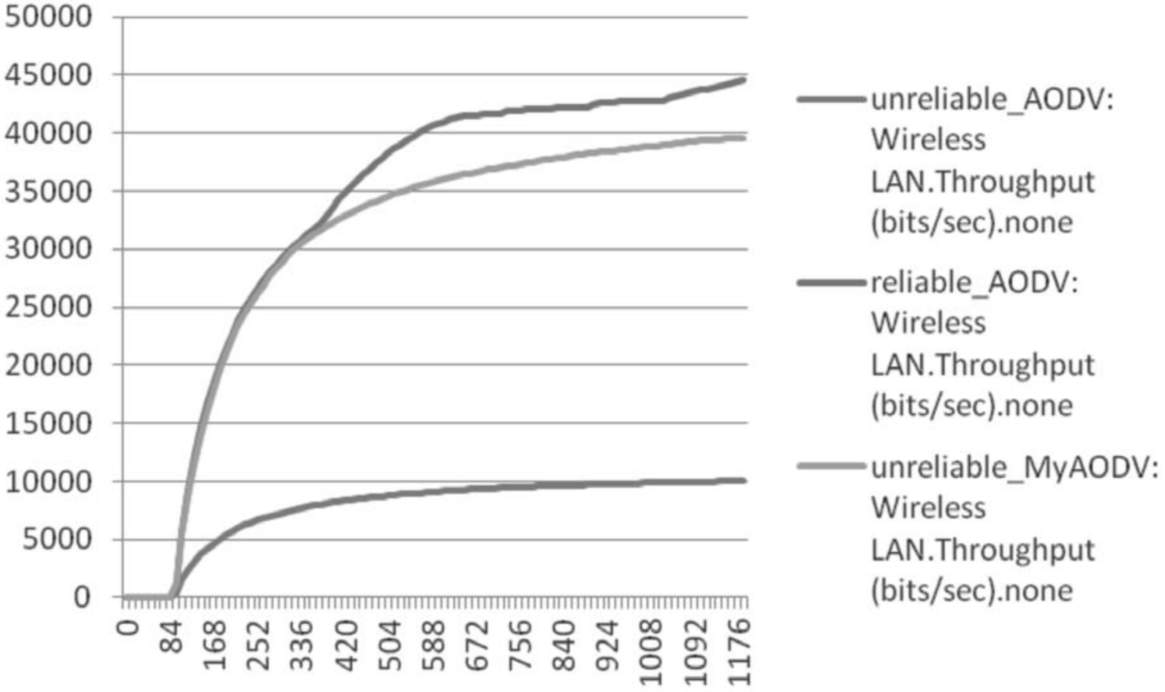

Fig. 3. Comparision of throughput

5.CONCLUSION

In our proposed trust based routing protocol we have calculated trust on each node by observing network traffic to or from each neighbor. Each node trust its neighbor node by observing their behavior. The node does not ask for recommendation from other nodes for trust worthiness of any node. Node itself take decision whether to trust a neighbor or not. Thus this is a scalable approach. The traffic monitoring and matching packets incurred some overhead which we can balance by using searching more than one route for communication. The result we obtained can show the effectiveness of our proposed scheme

6. REFERENCES

1. A boukerch, L. X.-K. (2007). Trust based security for wireless ad hoc and sensor networks. Computer communication science direct, 30, 2413-2427.
2. Gohil Bhumika, M. A. (2015). Trust based service discovery in mobile ad hoc networks. Lecture notes on Software engineering, 3(4), 308.
3. Ivan Daniel Burke, R. v. (2011). Analysing the fairness of trust based mobile adhoc network protocols(AODV and TAODV). Information Security South Africa (ISSA), 2011 . South Africa.
4. Lizi Zhang, S. J. (2012). Rubustness of trust models and combinations for handling unfair ratings . IFIPTM 2012. Surat.
5. Sonja Buchegger, J. Y. (2003). A robust reputation system for mobile ad hoc networks. EPFL-IC-LCA technical report IC/2003/50.
6. Srivastava, S. G. (2004). Reputation based framework for high integrity sensor netowrk. SASN'04 ACM 1-58113-000/00/0004. Washington DC USA.
7. Sun, M. D. (2008). probabilistic Trust management in pervasive computing. international conference on embedded and ubiquitous computing.
8. T H Lacey, R. F. (2012). RIPSec Using reputation based multi layer security to protect MANETs. Sciency direct, 31(Computer and security), 122-136.
9. Tupakula, V. B. (2008). Subjective logic based trust model for Mobile ad hoc networks. Securecomm'08 ACM ISBN 978-1-60558- 241-2, (pp. 22-25). Istambul, turkey.
10. Ulieru, Z. N. (2010). The State of the Art in Trust and Reputation Systems: A Framework for Comparison. Journal of Theoretical and Applied Electronic Commerce Research, 5(2), 97-117.
11. Vinesh H Patel, M. A. (2015). Trust based Routing in Moblie Ad hoc Networks. Lecture Notes on Software Engineering, 3(4), 318.
12. W. T. Luke Teacy, J. p. (2006). TRAVOS: Trust and Reputation in the Context of Inaccurate Information Sources. Autonomous Agents and Multi-Agent Systems, 12(2), 183-188.
13. Xiaoqi Li, M. T. (2004). A trust model based Routing protocol for Secure Ad hoc netwokrs. IEEE Aerospace Conference Proceedings.
14. J. Macker and S. Corson(1997) Mobile Ad hoc Networks (MANET), http://www.ietf.org/charters/manet-charter.html, IETF Working Group Charter
15. S. R. Das, C. Perkins, and E. Royer(2000), Performance comparison of Two On-demand Routing Protocols for Ad Hoc Networks, Proc. of IEEE INFOCOM 2000
16. K S Patel, J S shah Analysis of Existing Trust Based Routing Schemes Used in Wireless Network International Journal of Information Security and Privacy Volume 10 Issue 2 pg 26-40 April-June 2016 IGI Global
17. I R Chen, J. G. (2014). Trust management in mobile ad hoc network for bias minimization and application performance maximization. Ad hoc networks, 19, 59-74.
18. Datta, N. M. (2012). Light weight trust based routing protocol for secure ad hoc netwroks. Information Security, 6(2), 77-83
19. Guy Guemkam, D. K. (2013). ARMAN: Agent based Reputation for mobile adhoc networks. Springer-Verlag Berlin Heidelberg 2013, LNAI 7879(PAAMS 2013), 122-132