ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

IJIRSET

International Journal of Innovative Research in Science, Engineering and Technology

Volume 3, Special Issue 3, March 2014

2014 International Conference on Innovations in Engineering and Technology (ICIET'14)
On 21st & 22nd March Organized by

K.L.N. College of Engineering, Madurai, Tamil Nadu, India

Modified TSR Protocol to Support Trust in MANET Using Fuzzy

C.SenthilKumar[#1], T.Manikandan[#2], C.SebastinAlbina[#3] ,S.Shitharth[#4], Dr. N.Kamaraj[*5]

[#1]Department of CSE, Thiagarajar College of Engineering, Madurai, India.

[#2]Department of CSE, Thiagarajar College of Engineering, Madurai, India

[#3]Department of CSE, Thiagarajar College of Engineering, Madurai, India.

[#4]Department of CSE, Thiagarajar College of Engineering, Madurai, India.

[*5]Department of EEE, Thiagarajar College of Engineering, Madurai, India.

Abstract- A Mobile ad hoc network (MANET) is a self-organized system comprised of multiple mobile wireless nodes. In network topology and the absence of centralized administration in management, MANETs are vulnerable to attacks from malicious nodes. To conquer this, a Dynamic trust prediction model is proposed in this paper. This model is used to calculate the trust value, which is based on the nodes past behaviors through extensive fuzzy logic rules prediction. By using this, dishonest nodes can be eliminated, and to obtain a reliable packet delivery route that alleviate the attacks from malicious nodes. The protocol used here is Trust Based Source Routing (TSR) that provides a flexible and possible approach to choose the shortest route that meets the security requirements of data packet Transmission. Several experiments have been conducted, to evaluate the efficiency of the proposed mechanism in malicious node detection. The results show that TSR improves packet delivery ratio and reduces average end-to-end latency.

Keywords— Adhoc, Trust prediction, Source routing, Malicious node.

I. INTRODUCTION

A mobile ad-hoc network (MANET) is a wireless network with no fixed infrastructure and no central administration. Nodes in the network usually have limited resources for computation,bandwidth, memory, and energy. Because nodes are mobile, the topology of the network varies. A MANET is impossible to the lack of centralized services. Trust has been recently introduced in solving this problem and is used in existing protocols for ad hoc networks to improve security. Nodes may be deviate from the protocol for selfish or malicious reasons. Routing protocols must handle with such selfish and malicious behaviors. Trust-based Source Routing protocol (TSR), each node in a MANET predicts their neighbor's future behaviors and selects the shortest trusted route to transmit required packets.TSR protocol, which extends from Source Routing Mechanism with the extension of 'trust'. In this protocol, a source can establish multiple loop-free routes to a destination in one route discovery process, and each route has an evaluation vector composed of hop count and route trust value. A destination will respond with qualified routes as candidates that satisfy the trust requirements of transmitting data packets. The shortest one will be selected as the transmitting route.

The rest of the work is organized as follows. Section 2 summarizes the related work on the trust evaluation and trust based routing protocols. Section 3 covers the problem statement. Section 4 covers the existing system. Section 5 describes the new routing scheme in detail. Section 6 describes the implementation. Section 7 describes the x-graph. Section 8 presents the experimental results. Finally, the conclusion and future work are shown in section 9.

II. RELATED WORKS

David B.Johnson, David A.Maltz [1] proposed the dynamic source routing (DSR) protocol that can adapt to mobility of the nodes. The selected path may not be a trusted path and the overhead is high in case of route establishment.

Kamal Deep Meka, Mohit Veranda [2] Proposed a framework based on trust by using ad hoc on demand protocol (AODV) to provide a secure and reliable routing framework. The routing overhead is minimum compared to previous method and the path is selected based on trust.

Yan Lindsay Sun,Zhu Han [3] proposed a model for evaluating trust based on certain parameters, to protect against malicious attacks. The model is implemented in the distributed system and vulnerability analysis is performed.

A MANET is a self-organized multihop system comprised of multiple mobile wireless nodes with peer-to-peer relationships. The nodes in the network could not communicate with each other by well-established infrastructure, inspite of the limitation of energy; two peers out of communication range require intermediate nodes to transfer messages. Therefore a node in this network serves as a host and a router simultaneously. Each is assumed to relay packets for other nodes, and it can work well only if the nodes in the network topology, MANET often suffers from attacks by selfish or malicious nodes, such as the packet dropping (black hole) attack, selective forwarding (grey-hole)attack.

In the proposed method trust evaluation is implemented based on packet delivery ratio and the TSR protocol is implemented using the trustworthy nodes. The trustworthiness is measured using nodes historical and future behavior.

III. PROBLEM STATEMENT

To identify the reliable path between the nodes are very difficult because the energy level is low. The TSR protocol is used to improve the energy level and provide the flexible and feasible approach to choose the shortest route that meets the packet transmission.

In DSR protocol, a source node always computes an entire route for a packet to its destination. In case of a link failure, the node that cannot forward the packet to the next node sends an error message towards the source. But this is unsuited for the real time variation in trust degree. There is a requirement of improved TSR

IV. EXISTING STSTEM

The fuzzy system with three inputs namely, number of RREQ received (U), number of RREP received (R) and number of abnormal updates (A), and one output, Trust value (T). The membership functions and rule bases of the evaluator. The bases of functions are chosen so that they result in optimal value of performance measures. The first rule can be interpreted as, “If the number of RREQ received is LOW and number of RREP received is LOW and number of abnormal updates is LOW, the Trust is VERY HIGH”. Similarly the other rules are framed. Fuzzy logic-based trust evaluation gives a rational prediction of trust value and an accurate identification of malicious behavior based on fuzzy inference rules.

V. PROPOSED METHODOLOGY

A trust management model is proposed, which is divided into two parts: subjective trust evaluation model and trusted routing model. First, setup a subjective trust evaluation model considering the behaviors of the dynamic nodes in the open environment and the influencing attributes of nodes’ trustworthiness. Then through the analytic hierarchy process (AHP) decision making on the trust influencing attributes, trust value is obtained for each node. The value not only provides a relative identification between the good nodes and the malicious or suspected nodes, but also offers a prediction of one’s future behaviors. Then taking the trust value as the input, a trusted routing model is proposed, by using this we can eliminate the untrustworthy nodes, obtain a reliable packet delivery route and alleviate the attacks from Malicious nodes, which is called as Trust Based Source Routing (TSR). As an application of the proposed trusted routing algorithm, a reactive routing protocol on the basis of the standard DSR protocol is proposed. Based on the fuzzy dynamic programming theory, in trusted routing model, we present a trusted routing algorithm which can kick out the untrustworthy nodes such that a reliable passage delivery route is obtained. Moreover, FTDSR guarantees a higher packet delivery ratio and network throughput effectively compared when other protocols

VI. IMPLEMENTATION

MANETs is a collection of mobile nodes connected with wireless links. MANET has no fixed topology as the nodes are moving constantly from one place to another place. All the nodes must cooperate with each other in order to route the packets. In a mobile ad hoc network (MANET),a source node must rely on other nodes to forward its packet on multi-hop routes to the destination.

In DSR protocol, a source node always computes an entire route for a packet to its destination. In case of link failure, the node that cannot forward the packet to the next node sends an error message towards the source. But this is unsuited for the real time variation in trust degree.

Initially the MANET network should be setup in the NS2 simulator and the network is configured before the implementation of the proposed TSR protocol. Because of the link stability and route lifetime, no route overhead was considered in the simulation. In 1000X1000 areas, mobile nodes exist. Square area is used to increase average hop length of a route with relatively small nodes. Every mobile node is moving based on mobility data files that were generated by mobility generated module. The transmission range is fixed at 250 meters, 40 nodes of them have destinations and try finding route to their destination and try finding routes to their destination nodes. Maximum speed of node is set to 10 m/sec. All nodes do not stop moving, and the simulation time is 500 sec.

The figure 1 used to shows the overall process flow of the implementation of the proposed method. After the initial setup of the network the route discovery algorithm is implemented to identify the path between the nodes for data transmission.

Network formation is done in order to discover the route. The network flow information is stored in route cache and information will be retrieved when needed .For each node the trust value is calculated, then the results of the trust value is compared with the threshold value. If the computed value is less than the 0.7 it will considered as the trusted node, otherwise it is untrusted node.

During Route Discovery, the source node broadcasts a route request packet with a recorded source route listing only itself. Each node that hears the route request forwards the request (if appropriate), adding its own address to the recorded source route in the packet. The route request packet propagates hop-by-hop outward from the source node until either the destination node is found that can supply a route to the target. If the status of a link or node changes, the periodic updates will eventually reflect the change to all other nodes, resulting in the computation of new routes. However, using route discovery, there are no periodic messages of any kind from any of the mobile nodes .Instead, while a route in a use, the route maintenance procedure monitor the operation of the route and informs sender any routing errors. Route maintenance can also be performed using end-to-end acknowledgements rather than the hop-by-hop acknowledgements.

The trust of each node is calculated by using the behavior of the node with respect to the past history and the current transfer rate of the node. The nodes with higher trust values are selected for the route during the route discovery phase. Each node analyzes the behavior of all its neighboring nodes for evaluating the trust. If there is any misbehavior detected for any node then the trust of that particular node will be degraded. The trust is calculated by using the forwarding nature of the node. If a node can forward all the packets to the right destination then it can be said as a more trustworthy node. The trust can be calculated by using the formula [5] provided in Eq.(1).

$$TV(sd) = W1 * CPR + W2 * DPR \quad (1)$$

Where W1 and W2 are the weighting factor, CPR is the control Packet Ratio that shows the amount of control packets forwarded by the node and DPR is the Data Packet Ratio that shows the amount of data packets forwarded respectively.

And the route path trust can be calculated by using the formula in Eq. (2).

$$RouteTV(ij) = \prod(\{TVsd(t) \mid Vs, Vd \in p \,\&\, Vs \rightarrow Vd\}) \quad (2)$$

Where Vi and Vj are the two adjacent nodes. Vs is the source node and Vd is the destination node.

Before a source sends a data to the destination a route should be established. The source looks for the route cache for any possible available routes. The path trust of the selected route should be greater than the data transmission needed. If there is no such route available in the route cache then the source s initiates a route discovery process to the destination d. After identifying the routes they are added to the route cache automatically, the path that satisfy the path trust and has the smallest number of hop will be selected as the route for data transmissions. If more paths have the same distance then the path with highest trust value is selected. During the route discovery process a node can identify malicious nodes by using the local trust record list available for all the neighbor nodes and on that it selects a path with good trust.

There is also a need for route maintenance in the TSR protocol in case of any route failure. If any node in the route fails then the neighboring node will broadcast the message to all the other nodes to identify a new path. Since a node will know if there is a path to the destination through its neighbor, broadcasting will be useful to identify an alternate route faster. Loops can be avoided and the maintenance overhead is less since it is an on-demand protocol.

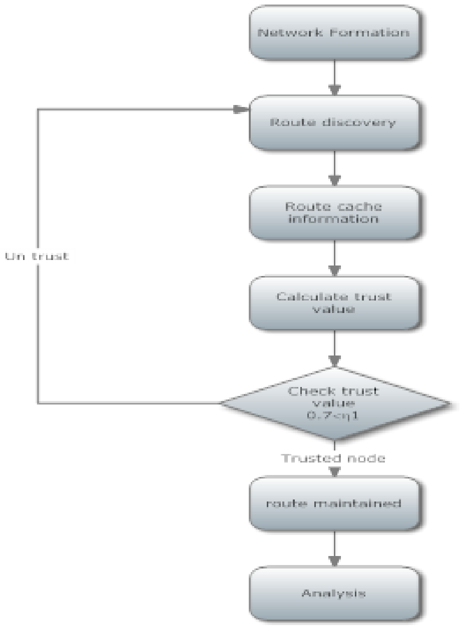


Figure 1.The process flow diagram

VII X-GRAPH

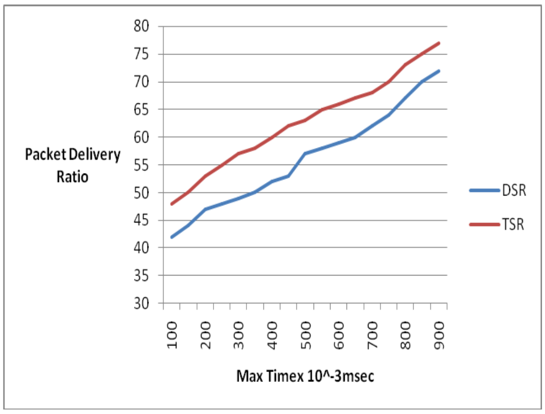
X Graph is an x-window application that includes: Interactive plotting and graphing Animated and derivatives to use graph in NS-2, the executable can be called within a TCL script. This will then load a graph displaying the information visually displaying the information of the file produced from the simulation. The output is a graph of size 800x400 displaying information on the traffic flow and time.

7.1 Performance metrics

We use five metrics to evaluate the performance of this routing protocol [5], in which the first two metrics are the most important for best effort route and transmit protocols.

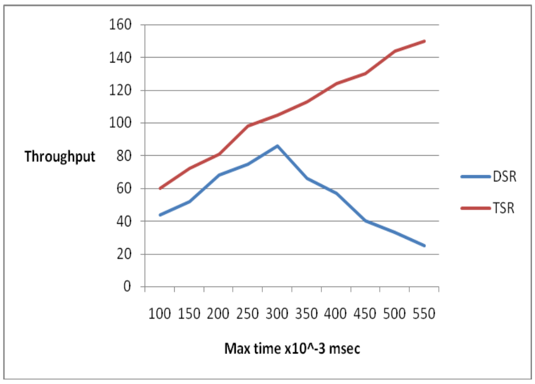
(1) Packet delivery ratio: the division of the data packets delivered to destination nodes to those sent by source nodes.
(2) Average end-to-end latency: the average time taken by the data packets from sources to destinations, with buffer delays during a route discovery.
(3) Routing packet overhead: the ratio of the number of control packets (including route request/reply/update/error packets) to the number of data packets.
(4) Network throughput: throughput indicates the amount of digital transmitted per unit time from source to destination
(5) Detection ratio: the ratio of the number of nodes whose behavior (malicious) is identified correctly to the actual number of such nodes in the network.

VIII. EXPERIMENTAL RESULTS



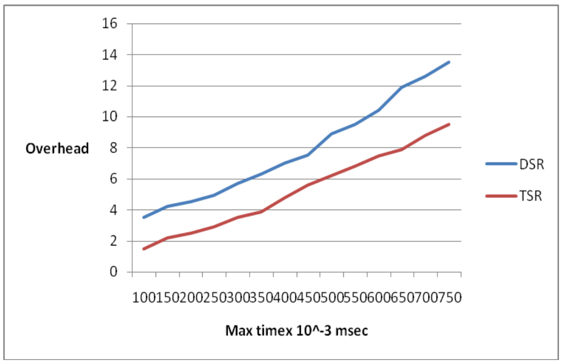
(a) Packet delivery ratio

The packet delivery ratio increases with increase in the time of the nodes. Also the delivery ratio in TSR protocol is higher compared to the normal DSR approach thus increasing the efficiency of the TSR protocol.



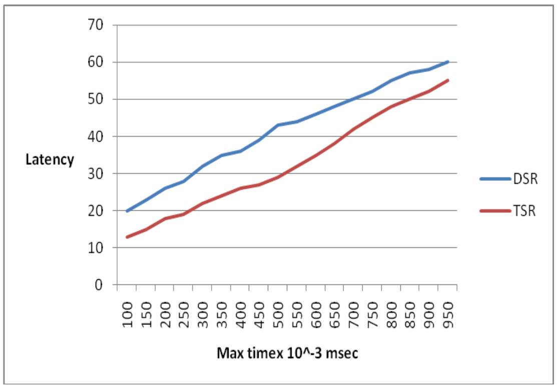
(b) Throughput

The overall throughput of the TSR routing protocol also increases with the maximum time compared to the DSR protocol. In DSR as the time increases the throughput drops rapidly at certain instances.



(c) Overhead

The overhead of the routing protocol determines the performance. The overhead is less in TSR comparing to that of the overhead in DSR protocol used. So the performance is more in TSR protocol for increasing time of the nodes.



(d) Latency

The latency or the delay in TSR protocol is less compared to that of the normal DSR protocol. The increasing time of the nodes reduces the latency in TSR protocol.

IX. CONCLUSIONS

The main issues in MANETs are the establishment of the secure and reliable path for communication. Due to the interruptions from malicious nodes there is packet loss and misbehavior of nodes. In this paper, the TSR protocol is proposed to establish a trustworthy path for communications by using the calculated trust value of each node based on their behavior. This way the malicious node can be identified during packet loss. By calculating the trust for route establishment the packet delivery ratio is increased and end to end latency is reduced. From the analysis it shows that the efficiency and performance of the TSR protocol is more compared to DSR protocol. In future the energy consumptions of each node can be calculated and this can also be used as criteria for implementing the routing algorithm.

REFERENCES

[1] D.Johnson, D. Maltz, Dynamic source routing in ad hoc wireless networks, in: I.Tomasz, K.Hank (Eds.), Mobile Computing,first ed., Kluwer Academic Press, 1996, pp. 153-181.

[2] K.Meka,M.Virendra,S.Upadhyaya,Trust based routing decisions in mobile ad-hoc networks, in:proceeding of the Workshop on secure knowledge Management(SKM 2006),2006.

[3] Y.L. Sun, W. Yu, Z. Han, K.J. Ray Liu, Information theoretic framework of trust modeling and evaluation for ad hoc networks, IEEE Journal on Selected Areas in Communications 24 (2) (2006) 305–319.

[4] E.M. Royer, C.K. Toh, A review of current routing protocols for ad hoc mobile wireless networks, IEEE Personal Comminations Magazine 6 (2) (1999) 46–55.

[5] Hui Xia, Zhiping Jia, Xin Li. Edwin H-M.Sha, Trust prediction and trust-based source routing in mobile ad hoc networks, Journal for Elsevier (2012).

[6] W.L.H. Deng, D.P. Agrawal, Routing security in wireless ad hoc networks, IEEE Communications Magazine (2002) 70–75.

[7] A.A. Pirzada, C. McDonald, A. Datta, Performance comparison of trust-based reactive routing protocols, IEEE Transactions on Mobile Computing 5 (6) (2006) 695–710.

[8] H. Xia, Z. Jia, L. Ju, X. Li, Y. Zhu, A subjective trust management model with multiple decision factors for MANET based on AHP and fuzzylogic rules, in: Proceedings of 2011 IEEE/ACM International Conference on Green Computing and Communications (GreenCom2011), 2011, pp. 124–130.

[9] C. Bettstetter, G. Resta, P. Santi, The node distribution of the random waypoint mobility model for wireless ad hoc networks, IEEE Transactions on Mobile Computing 2 (3) (2003) 257–269

[10] J.Manickam,Leo Martin,S.Shanmugavel, Fuzzy based trusted ad hoc on-demand distance vector routing protocol for MANET, Advanced Computing and Communications(2007) 414-421.

[11] H.Xia,Z.Jia,L.Ju,Y.Zhu,Trust management model for mobile ad hoc networks based on analytic hierarchy process and fuzzy theory,IET Wireless Sensor System 1(4) (2011) 248-266.

[12] 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.

[13] X. Li, Z. Jia, P. Zhang, R.Zhang, H. Wang, Trust-based on-denand multi path routing in mobile ad hoc networks, IET Special Issue on Multi-Agent & Distributed Information Security 4(4) (2010) 212-223.

[14] C.E. Perkins, E.M.Royer,Ad-hoc on-demand distance vector routing,in:Proceedings of International Workshop on Mobile Computing System and Applications (WMCSA),New Orleans,Louisiana,USA February 1999,pp.90-100.

[15] J.Lundberg, Routing Security in Ad hoc Networks,Technical Report Tik110.501,Helsinki University of Technology ,2000