VOL. 11, NO. 13, JULY 2016 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences


www.arpnjournals.com

# SECURE QUALITY OF SERVICE AWARE ROUTING IN MANET BASED ON COLLABORATIVE TRUST MODEL

D. R. Jiji Mol[1] and S. Behin Sam[2]
[1]Department of Computer Science, Bharathiar University, Coimbatore and Assistant Professor, Department of Computer Science, S.R.M Arts and Science College, Kattankulathur, Chennai, India
[2]Department of Computer Science, R. V. Government Arts College, Chengalpattu, Tamil Nadu, India
E-Mail: behinsam@gmail.com

**ABSTRACT**

Mobile ad hoc network (MANET) is a self-organised system comprised of mobile wireless nodes. All nodes act as both communicators and routers. Due to the absence of centralised administration in MANETs, communications between nodes are vulnerable to attacks by malicious nodes. In order to decrease the hazards from malicious nodes, recently researchers have given more importance to the concept of trust and recommendation in MANETs. In these models, the recommendations are prone to issues such as recommender's bias, honest-elicitation, and free-riding. In this paper we have tried to build a simple collaborative trust model to minimize those issues. This model is used to evaluate the trust of a node based on the trust value given by the neighbours. Weights are given to the trust value based on the trust degree of neighbours. The data packets get forwarded towards destination through the path having greatest trust value. The effectiveness and efficiency of the algorithm is demonstrated through an extensive simulation experiment and results are analyzed based on the Quality of Service metric.

**Keywords:** collaborative trust, routing, MANET.

## INTRODUCTION

In the last decade, researchers have explored many potential applications of mobile ad hoc networks (MANETs), which are usually deployed in harsh or uncontrolled environments. Due to the intrinsic characteristics (e.g., wireless medium, openness, the absence of a fixed infrastructure), such networks are vulnerable to a wide variety of attacks. Routing is a very important function in MANETs, which is productive unless all component nodes operate by a trustworthy manner. However, this is not always the case. The protocols used in this function are designed for minimizing the level of overhead and allowing every node to participate in the routing process, while usually not designed with security in mind and often are very vulnerable to node misbehaviours. Moreover, making routing protocols efficient often increases the security risk of the protocol and allows a single node to significantly impact the operation of the protocol because of the lack of protocol redundancy. An adversary or a malicious node can easily launch attacks on this important function, especially attacks on the packet routing (e.g., gray-hole, black-hole, cheating, or modification attack).

The normal communications in network may be prohibited or hindered due to these attacks. The distribution of false routing information may cause the potential of denial of service attacks, unintended network routing loops, or other nonfunctional routes. Therefore, the security of routing protocol is an important area that needs to be addressed for such networks to widespread adoption.

To address the above issues, a variety of security-considered routing protocols have been proposed. The motivation of designing these protocols is that the networks need to determine the validity and safety of routing information prior to making routing decisions (Govindan and Mohapatra, 2012). Basing on the protection way of reducing or eliminating malicious attacks, these protocols can be classified into two types, secure routing protocol and trust-based routing protocol. Most of the secure routing protocols use cryptographic primitive techniques to secure the routing information.

However, the disadvantage of using cryptographic tools is that the computational resource is very expensive, which is not suitable to be used in the resource-constrained mobile devices. These protocols create new avenues for denial of service (DoS) attacks in the attempt to prevent some other attacks (Li *et al*., 2012; Wang *et al*., 2011). Besides, several such secure routing protocols presume the existence of a centralized or distributed trusted third party, while this party actually violates the nature of self-organization (Wang *et al*., 2011). Moreover, such protocols usually cannot prevent the malicious attacks from malicious or compromised nodes which have been authorized as the participants in network from doing misbehaviors. Thus, it is becoming more acceptable to consider trust-based routing as a viable security solution.

Such trust-based routing protocols attempt to establish trusted routes rather than shortest routes as is done in traditional routing protocols, which make tradeoff between the trustworthiness and the performance of networks. The establishment of such protocols contains two important segments, trust model and trust-enhanced routing strategy. Every node in the network independently executes a designed trust model.

The task of trust model is to periodically quantify and establish the trustworthiness among entities based on some trust metrics or trust computational methods (Govindan and Mohapatra, 2012; Li *et al*., 2012; Wang *et al*., 2011; Liang and Shi, 2008; Xia *et al*., 2013a, 2013b;


Velloso *et al*., 2010; Cho *et al*., 2011; Cho and Chen, 2013; Carullo *et al*., 2013; Elgohary *et al*., 2014; Onolaja *et al*., 2011). The estimated trust value can be directly applied to ensure proper operations, such as routing decision, authentication, access control, malicious node detection, and intrusion detection system (Deb and Chaki, 2012).

Thus, in this paper we propose a collaborative trust model to predict the trust of intermediate nodes in the path/paths between source and destination. The trust values are then used by our trust based routing protocol which is simple, efficient and effective. This causes the proposed protocol to increase the quality of service of MANET.

## BACKGROUND STUDY

Over the last few years, a number of trust-based schemes, trust-based systems and trust-based applications have been developed. As we are planning on adopting trust in MANETs, we firstly focus our attention on some trust models, and subsequently do a deep research on the modifications of routing strategy proposed in trust-based routing protocols.

### Trust models in MANETs

By analyzing the existing trust models, we can see that although a lot of work has been done on the trust quantification, the research on trust is far from enough. A detailed survey on various trust computing approaches was presented (Govindan and Mohapatra, 2012). The summary and comparisons of these approaches were highlighted. The following contents are some efficient schemes used for estimating trust in MANETs found in the different references.

Observing a node's historical behaviors (e.g., packets delivery ratio, fully cooperation, bandwidth, residual energy and CPU usage) is an effective measure which is used to judge whether an interest entity is credible or not. In order to compute an interest entity's trust, we can introduce some polymerization mechanisms to aggregate these observations. The authors in (Li *et al*., 2012) argued that in general, this trust problem could be viewed as an instance of detecting nodes whose behavior was an outlier when compared with others. The search, evaluation, propagation, and evolution among each entity are combined to provide an independent trust evaluation model for a MANET (Wang *et al.*, 2011); trust was determined only by self-relevant knowledge. At present, most of the trust evaluation frameworks belong to a recommendation-based methodology such that the evaluation results are heavily dependent on the accurate measurement of the behaviors of neighboring entities and on the degree of honesty of the raters (Wang *et al*., 2011). Most researchers are advocating the use of recommendation and prefer making use of recommendation aggregation algorithms to quantify 'trust' from several aspects. The authors (Liang and Shi, 2008) proposed a judgement that whether the recommendation plays the same positive effect in the open computing environment as that used in human society. Then the persuasive experiments shown the problems existed in such mechanisms are that the recommendation is not always as helpful as what we expected, especially when the system is facing highly dynamic peer behaviors and malicious raters. Besides, such mechanisms put too much time and energy on the design of a complex recommendation aggregation measure, at the same time also increase the load of network entities. In paper (Xia *et al.*, 2013a), a monitoring entity may get recommendation experience by trust propagation along multiple directed recommending paths. By using the trust attenuation rules and the recommending path weighting rules proposed in this paper, this monitor can calculate these recommending paths' general weights and get the final recommendation.

(Velloso *et al*. 2010) proposed a human-based model which described a maturity-based trust relationship between entities for MANETs. The trust-based scheme aimed to isolate or discourage selfish behaviors of participating nodes. In (Cho *et al.* 2011), the authors sought to combine the notions of 'social trust' derived from social networks with 'quality-of-service (QoS) trust' derived from information and communication networks to obtain a composite trust metric. Then they proposed an improved trust model in paper (Cho and Chen, 2013). In this new model their interest is not so much in isolating selfish nodes but in quantifying the tradeoff between individual and global welfare, allowing each node to adapt to network dynamics and node status. Security in ubiquitous environment is a field that is growing up fast and spans across several fields. The authors in (Carullo *et al*. 2013) proposed a novel approach that establishes trust leveraging users' profiles. The information enables a task-aware trust model, namely a finer-grained model in which users are classified as trusted or not depending on the intended business activity. A recommendation subsystem based on the Wilson score confidence interval was introduced for the purpose of enabling the system to recognize malicious users. Two fundamental parameters (trust value and reputation value) were used in (Elgohary et al. 2014). The nodes with highest trust values are used to build the headship induction table and the high value of reputation of a node signifies that the node is trusted and is more reliable for data communication purposes.

In order to forecast trust for future decision making, (Onolaja *et al*. 2011) proposed a reliable and novel dynamic framework that utilized a data-driven approach for trust management. The framework used past interactions, recent and anticipated future trust values of every identity in the domain. In order to reduce the hazards from such nodes and enhance the security of network, the authors present a dynamic trust prediction model to evaluate the trustworthiness of nodes, which is based on the nodes' historical behaviors, as well as the future behaviors via extending the fuzzy logic rules prediction method (Xia *et al*., 2013b).

**Trust-based routing protocols in MANETs**

Applying trust mechanisms to routing strategy in MANETs is an intensive research field, and numerous solutions have been proposed. The selection of next hop or forwarding path is made according to the trust feedback information.

A light-weight trust-based routing protocol was presented in (Marchang and Datta 2012). With the benefits of consuming limited computational resource and ensuring scalability, the intrusion detection system (IDS) and the local information were used to estimate the trust. They integrated the proposed trust approach into the standard AODV and gave the performance analysis. In paper, (Eissa *et al*. 2013), by utilizing the friendship measure, the authors proposed a trust-based scheme for securing AODV routing protocol. Before forwarding the data through the candidate routes, the sending nodes can evaluate the available routing paths according to some selected features (e.g., identity information or node reputation). The authors applied a simple trust approach into the source routing mechanism (Xia *et al*., 2013b). The novel on-demand trust-based unicast routing protocol provides a flexible and feasible approach to choose the shortest route that meets the security requirement of data packets transmission. Then they made some improvements on the former trust model (Xia *et al*., 2013a), and proposed an on-demand trust-based multi-path routing protocol (AOTMDV) (Deb and Chaki, 2012), in which two novel trust mechanisms were proposed. Firstly, the Message Authentication Code (MAC) mechanism was used to protect the new fields added in the routing control packets. Secondly, in order to cope with the frequent changes of route trust, the route trust update mechanism was proposed. One of the main contributions in paper (Wang et al. 2011) was to enable a feasible delivery method for defending against possible selfish and malicious behaviors rather than just securing routing protocol messages. Furthermore, the authors proposed a new routing framework in a MANET based on a sophisticated trust model. The authors proposed a new mechanism termed as ASHFIK (Elgohary *et al*., 2014), which was used to make the routing protocol capable to maintain the group communications. In this mechanism, a new trusted core node is always ready to replace the original core node when it goes down. (Cho and Chen 2013) proposed and analyzed a trust management protocol for group communication systems where selfish nodes exist and system survivability is highly critical to mission execution. Rather than always encouraging altruistic behaviors, they considered the tradeoff between a node's individual welfare vs. global welfare. Moreover, in order to balance selfish vs. altruistic behaviors, they also identified the best design condition of this behavior model. The authors in (Mohanapriya and Krishnamurthi 2014) designed a routing solution that enables the dynamic source routing protocol to find a secure end-to-end route free of black hole nodes with the cooperation from the neighbors. Also this solution can protect the network in the presence of colluding attackers without the need of promiscuous monitoring the neighbor nodes.

**COLLABORATIVE TRUST MODEL (CTM)**

In this section we are proposing a model for predicting trust of other nodes with the help of trust values given by neighbours in a collaborative way. We started to define the CTM by first adopting the strategy of (Golbeck *et al*., 2005). Here we use the information coming from other collaborative nodes of the network. The users of the networks give trust scores to other nodes within its transmission range which indicate how much they trust each other. In general, $t_{a,u}$ is a number between 0 and 1 which indicates to what extent $a$ trusts $u$. Instead of just using the baseline strategy of simply computing the average rating, we use a weighted mean method for computing a trust of a node. Here we assign more weight to ratings of highly trusted users which help us to differentiate the sources. The following equation is used to compute the trust of a node:

$$T_{u,s} = \frac{\sum_{a \in R} t_{a,u} w_{u,s}}{\sum_{a \in R} t_{a,u}} \quad (1)$$

In the above equation $T_{u,s}$ represents trust value of node u computed by source node s, R represents the set of users who evaluated node u for which they have given $t_{a,u}$, and $W_{u,s}$ represents the weight given by source node s to the trusted users u. The rationale behind this strategy given in equation 1 is to compute the weighted mean of the ratings given by trustworthy neighbours. In our trust model, trust values are limited in a continuous range from 0 to 1 (i.e. $0 \leq t_{au} \leq 1$). The trust value of 0 signifies complete distrust whereas the value of 1 implies absolute trust. The weights are assigned based on the trust value of the raters and the levels of rater nodes trust are listed in Table-1.

**Table-1.** Trust level of nodes.

| Trust level | Meaning | Weight value |
|---|---|---|
| 1 | Poor trust worthy node | 0.5 |
| 2 | Fair trust worthy node | 0.75 |
| 3 | Average trust worthy node | 0.85 |
| 4 | Trust worthy node | 1 |

We can also further enhance equation 1 by only taking into account trustworthy neighbors-that is, users denoted by $R^+$.

$$T_{u,s} = \frac{\sum_{a \in R^+} t_{a,u} w_{u,s}}{\sum_{a \in R^+} t_{a,u}} \quad (2)$$

When a source node s discovers a path to a destination node d with the help of the multi-hop

forwarding nodes, the trust degree of the path should be computed according to the trust value $T_{u,s}$ of each node along the path. Consequently, the trust degree of a route depends on the trust value of all the nodes on the route. Let $TP_r$ be the trust path of route r, consisting of m nodes which may be represented by a sequence {1, 2, . . . , m}, where node u denotes the $u^{th}$ node in the sequence. Then, the trust path of route r, is to be computed as follows

$$TP_r = \prod_{u=1}^{m} T_{u,s} \quad (3)$$

**ROUTING BASED ON CTM (RBCTM)**

The routing protocol RBCTM proposed in this section contains seven steps as follows:

**Step 1:** Before a source *s* send a data packet to another node, say node *d*; the source looks up in the local routing table a route entry to node *d*. The qualified route should contain only the nodes that meet the trust requirement of the source. If such routes are found, go to step 3.

**Step 2:** If there is not such a route, node *s* initiates a route discovery for *d*. If one or more paths are discovered, a route entry for these paths will be created and inserted into the routing table of node *s*.

**Step 3:** Node *s* selects the route with greatest trust reliability.

**Step 4:** If not a trust reliable route is selected, node *s* will return no qualified routes.

**Step 5:** If a qualified route is selected node *s* forwards the date packets through node *u*.

**Step 6:** If the packet is forwarded correctly by node *u*, node *a* assigns a trust value $t_{a,u}$ for node *u* in its trust record list. The procedure is over.

**Step 7:** If the packet is not forwarded correctly by node *u*, then also assign a reduced trust value $t_{a,u}$ for node *u* and Go to step 2.

**Route discovery and path selection**

In this sub section packet fields for route discovery and path selection process is proposed. Route discovery is launched when no trusted routes exist. The node will initiate a network-wide flood by broadcasting a route request packet and wait for route reply packets.

**Route request:** A route request is initiated by the RREQ packet which contains the following fields: <Broadcastid, SourceAddr, SourceSequenceNo, DestAddr, DestSequenceNo, HopCounter, TrustAssigneeNodeNo, AssignedTrust >. The first six fields are similar to the corresponding ones in AODV (Perkins C.E *et al*., 1999). We have added two additional fields namely TrustAssigneeNodeNo and AssignedTrust.

**Route reply:** The intermediate node replies to an RREQ only when it has a route with a sequence number that is greater than that contained in the RREQ. If it does have a fresh route to the destination and the RREQ has not been processed previously, the node unicasts a route reply (RREP) packet back to its neighbour from which it received the RREQ. An RREP packet contains the following information: <SourceAddr, SourceSequenceNo, DestAddr, DestSequenceNo, HopCounter, LifeTime, TrustAssigneeNodeNo, AssignedTrust >. The first six fields are similar to the corresponding ones in AODV (Perkins C.E *et al*., 1999). We have added two additional fields namely TrustAssigneeNodeNo and Assigned Trust.

**Route maintenance:** A node maintains and updates its routing table when receiving an RREQ, RREP or route error (RERR) packet. In addition, a new trust route update (TRU) packet is used to update the trust of nodes in a route.

**Trust route update:** An TRU packet contains the following fields: <BroadcastId, SourceAddr, Source SequenceNo, UpdateDestAddr, UpdateDestSequenceNo, UpdateHopCounter, UpdateNodeTrust> where UpdateHop Counter represents the count of nodes in the path and UpdateNodeTrust denotes the new trust value of the nodes in the path from SourceAddr to UpdateDestAddr.

**Route error:** When a link failure is detected, an RERR is sent back to all sources using that broken link. An RERR packet contains the following fields: <BroadcastId, SourceAddr, SourceSequenceNo, DestCount, UnreachableDestList> where DestCount represents the count of unreachable nodes and UnreachableDestList is composed of the address and the sequence number of unreachable nodes in the source node's neighbours. The corresponding route entries are removed by an RERR along its way. Only when there is not a qualified route entry to the destination that a node needs to send packets to, the node initiates a new route discovery.

**RESULTS AND ANALYSIS**

**Experiment setup**

NS-2.35 (http://www.isi.edu/nsnam/ns/, 2012) is adopted to evaluate the performance of trust-based protocols in different conditions. Our simulation models a network of 40 mobile hosts placed randomly within a 1000 m Â 1000 m area. Radio propagation range for each node is 250 m and channel capacity is 2 Mbits/s. Each simulation executes for 600 s of simulation time. We take an un-slotted Carrier Sense Multiple Access protocol with Collision

Avoidance (CSMA/CA) to transmit data packets as well routing packets (Shen et al., 2015). The IEEE 802.11b Distributed Coordination Function (DCF) is used as the medium access control protocol. A traffic generator is developed to simulate constant bit rate sources. The size of data payload is 512 bytes. The node mobility uses the random waypoint model. In the following tests, malicious

nodes can launch two simple types of routing attacks, i.e., gray-hole and black-hole attacks. In the former one, malicious nodes selectively forward data packets at a ratio of 35, and in the latter one, malicious nodes drop all data packets, but both of them deliver route request and reply packets devotedly.

Three Quality of Service (QoS) metrics from (Velloso *et al*., 2010) are used to evaluate the performance of the routing protocols: (1) Packet delivery ratio: the fraction of the data packets delivered successfully at destination nodes to those sent by source nodes. This ratio represents the efficiency of routing; (2) Average end-to-end latency: the average time taken by the data packets from sources to destinations, including buffer delays during a route discovery, queuing delays at interface queues, retransmission delays at MAC layer and propagation time; (3) Routing packet overhead: the ratio of the number of control packets to the number of data packets. This metric is used to investigate how efficiently control packets are utilized in delivery data packets.

**Routing based On CTM evaluation**

We simulate and compare our proposed routing model RBCTM with the following schemes: the AOTMDV (Xia *et al.*, 2013a) and LTB-AOMDV (Deb and Chaki, 2012). To assess the performance of these protocols, we choose suitable parameters and simulate the routing by increasing the number of malicious nodes and the results are shown in the following Figures 1-3.

In a normal network without any malicious node, the packet delivery ratio is approximately the same in each protocol. This ratio of LTBAOMDV degrades sharply as the number of malicious nodes increases from 0 to 10, as shown in Figure-1, while this indicator of RBCTM drops smoothly. The delivery ratios of RBCTM is always much higher than that of, LTBAOMDV and AOTMDV. The reason is that, RBCTM the source nodes has the ability to quantify the trust for each node in the path and select the trustworthy path to transmit data stream, and therefore the delivery ratio is improved.

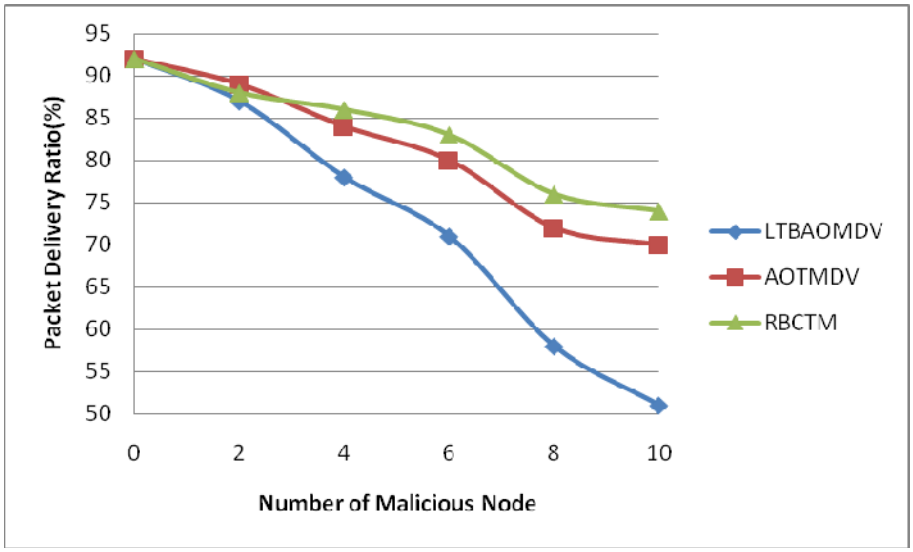


**Figure-1.** Packet delivery ratio.

With the increasing number of malicious nodes, the average end to end latency in RBCTM ascends slowly while the average latency in LTBAOMDV ascends sharply, as shown in Figure-2. The routing paths established by RBCTM mechanism eliminate the influence of malicious nodes thereby causing less end-to-end delay.

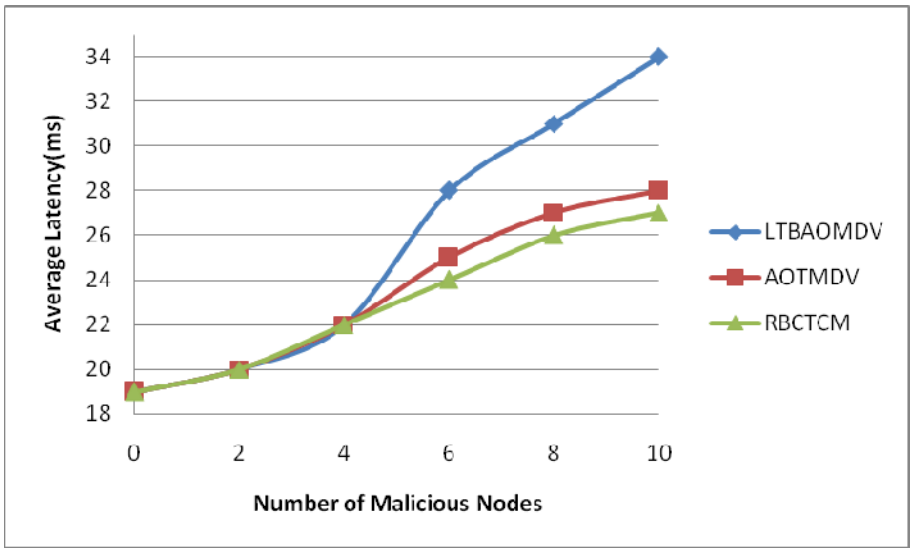


**Figure-2.** Average end to end latency.

As shown in Figure-3, the routing packet overhead of RBCTM is much less compared to LTBAOMDV and AOTMDV. The difference becomes more apparent as malicious nodes increases. The main reason being usage of less control packets than the other protocols causes decrease in routing overhead.

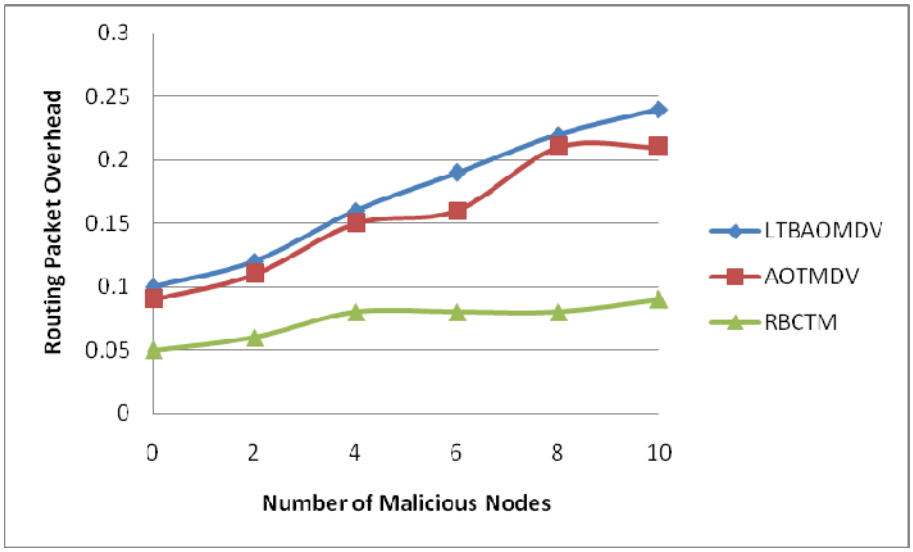


**Figure-3.** Routing overhead.

## CONCLUSIONS

Thus we have established a collaborative trust model, on the basis of trust recommended by the neighbours. This model is used for routing data packets between nodes through the path having high reliable trust. The simulation results has clearly shown that the proposed secure routing algorithm based on collaborative trust model is very effective and efficient and increases the quality of service of MANET.

## REFERENCES

Cho J, Swami A, Chen I. 2011. A survey on trust management for mobile ad hoc networks. IEEE CommunSurvTutor. 13(4): 562-583.

Cho J, Chen I. 2013. On the tradeoff between altruism and selfishness in MANET trust management. Ad Hoc Netw. 11(8): 2217-2234.

Carullo G, Castiglione A, Cattaneo G, De Santis A, Fiore U, Palmieri F. 2013. FeelTrust: providing trustworthy


communications in ubiquitous mobile environment. In: Proceedings of the IEEE 27th international conference on advanced information networking and applications (AINA). pp. 1113-1120.

Chen IR, Bao FY, Chang M, Cho JH. 2014. Dynamic trust management for delay tolerant networks and its application to secure routing. IEEE Trans Parallel Distrib Syst. 25(5): 1200-1210.

Deb N, Chaki N. 2012. TIDS: trust-based intrusion detection system for wireless ad-hoc networks. Comput Inf SystInd Manag. 7564: 80-91. 127.

Elgohary Ashraf, Sobh Tarek S, Nouh Sayed A, Zaki M. 2014. An efficient and dependable protocol for critical MANETs. J High Speed Netw. 20(3): 153-168.

Eissa T, Razak S, Khokhar R. 2013. Trust-based routing mechanism in MANET: design and implementation. Mobile Netw Appl. 18(5): 666-677.

Golbeck J.A. 2005. Computing and Applying Trust in Web-Based Social Networks. Doctoral thesis, Univ. Of Maryland, College Park.

Govindan K, Mohapatra P. 2012. Trust computations and trust dynamics in mobile adhoc networks: a survey. IEEE Commun Surv Tutor. 14(2): 279-98. http://www.isi.edu/nsnam/ns/; 2012 [accessed December, 2012].

Li W, Parker J, Joshi A. 2012. Security through collaboration and trust in MANETs. Mobile Netw Appl. 17(3): 342-352.

Liang Z, Shi W. 2008. Analysis of ratings on trust inference in open environments. Perform Eval. 65(2): 99-128.

Marchang N, Datta R. 2012. Light-weight trust-based routing protocol for mobile ad hoc networks. IET-Inf Secur. 6(2): 77-83.

Mohanapriya M, Krishnamurthi I. 2014. Trust based DSR routing protocol for mitigating cooperative black hole attacks in ad hoc networks. Arab J Sci Eng. 39(3): 1825-1833.

Onolaja O, Bahsoon R, Theodoropoulos G. 2011. Trust dynamics: a data-driven simulation approach. Trust Manag. 358: 323-334.

Perkins C.E, Royer E.M, Das S. 1999. Ad-hoc on demand distance vector routing'. Proc. Int. Workshop on Mobile Computing Systems and Applications (WMCSA), New Orleans, LA, USA. pp. 90-100.

Rahimi M, Riazi A. 2014. On local entropy of fuzzy partitions. Fuzzy Sets Syst. 34: 97-108.

Shaw Krishnendu, Shankar Ravi, Yadav Surendra S, Thakur Lakshman S. 2012. Supplier selection using fuzzy AHP and fuzzy multi-objective linear programming for developing low carbon supply chain. Expert Syst Appl. 39(9): 8182–8192.

Shen J, Tan H, Wang J, Wang J, Lee S. 2015. A novel routing protocol providing good transmission reliability in underwater sensor networks. J Internet Technol. 16(1): 171-178.

Velloso P, Laufer R, Cunha D, Duarte O, Pujolle G. 2010. Trust management in mobile ad hoc networks using a scalable maturity-based model. IEEE Trans Netw Serv Manag. 7(3): 172-185.

Wang Jian, Liu Y, Jiao Y. 2011. Building a trusted route in a mobile ad hoc network considering communication reliability and path length. J Netw Comput Appl. 34(4): 1138-1149.

Wu Gin-Der, Zhu Zhen-Wei. 2014. An enhanced discriminability recurrent fuzzy neural network for temporal classification problems. Fuzzy Sets Syst. 237: 47-62.

Xia H, Jia Z, Li X, Ju L, Sha E. 2013. Impact of trust model on on-demand multi-path routing in mobile ad hoc networks. Comput Commun. 36(9): 1078-1093.

Xia H, Jia Z, Li X, Ju L, Sha E. 2013. Trust prediction and trust-based source routing in mobile ad hoc networks. Ad Hoc Netw. 11(7): 2096-2114.

Xie YH, Hu JK, Xiang YH, Yu S, Tang SS, Wang Y. 2013. Modeling oscillation behavior of network traffic by nested hidden markov model with variable state-duration. IEEE Transn Parallel Distrib Syst. 24(9): 1807-1817.

Zhao HY, Yang X, Li XL. 2013. cTrust: trust management in cyclic mobile ad hoc networks. IEEE Trans Veh Technol. 62(6): 2792-2806.

Zhang LX, Lam J. 2010. Necessary and sufficient conditions for analysis and synthesis of Markov jump linear systems with incomplete transition descriptions. IEEE 9Trans Autom Control. 55(7): 1695-1701.