IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501
Vol.6, No 2, Mar-Apr 2016

Security Enhanced Dynamic Trust Based Routing Decisions for Mobile Adhoc Networks

Jayalakshmi V
Research and Development Center,
Bharathiar University,
Coimbatore, India

Dr. Abdul Razak T
Department of Computer Science,
Jamal Mohamed College,
Tiruchirappalli, India.

***Abstract*—Mobile ad hoc networks (MANETs) are defined as multi-hop wireless networks dynamically formed by mobile nodes, operating without any centralized infrastructure. MANETs are very susceptible to various attacks from malicious nodes because of the openness in the network. The mobile nodes in the network must be trust worthy and behave cooperatively for the better performance of the network. In order to enhance the security of network and protect the nodes from vulnerabilities, this paper proposes a trust-based framework for improving the security and robustness of ad-hoc network routing protocols. Trust value is calculated based on nodes packet forwarding behavior. This scheme allows source nodes to choose the shortest trusted path during route discovery in ad-hoc networks and isolates any malicious nodes from the network. We have integrated the proposed trust framework in to the popular and widely used Ad-hoc On-demand Distance Vector (AODV) routing by making minimal changes in the AODV protocol to enhance security and reliability. With the help of the simulations, we demonstrate the performance of our proposed protocol is better than AODV in terms of packet delivery ratio and average latency in the presence of attacks by the malicious nodes.**

Keywords- ***Attack; AODV; Trust; Malicious node; MANET***

I. INTRODUCTION

A Mobile Ad Hoc Network (MANET) is a collection of mobile nodes which are capable of communicating with each other without help from any centralized infrastructure. Classic Examples of these applications are deployments of moving people over a surface area (military deployments, rescue exercises, etc...) or wireless sensor networks. In these situations, the routing of packets between nodes which do not have any direct communication needs to be carried out with the co-operation of all the nodes which make up the network. The well-known protocols which are undergoing active research are AODV [1], DSR [2], and TORA [3].These protocols have been developed for networks where all nodes behave in cooperative and faithful manner in forwarding the packets. However, in real life, such an unselfish approach is hard to attain and so, these protocols are more often executed by malicious nodes which disturb the performance of the network [4, 5]. In order to maintain the unstructured nature of ad hoc networks without making any superfluous assumptions, a trust-based scheme is usually needed to protect these routing protocols. As nodes may not aware to which nodes it is connected with or which nodes connected to them. Therefore access to resources or information can be shared among both trusted and non-trusted nodes. The networks work well only if the mobile nodes are trust worthy and behave cooperatively [6]. Assigning a local trust level to a node pair can not only alleviate the negative effects caused by misbehaviors but also make communication occur only among trustworthy neighbors with respect to the fact that the exchange of information with compromised nodes which can weaken the performance of ad hoc networks. Therefore, incorporating a relationship of trust into MANET nodes is important [7]. The inherent freedom in self-organized mobile ad hoc networks introduces challenges for trust management. Some trust management models have been developed for wired networks but they are inapplicable to MANETs because of their dynamic topology and application scenario. In this paper, a dynamic trust based scheme is proposed for MANET with the objectives: (1) Describing a trust-based framework that provides metrics for evaluating route dependability, (2) Providing motivation and rewards for nodes to cooperate and behave responsibly in the network , and (3) Identifying and isolating any malicious nodes in the network.

In the On-demand Distance Vector Routing (AODV) [1], the selected shortest paths to the destination may not always be the best. Such paths may be congested, they may include malicious or selfish nodes, or they may be adversely affected by other network or physical conditions. The source node may not be aware of any such route conditions for forwarding packets. AODV route replies would only contain information about the number of hops, route freshness, sequence numbers, and the source and destination IDs. It does not have any in-built measures to detect the malicious nodes in the route. In this paper, a new trust management model is proposed which calculates the trust value of each node by their packet forwarding behavior. A node's creditability is evaluated on multiple factors such as weight of each packet, time taken to forward the packets. If a packet is transmitted within the stipulated time, a reward is given to the node to encourage the cooperation in the network. Our proposed framework evaluates trust on a continuous scale and takes into account both route trust and node trust. An application of the proposed trust management model, a novel reactive routing protocol called Trusted Reactive Routing (TRR) Protocol is proposed on the basis of the standard AODV protocol. The proposed protocol kicks out

the malicious nodes and establishes a reliable trusted routing path for packet transmission.

The rest of the paper is structured as follows. Section 2 presents the related work. In section 3, we present the trust calculation methods adopted in this paper and the description of the proposed TRR protocol, Section 4 presents the simulation results to evaluate the performance of the proposed scheme. Section 5 concludes the paper.

II. Related Work

The Watchdog and Pathrater mechanism [8] has been specifically designed to optimize the forwarding mechanism in the Dynamic Source Routing protocol. The mechanism basically consists of two components: Watchdog and Pathrater. The Watchdog is responsible for detecting selfish nodes that do not forward packets. The Pathrater assigns different rating to the nodes based upon the feedback that it receives from the Watchdog. One disadvantage of this protocol is that it merely avoids routing through malicious nodes, and it does not do anything to penalize them. This allows a lazy or selfish node not to forward traffic for its neighbors while its neighbors will continue to forward its traffic. Pirzada and McDonald develop a protocol based on DSR in [9], their protocol takes advantage of the full route information available in DSR [2]. Unlike other recommendations, however, they only consider trust from direct observations rather than including third party opinions. In their protocol, however, lazy nodes are not penalized and therefore have no incentive to participate. Trusted-DSR [10] extended from DSR selects a forward path based on a local evaluation of the trust values of all intermediate nodes along the path to the destination. 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, while every retransmission decreases the trusts. But, it is impossible for senders to know which nodes discard packets. Pirzada et al. [11] 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. In particular, trust-based AODV routing maintains a stable throughput and surpasses TORA and DSR at higher traffic loads. Manickam et al. proposed a Fuzzy based Ad hoc on demand Distance Vector (FAODV) Routing Protocol [12]. The authors used fuzzy logic for trust evaluation and setup a Threshold Trust Value (TTV) for trust verification. Fuzzy logic based trust evaluation gives a rational prediction of trust value and an accurate identification of malicious behavior based on fuzzy inference rules. However, the FAODV model only considers the protection method against modification attacks. Furthermore, the trust evaluation process only monitors the node's behavior for route discovery but not for the transmission of data packets.

As another extension to DSR, Guoet al. [13] gave a dynamic trust evaluation scheme based on routing model (Trust-DSR). Five route selection strategies have been proposed, which are based on the trust evaluation of the transmission links. Since its route selection is limited on the routes that obtained from standard DSR, the ultimate selected route is not necessarily the most trusted one

Xia et al. proposed Fuzzy Trusted Dynamic Source Routing FTDSR protocol [14].The subjective trust evaluation model proposed by the authors use the credibility of nodes can be evaluated by considering different trust decision factors and they used analytic hierarchy process theory and fuzzy logic rules prediction method to predict the nodes behavior. Xia et al. proposed Trust-based Source Routing protocol (TSR) [15].The authors uses only the forwarding ratios to recognize a monitored node's historical behaviors and they used fuzzy logic rules prediction method to calculate the evaluated node's current trust on the point view of the monitor. Jayalakshmi and Abdul Razak proposed Trust Vector Based DSR Protocol TV-DSR [16] trust value for each node is calculated by employing different factors namely Weight based Forwarding Ratio Factor, similarity Factor and Time Aging Factor based on the history of interaction between the nodes. For the trust inference, vector trust is used for aggregation of distributed trust scores.

In, most of the previous work only takes into account the measure of the forwarding mechanism by network nodes. The factors such as importance of the packets forwarded and the time a forwarding node takes to transmit packets are not considered.

III. Proposed Trusted Reactive Routing (TRR) Protocol

During Route discovery, the AODV protocol considers only hop count in order to find the shortest path. This condition needs to be changed for enhancing security in the decentralized infrastructure networks since the performance of the network is highly dependent on the collaboration among the participating nodes in the network. So we need to consider the trust level of a forwarding node during route selection for improving the performance. In most existing trust models, direct trust is based on the two neighbour entities historical interactions. In this paper, the trust value is calculated by summing the weighted packet forwarding ratio, reward factor and penalty factor.

A. Node Trust Value (NTV)

Our proposed model, calculates the trust value with multiple constraints: weight factor assigned to each packet transmitted, Reward Factor, Penalty Factor and time aging factor. Trust normally fades with time variation. A weight is assigned to each data being forwarded because some malicious nodes may forward data packets if they are of less importance and do not forward data packets of high importance. The Reward factor and penalty factor are used to distinguish the amount of time a node takes to forward the packets. Reward for the nodes is given based on their speed of forwarding capability to transmit packets within the stipulated time. The

purpose of including the reward and penalty factor is to encourage the nodes to transmit the packets quickly without any delay. The nodes which transmit the packets after the stipulated time will get penalty and the nodes may launch the modification attacks, gray-hole attacks and black hole attacks. Based on the above constrains the trust value for each node is calculated as follows

$$NTV_{(t)} = \frac{\sum_{j=1}^{n} \delta_j}{\sum_{i=1}^{m} \delta_i} + \sum_{k=1}^{b \le n} RF_k + \sum_{p=1}^{q \le n} PF_p \qquad (1)$$

$$NTV_{(t)} = \begin{cases} 1 & (NTV_{(t)} > 1) \\ NTV_{(t)} & (0 \le NTV_{(t)} \ge 1) \\ 0 & (NTV_{(t)} > 1) \end{cases} \qquad (2)$$

δ is the weightage factor for the data based on its importance as shown below in the table 1. *n* is the number of packets correctly forwarded and *m* is the total number of packets forwarded.

TABLE 1.WEIGHT OF PACKETS FORWARDED

S.No.	Importance	Value
1.	Important/Rare	>=0.8
2.	Control packets/ Medium	>=0.4 to <0.8
3.	Unwanted	<0.4

The RF and PF are the reward factor and penalty factor respectively. RF and PF should satisfy the following conditions: 1≥RF>PF≥0 and the sum of RF and PF should not exceed 1. (RF+PF =1).
The value of RF can be calculated in eq. (3)

$$RF = \begin{cases} \alpha \text{ x d x } 0.02 & (0 \ge pft \le 15ms) \\ \alpha \text{ x d x } 0.01 & (15ms \ge pft \le 30ms) \end{cases} \qquad (3)$$

Similarly the Pf can calculated be calculated in eq. (4)

$$PF = \begin{cases} \alpha \text{ x d x } (-0.01) & (30 \ge pft \le 45ms) \\ \alpha \text{ x d x } (-0.02) & (45ms \ge pft \le 60ms) \end{cases} \qquad (4)$$

Where pft is the time taken to forward a packet, d is the distance between the two neighboring nodes and the value of α can be determined experimentally based on the distance.

Trust value normally fades with time. The time interval Δt to update the trust value in our work is taken as 15 s.Δt, RF and PF values can also be determined according to the practical requirement.

B. Route Trust Value (RTV)

The concatenation propagation of trust does not increase trust, route trust should not be more than the trust values of intermediate nodes. So, at time t, the trust of a route denoted by RTV (t)) is equal to the continued product of node trust values in the route. The NTV value of each node along the route is multiplied to obtain the RTV value for the route using the following equation

$$RTV = \prod_{i=1}^{k} NTV_i \qquad (5)$$

Here, k is the number of nodes in the specific route, and by taking product we get values in range (0, 1).

C. Trust Info Table

To remember trust information, we introduce a table called trust info. Each node will maintain a trust information for every neighbour which has been sent packets to for forwarding.

Node ID
SWAF
SWCF
RF
PF
Packet Cache

Figure 2. Structure of Trust Info Table

It consists of a node ID, weighted sum of all the packets forwarded (SWAF), weighted sum of packets forwarded correctly (SWCF) and packet cache. Two counters one for summing the weights of all the packets and the other one for summing the weights of all the packets correctly forwarded. The Packet Cache is used to store all the packets sent and older packets are deleted in order to give room for the newly arrived packets. In this work, if there is no space in the cache, then the packet which is stored earlier will be removed.

Before sending a packet to a neighbour, the sender looks up the trust info table corresponding to the neighbour and adds the weight of all packets to SWAF. To add the weight of packet to the correctly forwarded packet field in the table first it checks whether the packet is successfully forwarded, the packet will not be deleted immediately after being sent. Then it will be stored in the packet cache and wait for acknowledgment. If the packet is forwarded correctly and its weight is added to the SWCF and it will be removed from the packet cache.

D. Trust Table

Each forwarding node maintains a trust table to store trust information about the neighboring nodes. The fields in

the trust table are neighbour node id, node trust value and Status which indicates whether node is malicious or trusted. For example the trust table maintained by the Node D in the figure 1 is given in Table 2.

TABLE 2. TRUST TABLE OF NODE D

Neighbor Node ID	NTV	Status
C	0.6	Trusted
G	0.7	Trusted
F	0.3	Malicious

E. Route Discovery

In the proposed protocol, whenever the source node needs to find a path to new destination, it checks the black list in the trust table. It broadcasts a route Request packet (RREQ) to the neighboring node only it is a trusted node and appends a new filed called NTV is appended in the RREQ packet to carry the trust information about the node. Each node on receiving the RREQ further forwards it to the trusted neighbors by checking their respective trust table until it reaches the destination. Nodes only reply back to RREQ packet if they are the destination. Each intermediate node on receiving the RREQ packet complements their NTV value inside RREQ's NTV field by multiplying with the value contained in the packet. The NTV value of all the nodes along the route is multiplied to obtain the route trust value RTV as given in eq. (5).

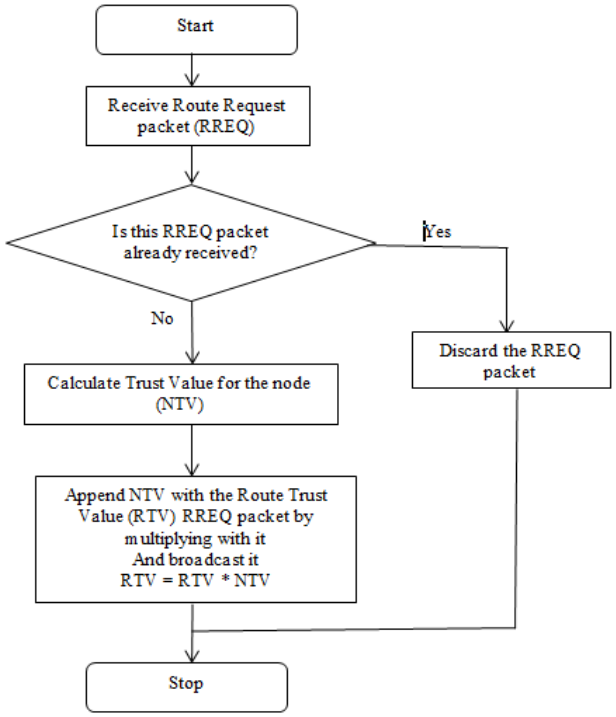

Figure 3. RREQ received by intermediate node

F. Route Reply by the Destination Node

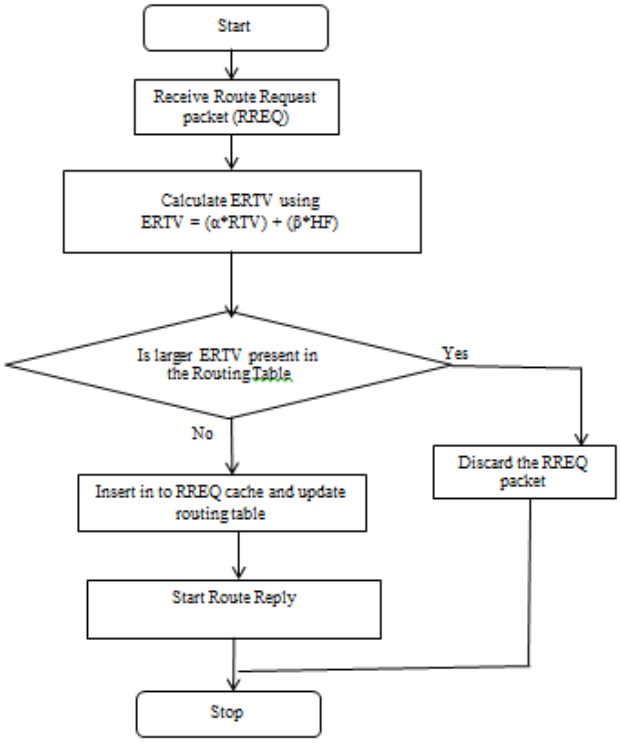

Figure 4. Route reply by the destination Node

In the proposed protocol, intermediate nodes are not allowed to reply back to RREQs even if they have route to destination, and they continue to propagate RREQ packet along the trusted route till it reaches the destination node. This is to ensure that the highest trusted route is selected by the destination node for sending a route reply. In the standard AODV, because of the shortest route finding behavior when a destination node receives the first RREQ sends a route reply and discards any further route requests. But in the proposed protocol, when a destination node receives a first RREQ, it waits for a small interval Δt and then replies back for a route with maximum ERTV value as shown in fig 4.The Entire route trust value ERTV from source to destination is evaluated to cater for the hop count in route selection is obtained by using the following eq.

$$ERTV = (\alpha \times RTV) + (\beta \times HF) \qquad (6)$$

where α and β are the weights for the route trust value and hop factor. The values of α and β are chosen in such a way that $\alpha + \beta = 1$, $0 < \alpha < 1$ and $0 < \beta < 1$.

The Hop Factor HF is calculated as follows

$$HF = \frac{Hop_{\max} - Hop_{Count}}{Hop_{\max}} \qquad (7)$$

where $Hop_{\max}$ is the present hop count and Hop_{Count} is the maximum hop count allowed by the protocol. Hop factor will have the value in range (0, 1) with direct links from source to destination having Hop factor as 1 and will keep on reducing with the rise in the number of intermediate nodes. A and β are weights that can be varied based on the importance of trusted route and hop count during route selection. Here, in our work, values of each one of them to 0.5.

IV. EXPERIMENTAL RESULTS

Our protocol in this paper is extended from AODV which is a standard and widely used routing protocol for wireless ad hoc network. To enhance the security of AODV, the trust management model is incorporated in to the protocol and a novel protocol called TRRP is proposed. While maintaining the advantage of original protocol, the new protocol is added with security features which mitigate any type of attacks from the malicious nodes. To evaluate the performance of AODV and TRRP we have conducted a comprehensive test using NS-2 network simulator [17].

A. Experimental Setup

Ns2 simulator is used to evaluate the performance of the newly proposed protocol under different scenarios. Within a rectangular field of 1000 m × 1000 m, 30 nodes are randomly dispersed and the transmission radius of every node in one hop is fixed at 250 m. The node mobility uses the random waypoint model [18] in which each packet starts its journey from a location to another at a randomly chosen speed. A maximum speed of 0 m/s implies that the MANET is a static network. The fixed simulation parameters in NS-2 are listed in Table 4.

TABLE 3. SIMULATION PARAMETERS

Parameter	**Value**
simulation time	200 s
number of nodes	30
map size	1000 m×1000 m
mobility model	random way point
traffic type	constant bit rate (CBR)/UDP
transmission radius	250 m
packet size	512 bytes
connection rate	4 pkts/s
pause time	2 S

B. Performance Metrics

We use 3 metrics to evaluate the performance of these routing protocols, in which the first two metrics are the most important for best effort route and transmit protocols.

1. Packet delivery ratio: the fraction 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, 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 (including route request/reply/update/error packets) to the number of data packets.

C. Scenario 1: Varying Node Speeds

In the first test, we compare the performance of the TRR with that of other two protocols as maximum speed of nodes varies from 0 m/s to 30 m/s. As shown in Figure 5(a), the delivery ratios of AODV declines as nodes speed while the delivery ratio of TRR fluctuates. The performance differences become more apparent at higher speed. This advancement of TRR can be attributed to the improved probability of node behavior detection due to the more interactions. Each data packet being forwarded by the intermediary nodes is supported by trusted route discovery, which elevates the probability of successful delivery to a trusted node. In contrast, nodes executing AODV only maintain limited routes to a destination and are unable to aid in packet delivery in case of the unavailability of a trusted next hop link leading to a destination.

Figure 5(b) and 5(c) illustrate that the average end-to-end latency and routing packet overhead for these protocols rise with the increase in speed. At higher speeds, the links are frequently disconnected and thus the nodes initiate additional route discoveries to sustain ongoing data connections. At the highest speed of 30 m/s, the average latency reaches their peaks, respectively. TRR has a lower average latency than AODV when the speed is greater than 5 m/s because it avoids malicious nodes more accurately, thus reducing the risk of adding delay for resenting the failed routing packets.

In Figure 5c, the routing packet overhead in these protocols rises with the increase of maximum speed. When the speed is smaller than 20 m/s, the overhead in TRR remains comparatively higher than that in AODV. The reasons for different period are: (i) More RREQ and RREP packets need to be sent for qualified routes to meet trust requirement in TRR and meanwhile, trust requirement is not considered in AODV; the additional route update and maintenance packets increase the amount of control packets and the routing packet overhead in TRR. Along with the speed increasing, there is an opposite impact. As the nodes move faster, the number of interactions between the nodes increases steadily. The trust is transferred to the entire network. For the low credibility of the nodes, in the route discovery process of the future, the network does not need to send route query packets to them again, and this reduces the routing overhead. But in AODV, along with the increase of maximum speed, the routing routes break down

easily, leading to send more route request and route maintenance packets.

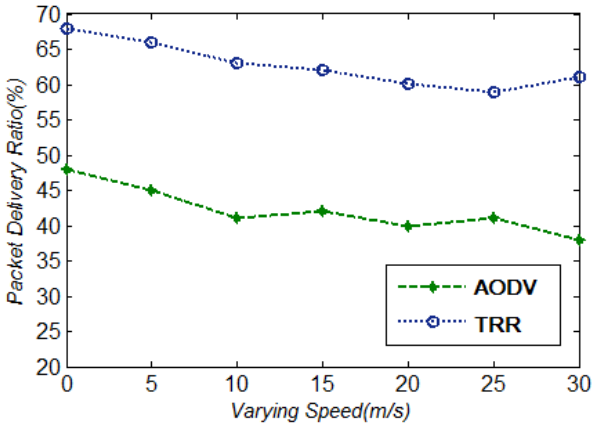

Figure 5a. Packet Delivery Ratio vs Varying Speed

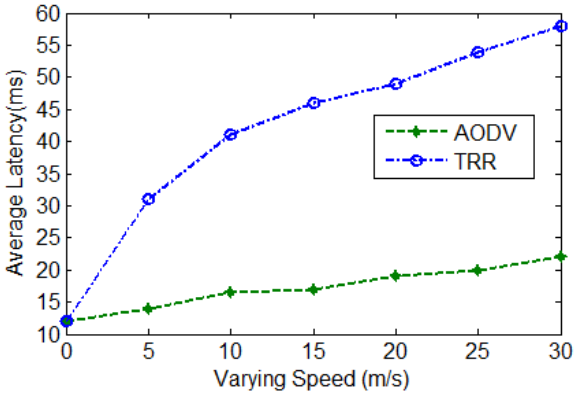

Figure 5b. Average Latency vs Varying Speed

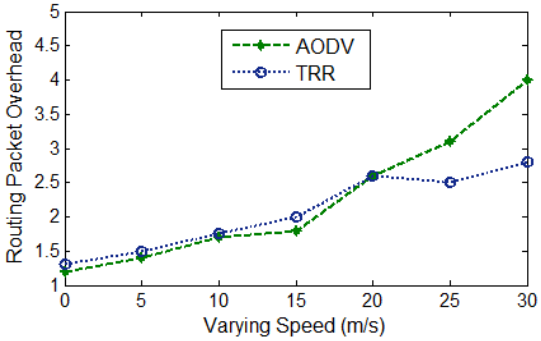

Figure 5c. Routing Packet Overhead vs Varying Speed

D. Scenario 2: Varying Number of Malicious Nodes

In scenario 2, we evaluate the effects on these protocols under varying number of malicious nodes. In the absence of malicious nodes, the typical packet loss is about 1 percent for AODV, TRR. As shown in Figure 6(a), the delivery ratio of all protocols degrades sharply as malicious nodes increase. The delivery ratio of AODV drops from 99% to 39% as the number of malicious nodes varies from 0 to 15. Lower packet delivery ratio means less network throughput.

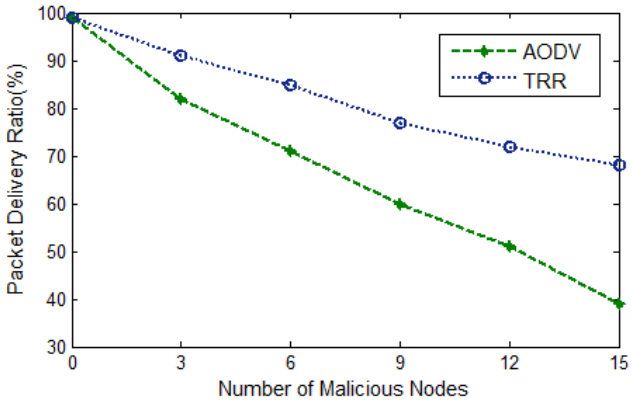

Figure 6a. Packet Delivery Ratio vs Number of Malicious Nodes

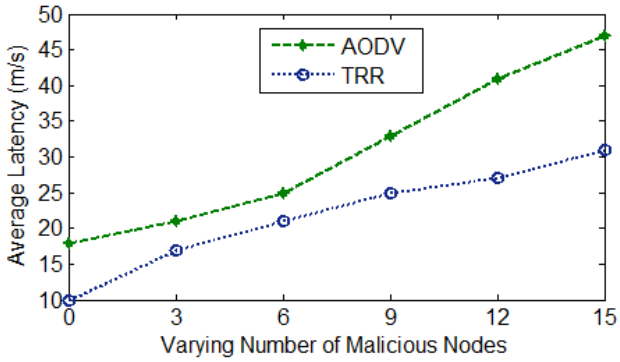

Figure 6b. Average Latency vs Varying Number of Malicious Nodes

As shown in Figure 6b, the average latency in TRR ascends slowly with the increase in number of malicious nodes, but the average latency in AODV arises sharply. This average latency is mainly caused by queuing delays and retransmission delays. But there is an apparent reduction in the average latency with TRR when compared to AODV. As a result, in the process of establishing a trusted routing route, the network will be possible to avoid the suspect and malicious nodes. This can contribute to effectively reduce the end-to-end latency.

When the number of malicious nodes increases to 15 (50% of the whole nodes), the routing packet overhead of is approximately 2.9 as shown in Figure 6c. The value is smaller than the routing packet overhead in AODV. When the number of malicious nodes is smaller than 5, the routing packet overhead in TRR is bigger than in AODV, the reason is that, the increased control packets in TRR is primarily due to its route discovery mechanism that broadcasts more RREQ and RREP packets to look for trustworthy routes to destinations. When the number of malicious nodes is bigger than 5, the routing packet overhead in TRR is smaller than AODV, because of the huge damage on routing path from malicious nodes.

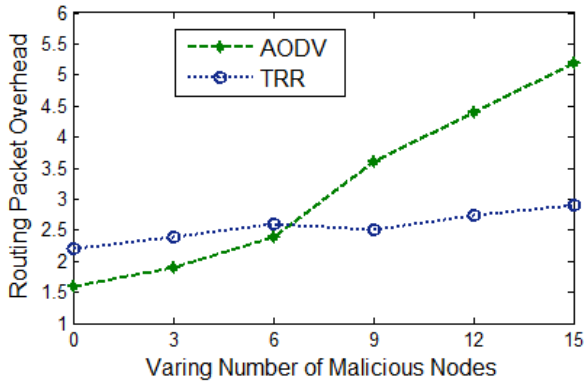

Figure 6c. Routing Packet Overhead vs Varying Number of Malicious Nodes

The experiment results in test 1 and 2 show that our trust model is effective and the TRR protocol performs better than AODV as it gives higher packet throughput (delivery ratio), lower end-to-end latency and less packet overhead.

V. CONCLUSION

In this paper, a new trust based reactive routing protocol is proposed. The node rust value is calculated based on the factors namely weighted forwarding ratio, Reward factor and penalty factor. The route trust for each route is calculated and the best trusted route is chosen from the out of several available routes which has a minimal hop count. This proposed strategy is integrated in to the AODV routing protocol by making minimal changes in the existing AODV protocol. The proposed Trust based Reactive Routing (TRR) protocol can eradicate the untrustworthy nodes to obtain t a reliable passage delivery route. Performance comparison of standard AODV and proposed TRR shows that TRR is able to achieve a significant improvement in the packet delivery ratio in the presence of malicious nodes. The proposed protocol is modular, scalable and flexible enough to be easily combined with other existing schemes for increased security.

For future work, ,in order to avoid node failures because of the energy depletion in a node, while making routing decision ,residual battery power of nodes will also be considered along with the calculated trust value . The proposed trust model will be incorporated into other protocols namely DSR, TORA and the multipath variant of AODV, AOMDV

REFERENCES

[1] C.E. Perkins, E.M. Royer, S.R. Das, "Ad-hoc on-demand distance vector routing', In Proceedings of International Workshop on Mobile Computing Systems and Applications (WMCSA), New Orleans, Louisiana, USA, pp. 90–100,1999

[2] Johnson, David B., and David A. Maltz. "Dynamic source routing in ad hoc wireless networks." In Mobile computing, pp. 153-181. Springer US, 1996.

[3] Park, Vincent, and M. Scott Corson. Temporally-ordered routing algorithm (TORA) version 1 functional specification. Internet-Draft, draft-ietf-manet-tora-spec-00. txt, 1997.

[4] Lundberg, Janne. "Routing security in ad hoc networks." Helsinki University of Technology, http://citeseer. nj. nec. com/400961. html (2000).

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

[6] T. Hughes, J. Denny, P.A. Muckelbauer, J. Etzl, "Dynamic trust applied to ad hoc network resources", in: Proceedings of the Autonomous Agents and Multi-Agent Systems Conference, pp. 273–280,2003

[7] N. Griffiths, A. Jhumka, A. Dawson, R. Myers, "A simple trust model for on-demand routing in mobile ad-hoc networks", In proceedings of International Symposium on Intelligent Distributed Computing (IDC 2008), pp. 105–114, 2008.

[8] Marti, Sergio, Thomas J. Giuli, Kevin Lai, and Mary Baker. "Mitigating routing misbehavior in mobile ad hoc networks." In Proceedings of the 6th annual international conference on Mobile computing and networking, pp. 255-265. ACM, 2000.

[9] K. Meka, M. Virendra, S. Upadhyaya, "Trust based routing decisions in mobile ad-hoc networks", In proceedings of the Workshop on Secure Knowledge Management (SKM 2006), 2006

[10] C.D. Jensen, P.O. Connell, "Trust-based route selection in dynamic source routing",In proceedings of International Conference on Trust Management pp150–163,2006.

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

[12] Manickam, J., and S. Shanmugavel. "Fuzzy based trusted ad hoc on-demand distance vector routing protocol for MANET." In Advanced Computing and Communications, ADCOM 2007. International Conference on, pp. 414-421. IEEE, 2007.

[13] Wei, Guo, Xiong Zhongwei, and Li Zhitang. "Dynamic trust evaluation based routing model for ad hoc networks." In Wireless Communications, Networking and Mobile Computing, 2005. Proceedings. 2005 International Conference on, vol. 2, pp. 727-730. IEEE, 2005.

[14] Xia, Hui, Zhiping Jia, Lei Ju, and Youqin Zhu. "Trust management model for mobile ad hoc network based on analytic hierarchy process and fuzzy theory." IET wireless sensor systems 1, no. 4,pp 248-266,2011.

[15] Xia, Hui, Zhiping Jia, Xin Li, Lei Ju, and Edwin H-M. Sha. "Trust prediction and trust-based source routing in mobile ad hoc networks." Ad Hoc Networks 11, no. 7,pp 2096-2114,2013.

[16] Jayalakshmi V, Abdul Razak T, "TV-DSR : Trust Vector Based DSR Protocol For Secure Routing In Mobile Adhoc Networks" , International Journal of Applied Engineering Research 10,no 9 (2015) pp. 23797-23814

[17] http://www.isi.edu/nsnam/ns/

[18] Bettstetter, C., Resta, G., Santi, P.: 'The node distribution of the random waypoint mobility model for wirelessad hocnetworks',IEEE Trans.Mobile Comput., 2, no 3, pp. 257–269,2003