DOI: http://dx.doi.org/10.26483/ijarcs.v12i3.6740

Volume 12, No. 3, May-June 2021

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

EFFICIENT TRUST BASED SCHEMES FOR QUALITY OF SERVICE IN MANET

K. Divya
Ph.D Research Scholar
Department of Computer Science
Gobi Arts & Science College
Gobichettipalayam, India

Abstract: Security is another crucial aspect of providing QoS since the existence of malicious nodes present all kinds of threats to MANETs. Although a number of mechanisms have been proposed for protecting MANETs, most of the solutions are only effective for a particular kind of attacks or provide security at the cost of sacrificing QoS. In this paper, we propose a trust-based secure QoS routing scheme by combining social and QoS trust. The primary approach of the proposed scheme relies on mitigating nodes that exhibit various packet forwarding misbehavior and on discovering the path that ensures reliable communication through the trust mechanism. The scheme would select the best forwarding node based on packet forwarding behavior as well as capability in terms of QoS parameters, such as residual energy, channel quality, link quality, etc. Simulation experiment using Network Simulator-2 (NS2) and under various network conditions show that mixing social and QoS trust parameters can greatly improve security and quality of service routing in terms of overhead, packet delivery ratio and energy consumption.

Keywords: mobile ad hoc networks; QoS routing; packet-forwarding; misbehavior; trust-based scheme

I. INTRODUCTION

MANET is a self-organizing, dynamic, infrastructure-less network consisting of a set of wireless nodes that communicate with one another over one or more connections or hops without the need of a central authority. In a MANET, each and every node can function both as a terminal node and as a router, meaning that each node could generate its own traffic while receiving data packets from other nodes and forwarding them to the neighboring nodes. MANETs can be deployed quickly and easily, making them very suitable for applications such as environmental monitoring, military surveillance, disaster rescue, etc. A major challenge for MANETs is the design of a secure and efficient routing protocol that can also ensure the overall quality of service during the routing process as MANET nodes communicate with each other only when they are located within the communication range of each other.

Another important issue in MANETs is security since malicious nodes can deliberately misbehave so that packet contents can be altered and packet routing to the desired destinations can be disrupted, lowering packet delivery ratio as well as reliability.

In trust-based security, when trust level increases, so do the access privilege for security protection. In MANETs, trust can be defined based on "the closeness of the relationships between entities that participate in a protocol interaction". There are generally two types of trust: social trust and QoS trust with social trust being obtained based on social relationships, e.g., friendship, honesty, privacy and intimacy while QoS trust being obtained based on competency, reliability, experience, number of packets forwarded, etc. There have already been some proposals for securing the process of routing in MANETs. The notion of trust is very useful in a highly dynamic environment where nodes need to depend upon each other to accomplish their common goals. Trust-based routing has been considered as an effective measure to deal with security threats caused by malicious nodes through detecting and isolating un trusted nodes in MANETs.

The proposed scheme would select a forwarding node by considering channel quality, link quality and residual energy in order to establish an optimal path in a very dynamic environment and detect intrusions by using the trust of neighboring nodes to mitigate threats by nodes misbehave in packet forwarding during the routing process. The proposed solution relies on the trust mechanism to provide reliable performance and secure links for data transmission and energy efficiency.

II. RELATED WORK

An objective trust management framework is used in this approach for solving problems such as handling high node mobility, energy drain, and limited processing capabilities of network devices by establishing a network of nodes with an acceptable level of trust relationships among themselves. The weighted trust is computed for each node, by the proposed algorithm considering the packet delivery ratio, energy consumption rate and buffer length into account. In this solution, intermediate nodes' opinion trust is computed and based on such an opinion trust value, the decision can be made regarding the use of a particular route for communication. Communication in MANETs has to be carried out through using intermediate nodes due to limited radio range. As a result, malicious nodes can join the network and harm the routing process. Thus, trust evaluation can yield two values at the minimum: negative and positive,

in the process of finding Future Internet a trustworthy node. After deriving the trust values for all the nodes along a path, route discovery can be performed by taking the opinion of the neighboring nodes.

The proposed model is multilayered and composed of a set of modules, i.e., packet receiver, packet forwarder, QoS routing module (RM), system security module (SSM) and data security module (DSM). All the modules are needed in order to identify QoS parameters and to detect selfish and malicious nodes. Efficient and reliable communication is ensured by selecting an appropriate router between a source and a destination through trusted nodes in the place of eliminated nodes. Performance evaluation was done in an established secure environment to show the improvement over AODV for different QoS parameters for both single and multi-path environments.

The proposed method used an algorithm based on Dynamic Adaptive Fuzzy Petri Net (DAFPN) with concurrent reasoning. DAFPN is an expert system to represent, capture and store fuzzy knowledge with the help of parameters such as threshold value, certainty factor and weight. The concurrent reasoning algorithm (CRA) is a matrix operation based algorithm, which can automate the procedure of DAFPN in which a MANET topology was modeled as a DAFPN to which FPN rules were applied.

The idea behind this approach is to assign a trust value to each node dynamically. Due to high mobility, there should be an integration of trust and energy consumption of every node. A new trust management model was thus proposed to enhance the routing security in the network in which both direct and indirect trust values were employed in trust calculation. Final trust value is derived based on direct trust value and indirect trust value. The Bayesian probability was also used as a technique for trust management to refine the calculation of trust.

Considering these notes, we combine both the types of trust components in our work. We believe that the success rate of any security scheme largely depends upon the mode of operations of the adversaries, but it is to be noted that most of these schemes do not precisely describe the mode of operation for adversary models during route discovery phase and data transmission phase, to identify patterns followed by malicious nodes, while selecting trusted route for data transmission. We address this issue by introducing an efficient trust-based scheme which integrates attack pattern discovery to the trust mechanism by observing the packet forwarding behavior of nodes continuously.

III. THE ADVERSARY MODEL

In this adversary model a type of gray-hole attack described as Attack1 in, a malicious node continuously monitors the field value of received as well as overheard control packets, in order to keep track of the highest recorded value of the destination sequence number. During the routing process, the malicious node replies to a Route Request (RREQ) with the lowest hop count and the highest possible value of the destination sequence number. Even though the malicious node does not have a valid path, a genuine source node employing AODV protocol immediately can build a route through the adversary.

A. The QoS Parameters

The proposed routing scheme would select the next node for packet forwarding to the destination node based on the following three parameters: channel quality, link quality, and residual energy.

B. Channel Quality

In our scheme, channel quality means the availability of the channel during transmission. Measurement of interference in a channel can help utilize resources more effectively to ensure reliable communication. The use of channel quality metric also helps to reduce end-to-end delay through the allocation of on-the-fly radio resources.

Procedure 1: Actions by the malicious node after receiving RREQ from the source node

If (RREQ is not for me) **then**
Discard the received RREQ
//A random value between 1 to 10 add to RREQ DestSeqno
RREP packet Fill up with DestSeqno= RREQ DestSeqno + Random Number (1:10) and hop Count=1
Unicast the forged RREP on the reverse path to the source
Else
Fill up the RREP packet with own Seqno and Hop count=1
Discard the received RREQ
Unicast the genuine RREP on the reverse path to the source
END If

Procedure 2: Actions by the malicious node after receiving data packets from the source node

If (data packet is not for me) **then**
If (Current Time > time1&& Current Time <= time2) then//time2-time1=50% time period
The packets received from the source will be drop
Else
If a valid route is available the data packets will be forwarded
END If
Else
Receive the data packet for me
End If

Figure 1 Adversary model Route Request (RREQ); Route Reply (RREP)

C. Link Quality

In this paper, a new metric, i.e., link quality, is introduced which is measured as the length of time of the existence of a link between two nodes (link residual life). In our proposed scheme, we use the measurement value of the link quality to help reduce the route failure in a highly dynamic environment. Although the accurate depiction of wireless links in MANETs is a tedious task, link residual life can be relatively easily estimated based on the range of communication and a relative velocity between nodes. The time during which a link exists between nodes can be estimated as follows. First, we need to find the distance between nodes and its relative velocity. Consider a link between nodes A and B, let D be the distance between the two nodes. If (x1, y1) and (x2, y2) are the coordinates of nodes A and B, respectively, the distance can be calculated by using the following formula:

$$D = q\ ((x2 - x1)\ 2 + (y2 - y1))$$

D. Trust Based Secure and QoS Routing Scheme

A trust model is employed in TSQRS to improve the cooperative routing and the performance of MANETs through evaluating the trustworthiness of the nodes in the networks. In the trust model, a node promiscuously listens to its neighboring nodes to evaluate the trust of these values. Due to the broadcast nature of MANETs, a node can observe and estimate the resources of a neighboring node through their direct interactions in a passive mode. When direct observation is involved, a complete history of trustworthiness can be provided by a node. Such a history would include information about communication quality of the node. In TSQRS, we include in our scheme the direct observations to derive trust values on neighboring nodes through using the social and the QoS trust parameters. In addition, trust is assessed on a continuous basis with a fixed time interval and trust value is calculated according to the quality of the behavior in packet forwarding by a node.

Following are the mechanisms that are used in our scheme for trust management

- Trust recommendation using HELLO messages.
- Trust update.
- Trust based secure QoS routing strategy

a) Trust Recommendation Using HELLO Messages

Figure 2 is the flowchart for the exchange of HELLO messages which are mostly used in the ad-hoc on demand distance vector routing protocol (AODV) to determine link connectivity. If each and every node keeps information about its neighboring nodes, it would help any node to make a better decision on routing. Since our routing scheme also uses HELLO messages to exchange QoS trust recommendations and to discover neighbors, we modify the HELLO packets to include some extra fields i.e., Residual Energy, Link Quality and Channel Quality as these parameters are the major reasons for unintentional node failure in mobile Ad hoc network affecting the QoS provided by MANET. Thus, QoS trust values are propagated through the HELLO packets. Each and every node periodically sends HELLO packets which incorporate the QoS parameters, allowing each node to obtain information about QoS trust values of its neighbors.

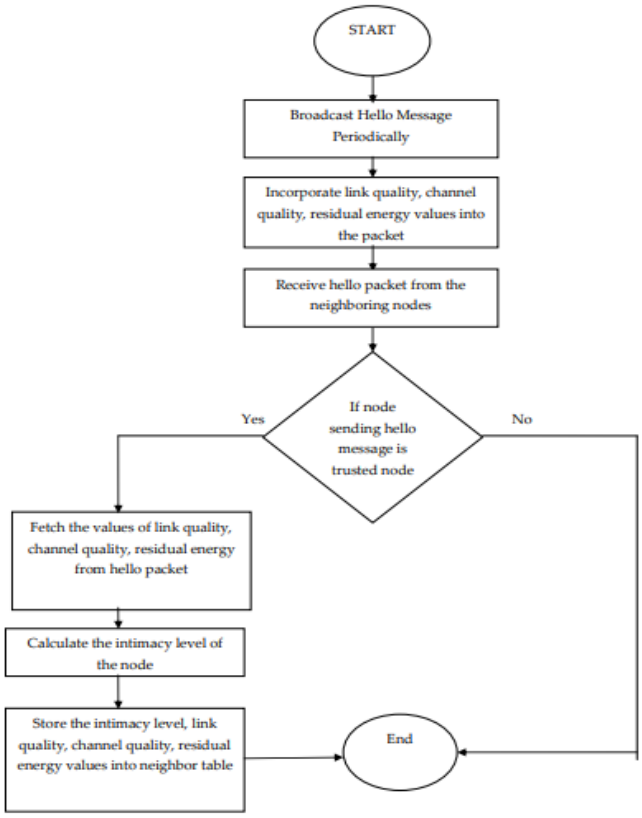

Figure 2 Trust recommendation using HELLO message exchange

b) Trust Update

This includes cases such as breakage of links to a node, causing disconnection from the current group, voluntary disconnection (for saving power) or involuntary disconnection (due to physical terrain or low energy). We also assume the malicious behavior of individual nodes in resource-constrained MANETs. In a routing process, neighbor node's trust is evaluated by the sender by observing activities carried out by that neighbor and forwarding behaviors of neighbors. To be specific, a source node will observe the trust of its neighbor node based on its data forwarding behaviors and QoS parameters. In our proposed trust-based model, we calculate historical trust consistently after a particular time interim called trust update so that we can identify all the nodes that behave maliciously and then update secure routes towards destinations by Figure 2. Trust recommendation using HELLO message exchange.

Our trust-based model takes the mobility of the network into account. Without further updates or continuous interactions between nodes, trust values would decay over time. Node mobility may also cause continuous interactions between a node and other group members, lowering the chance of nodes' evaluating each other in the same group. This includes cases such as breakage of links to a node, causing disconnection from the current group, voluntary disconnection (for saving power) or involuntary disconnection (due to physical terrain or low energy). We also assume the malicious behavior of individual nodes in resource-constrained MANETs. In a routing process, neighbor node's trust is evaluated by the sender by observing activities carried out by that neighbor and forwarding behaviors of neighbors.

$$Neighbor_{Trust} = w1 \times CFR + w2 \times DFR + w3 \times Intimacy_{level} + w4 \times Residual_{Energy} + w5 \times Link_{Quality} + w6 \times Channel_{Quality}$$

CFR is the ratio of number of control packets forwarded correctly by a node against total number of control packets supposed to be forwarded, and DFR is the ratio of total number of data packets forwarded correctly by a node against total number of data packets supposed to be forwarded. w1, w2, w3, w4, w5, w6 are the weights where $0 \leq w1, w2, w3, w4, w5, w6 \leq 1$ and $w1 + w2 + w3 + w4 + w5 + w6 = 1$. The values for the weights are purely decided by the empirical way. At the same time, they are decided by MANET application and QoS parameters that a user would give higher priority. Meanwhile, according to the behavior of neighbor nodes, trust value varies over the time. We use trust threshold η for the nodes to differentiate malicious nodes from benign ones. During the whole trust update process shown in Figure 3, nodes having poor quality and false behavior are marked as malicious and the routing table is updated with the most recent routing information continuously in order to build optimal and secure paths.

c) Trust Based Secure and QoS Routing Strategy

All the nodes including the source, the intermediates, and the destination are cooperating during the route discovery process. The process of sending data towards the destination is as follows

Before data transmission begins, the source node finds the entry of the destination node in its routing table. If such an entry exists, the data is sent to the destination through a trusted hop. Otherwise, the source node starts a route discovery process by flooding route request (RREQ) packets into the network to discover a route to the destination node. After the destination node is found, the route reply (RREP) is sent back to the sender node through trusted hops. If more than one RREP are delivered to the source node than the route with the highest destination sequence number is chosen and a trusted route is created for the destination node and saved in the routing table for routing.

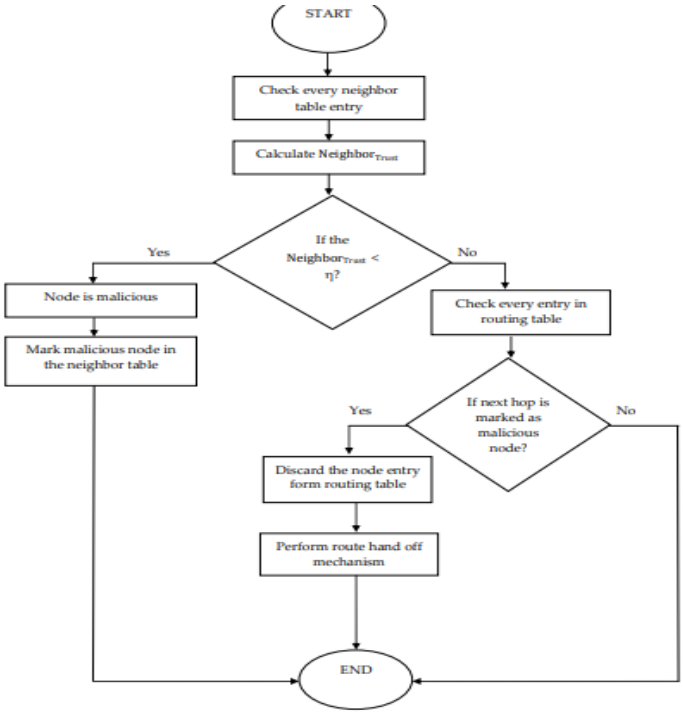

Figure 3 Trust Update

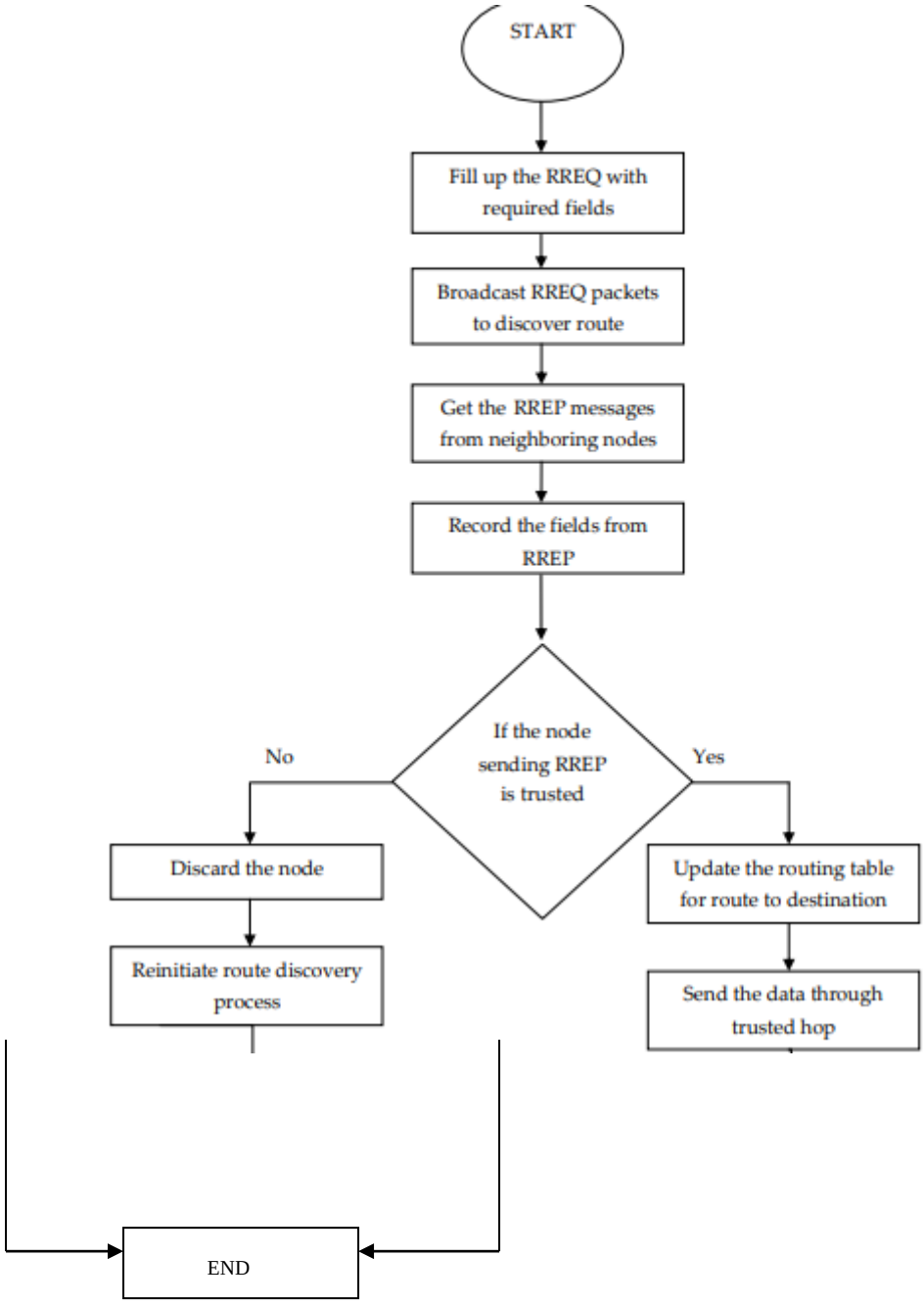

Figure 4 Trust based secure Quality of Service (QoS) routing strategy

IV. SIMULATION AND RESULT ANALYSIS

By varying the mobility of nodes and by varying the number of malicious nodes, we use packet drop ratio (PDR), routing overhead (RO), energy consumption (EC) to assess the performance of our proposed scheme. To show that TSQRS can achieve better routing decisions, the performance of TSQRS is compared to ETRS-PD and AODV with the adversary model. The begin nodes were distributed randomly throughout the network which employs the AODV, ETRS-PD and TSQRS protocols. Randomly positioned nodes perform various packet forwarding misbehaviors according to the adversary model.

Table I Simulation parameters, Constant Bit Rate (CBR), User Datagram Protocol (UDP)

Parameter	Value
Simulator	NS 2.34
Routing Protocol	AODV, Adversary Model, TSQRS
Scenario Size	1000 × 1000 m^2
Number of Nodes	50
Misbehaving Nodes	0–40%
Simulation Time	240 s
Traffic Type	CBR/UDP
Number of connections	15
Pause Time	5 s
Mobility	4–20 m/s

A. Evaluation Considering Node Mobility

PDR of AODV decreases from around 50 to 37% while that of ETRS-PD decreases from around 71 to 52%. As the speed gets higher, there is an expanded number of

link failures, causing packet loss. TSQRS shows improvement in PDR from 85 to 75% compared to AODV and ETRS-PD. As mobility level increases, there are an increasing number of link breakages, resulting in more path failure and unusual packet loss.

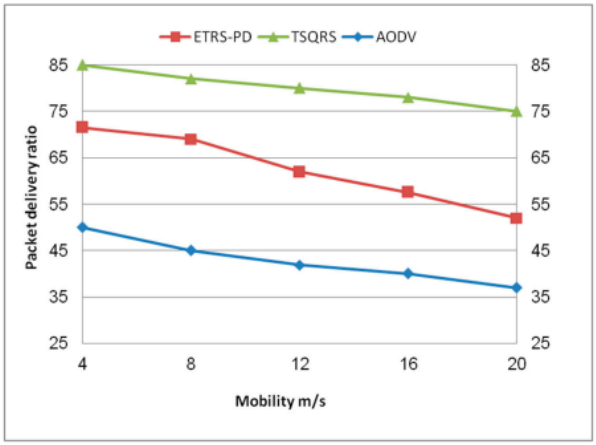

Figure 5 Packet delivery ratio (PDR) against mobility

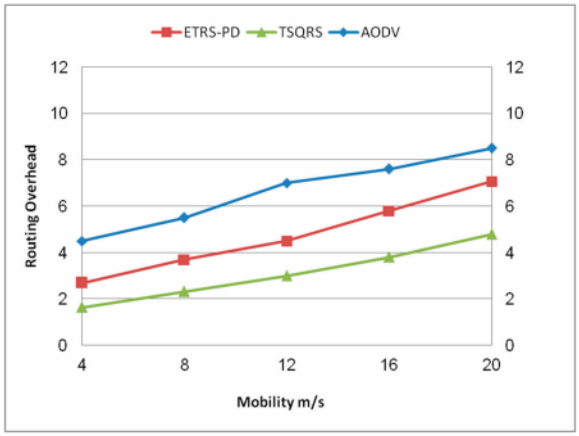

Figure 6 Routing overhead (RO) against mobility

B. Evaluation Considering the Percentage of Malicious Nodes

In this experiment, the three protocols were evaluated against the same adversary model and by varying the percentage of malicious nodes between 0 and 40% with other parameters being kept fixed. Especially, the mobility parameter is constant at 20 m/s.

C. Packet delivery ratio (PDR)

As shown in Figure 7, as the percentage of malicious nodes increases, there is an expansion in the number of packet drops in which PDR of AODV decays to about 30% under the adversary model while ETRS-PD provides some improvement to nearly 51.67%. TSQRS shows an improvement in PDR compared to AODV and ETRS-PD to achieve 60%. Trust mechanism that is used in TSQRS to judge the false behavior of neighboring nodes helps to eliminate the malicious nodes during routing, which in turn reduces the number of dropped packets.

D. Routing overhead (RO)

The RO of AODV fluctuates in the range 4.8 to 9.9 under the adversary model as shown in Figure 9. ETRS-PD again enhances RO to the range of 4.8 to 6.5 when contrasted to AODV. TSQRS achieves further improvement in RO. It is clear that the more the number of malicious nodes, the more easily they can cause damage. Since TSQRS selects only those nodes that are secure and have good link quality, there is a lower number of route failures, causing less number of control packets to be re-forwarded for route establishment.

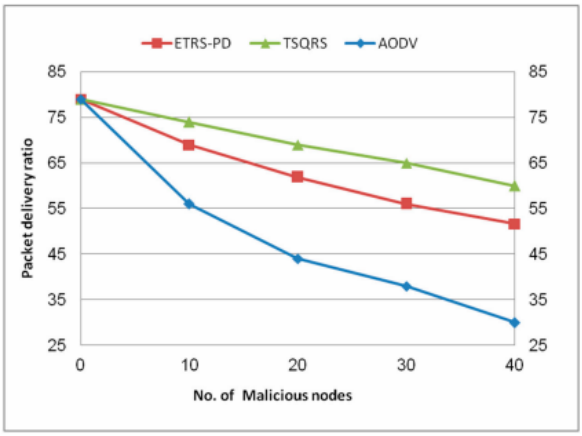

Figure 7 PDR against percentage of malicious nodes

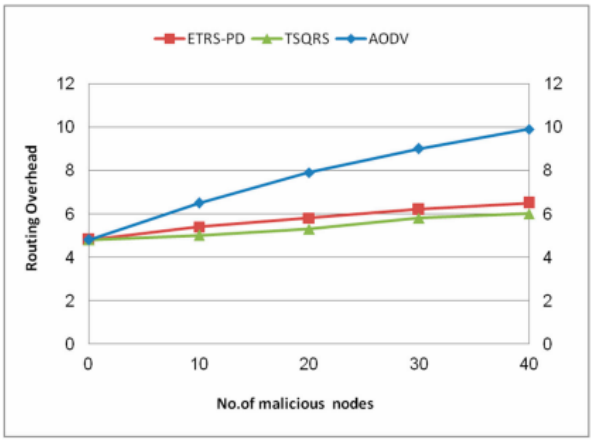

Figure 8 RO against percentage of malicious nodes

E. Energy consumption (EC)

Under the adversary model, EC in ETRS-PD varies between 311.96 to 313.5 J while TSQRS provides an improvement to achieve 310.36 to 309 J, a difference of 1.6 and 4.5 J, respectively. Thus, TSQRS is more energy efficient compared to ETRS-PD in different percentages of malicious nodes due to fewer route failures.

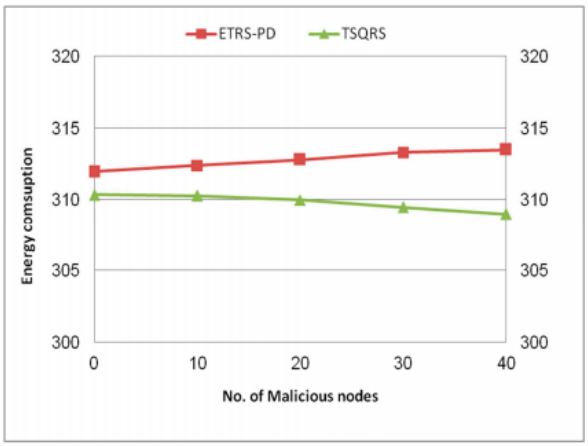

Figure 9 EC against percentage of malicious nodes

V. CONCLUSIONS

As a part of the literature survey, we observed that integration of QoS trust and social trust could improve the performance of routing in MANETs as both quality and security are very important aspects of such networks. To facilitate reliable communication in the highly dynamic environment of MANETs, TSQRS considers three important parameters during the discovery of on-demand routes, i.e., channel quality, link residual life and residual energy, to reduce route failures and to increase the overall system performance. Performance comparison of TSQRS to ETRS-PD and AODV under the same adversary model shows that TSQRS can improve consistently packet delivery ratio, routing overhead and energy consumption due to the enhancement to the routing process and due to the inclusion of new trust components for improving and securing the routing process. Adaptation of intelligent prediction functions such as software agents for evaluating nodes capability and reliability are suitable where the environment is unreliable, unpredictable and much dynamic. Intelligent Agents can be deployed at each sensor node to accurately predict the resource availability and reliability in order to perform organized allocation of the resource before the data routing.

VI. REFERENCES

[1] Jhaveri, R.H Patel, N.M.; Jinwala, D.C, "A Composite Trust Model for Secure Routing in Mobile Ad-Hoc Networks," In Ad Hoc Netw,Ortiz, J.H, de la Cruz, A.P Eds, In Tech, London, UK, 2017, ISBN 978-953-51-3109-0.

[2] Sethuraman, P, Kannan N, "Refined trust energy-ad hoc on demand distance vector (ReTE-AODV) routing algorithm for secured routing in MANET," Wirel Netw, 2017, 23, 2227–2237.

[3] Cho, J.-H, Chen, I.-R, Kevin, S.J, "Trust threshold based public key management in mobile ad hoc networks. Ad Hoc Netw," 2016, 44, 58–75.

[4] Gite, P, Kanellopoulos, D, Choukse, D, "An extended AODV routing protocol for secure MANETs based on node trust values," Int. Journal Int Tech Secur Tran.

[5] Hinge R, Dubey J, "Opinion based trusted AODV routing protocol for MANET," In Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies (ICTCS), Udaipur, India, 4–5 March 2016, ACM New York, NY, USA, 2016.

[6] Sumathi, K., Priyadharshini A, "Energy Optimization in MANETs Using On-demand Routing Protocol," Procedia Comput Sci 2015, 47, 460–470.

[7] Mylsamy R,Sankaranarayanan S, "A Preference-Based Protocol for Trust and Head Selection for Cluster-Based MANET," Wirel Pers Commun 2016, 86, 1611–1627.

[8] Sirisala N, Bindu C.S, "A Novel QoS Trust Computation in MANETs Using Fuzzy Petri Nets," Int Journal Intell Eng Syst, 2016, 10, 116–125.

[9] Khamayseh Y.M, Aljawarneh S.A., Asaad A.E, "Ensuring survivability against Black Hole Attacks in MANETS for preserving energy efficiency," Sustain Comput Inform Syst 2017.

[10] Venkanna U, Agarwal J.K., Velusam, R.L, "Cooperative Routing for MANET Based on Distributed Trust and Energy Management," Wirel Pers Commun 2015, 81, 961–979.