International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2022/215913 Volume 9, Issue 5, September – October (2022)

RESEARCH ARTICLE

A Trust-Based Design for Secure and Quality of Service Routing in Mobile Ad Hoc Networks

G. Sripriya
Department of Computer Science, Dr. G. R. D. College of Science, Coimbatore, Tamil Nadu, India.
kshresearch478@gmail.com

T. Santha
Dr.G.R.D. College of Science, Coimbatore, Tamil Nadu, India.
smresearch8@gmail.com

Received: 23 June 2022 / Revised: 29 July 2022 / Accepted: 28 August 2022 / Published: 30 October 2022

Abstract – The Mobile Ad Hoc Network (MANET), with its high dynamics, vulnerable links, and total decentralization, poses significant security issues. The MAODV (Multicast Ad-hoc On-Demand Distance Vector) protocol, a crucial routing protocol used in ad-hoc networks, falls short of security standards and is susceptible to assaults brought on by the hostile environment. The harmful nodal points can readily damage Mobile Ad-Hoc Networks (MANETs), which are made up of numerous wireless networks. The hardest task will be sharing bandwidth between wireless nodes while maintaining Quality of Service (QoS) for routing. To identify the potentially harmful nodes, trust-based routing strategies must be developed. The proposed effort entails constructing trust-based QoS routing with a secure mix of social and QoS trust. The suggested design's first method begins with the eradication of dead nodes, which leads to a packet collecting error. These dead nodes may also cause difficulty in the route analysis when employing trust mechanisms for communication. The suggested approach will perform better in terms of forwarding node selection based on packet behavioral characteristics. The forward node will be chosen depending on several parameters, including the residual energy between nodal locations, channel quality between nodes, and connection quality. The proposed method is simulated using the Network Simulator tool (NS2), and the simulation results show that the proposed approach is accurate and efficient in identifying and detaching problematic nodes at regular intervals.

Index Terms – Mobile Ad-Hoc Networks (MANETs), Trust-Based QoS Routing, Forward Node Selection, Network Simulator Tool (NS2).

1. INTRODUCTION

MANETs which is one of the types of the ad-hoc network consist of wireless communication from one node to another. The communication that takes place between the nodes is due to the exchange of data without any remembrance of pre-existing infrastructure. In recent years, the growth of devices connected to the network is evident, including IoT, which are increasingly common and necessary in our daily lives. Many of these fulfill a certain function according to the field for which they were developed, some have cameras and small microphones that help capture multimedia content from a physical environment. The different coding techniques have been improving more and more in order to design and build efficient routing that have good energy efficiency [1].

Various MANET work has reviewed that it has user-friendly environmental conditions and is free from the issues like channel access in wireless networks, multi-hop routing procedures, power factors, and networking problems. But the major issues of the MANET network are that they are affected by harmful nodal point which could bring network failure. Therefore, secured network formation becomes the major factor to preserve the network from attacking of harmful nodes.

The main objective of the proposed is to design a trust-based Quality of Service (QoS) routing technique. Routing for Quality of Service (QoS) is a critical component of MANET. The QoS routing approach, which is based on bandwidth or latency characteristics, may be used to find the path from the source to the destination. The routing protocol's security and efficacy are the most important factors to consider while creating a MANET. These characteristics may improve Quality of Service (QoS) accuracy throughout the routing process, which is mostly communication between nodes.

MANET disadvantages majorly depend upon the harmful nodes which can suddenly corrupt the network accuracy from one of the following defects. The defects may be termed as packet delaying or missing data, buffer overflow, battery drain-off, bandwidth factors, link breakage between the nodes, and loss of information.

Due to these factors, there is a major need for developing the trust-based QoS secured protocol in wireless networks. One of the formal approaches for the trust determination in Ad-hoc networks includes the Marsh formalism [2], which gives the

RESEARCH ARTICLE

analytical study that the interaction between the nodes results in the formation of a trusted structure between the nodes.

A node test with another node fulfills the responsibilities of each node after the communication process during the interaction. If the trust between the nodes is fulfilled, the communication increases else it will decrease gradually. Based on the formalism, Algorithm based on the trust and secured mechanism has been developed. The proposed work comprised of a literature survey, and the proposed work of Trust-Based secure QoS Routing Algorithm. The major contributions of the work is to design a trust based secure routing protocol for reliable communication using social and QoS trust score.

To improve cooperative routing and the efficiency of MANETs, the proposed protocol employs a trust model to assess network node reliability. A node in the trust model routinely solicits feedback from its neighbours in order to ascertain their level of trust in these values. Because MANETs are broadcast networks, a node can see and track the resources of a neighbouring node via direct interactions. When direct observation is used, a node can provide a detailed history of dependability. A history of this type would reveal information about the node's communication capability. The proposed methodology combines direct observations with the social and QoS trust features to generate trust values on nearby nodes. Furthermore, trust is evaluated on a regular basis over a set period of time, and trust value is determined by how efficiently a node forwards packets. The process is repeated until the target node is located and an optimal and secure path between the source and the destination is established. The information from the trust feedback is used to select the intermediary nodes or the forwarding path.

The paper's remainder section is structured as follows. A basic introduction to trust-based key management in MANETs is covered in Section 1. For ease of comprehension, Section 2 gives a discussion and table of the numerous literatures and contributions made in the field of key management. QoS routing is introduced in Section 3; the suggested trust-based routing method is described in Section 4 along with the algorithm; the simulation results are discussed in Section 5; and the paper is concluded in Section 6 with references cited.

2. LITERATURE SURVEY

Trust is an important role in the process of routing, data aggregation, harmful node detection, time synchronization, accuracy, allotment of nodes from monitoring techniques as included by Pathan et al [1]. This reviewed work includes the characteristics of the nodes in the trustworthy analysis.

Singh et al [3] designed a trust determination algorithm which is mainly concentrated for health care system in the basis of weighted voting of each node in the wireless body area network. This node is processed with the receiving of messages from the nearby neighborhood nodes. By the receiving process acknowledgement, we can estimate the trustworthy procedure of the one-hop neighbor nodes. He also surveyed that the miss-behavioral detection is the major problem as it affects the nodes in sharing the routing information from source towards destination. The trusting process is implemented to secure the routing mechanism by formulating the trusted weights in the nodal points. Ferdous et al. [4] analyzed the unique scheme of trust determination in the MANETs which is termed to be the Network Trust Management (NTM) scheme which implement the responsibility of constructing the trust and monitoring the trust at the nodal level.

Lwin et al. [5] came to the conclusion that the Dynamic Trust-Based Resources (DyTR) system, which is a kind of trust-based management in the routing protocol, is based on the network structure and its members' behaviour with regard to the external environment. The work that was put into practice is based on the ad-hoc networks' cognitive model.

The review work of Harold and Golden et al [6] implies that policy-based administration protocol can prevent the loss of data about the nodes during the routing protocol. Am et al. [7] implemented the routing algorithm which is represented as the secure and Energy Efficient Trust Aware Routing Protocol (ETARP) which increases the reliability and protection against the harmful nodes. The major part of the reviewed work is the simulation results which provides the better security during the packet delivery with the comparison with existing protocols of routing.

According to Gayathri and Janaki Raman's [8] theory, a combination of consumed energy, time taken for the communication, packets delivery ratio (pdr), strength and quality of the signal make up the trust in ad-hoc networks. Since the establishment of a trustworthy and safe routing protocol, the distance vector protocol has been used to divert harmful node attacks. As a result of employing an OLSR-based strategy, the two main implementations, Black Hole Attack and Jelly Fish Attack, have been removed.

Sheikh et al [9] discovered that marsh formalism technique which is based on the ReGreT and FIRE that add the major advantages toward s the third parties which the major information about the social structures implemented with the trusted sources. Even though it is powerful trust-based technique it would have the various limitations such as limited information about the nodes is not accessible. Vaseeret al [10] represented that the distributed trust-based security scheme which is free from the various attacking methods such as Probe, Denial-of-Service (DoS), Vampire, User-to-Root (U2R). This simulation results concludes that the secureness can be analyzed with the variable nodal densities in the network administration.

RESEARCH ARTICLE

Wadhwani et al. [11] represented the analytical work that gives the accuracy of trusted formation in routing protocol. As the two trusted protocols have been developed which is tends to be entropy-based and probability-based models, which satisfy all the axioms. By the improvement in the network throughput the developed models detect and eliminate the harmful nodes within the network. The certificate distribution and a Trust-based threshold revocation technique were concluded by Rajkumar et al.[12] By merging public key certificates, the approach provides a solution to the fulfilled process for certificate revocation and validation. According to Cho et al, the composite key management solution will perform worse with harmful nodes [13].

The central point control strategy relies on the preset central node to control the information of all replica nodes, so it is also called a centralized consistency maintenance strategy. Like many centralized networks, this strategy is a static, active, and fast consistency maintenance Strategy. Due to the existence of the preset central node, and the central node knows the location of all replica nodes, the central point control strategy greatly simplifies the process of finding replica nodes in the consistency maintenance process. At present, there are a few small-scale P2P systems this strategy is adopted. However, as the P2P system expands more and more rapidly, the replica node information that the central node needs to record has also increased exponentially, and the processing speed and storage space of the central node have become the limitation of the central point control strategy consistency maintenance efficiency. The bottleneck [13]. More serious is that the central node may be damaged by malicious attacks or be paralyzed by a Denial of Service (DoS) attack, which brings the risk of a single point of failure to the entire consistency maintenance system [14].

The distributed update strategy does not rely on the preset central node to control the location information of all replica nodes. It is a distributed and scalable consistency maintenance strategy. It is very suitable for the large-scale and highly turbulent P2P network, and it is also suitable for most structured P2P systems, such as CAN [15], Chord [16], Pastry [17] and Tapestry [18]. This strategy can be subdivided into: Flooding-based consensus Maintenance strategy [19] and structured-based consistency maintenance strategy. The consistency maintenance strategy based on flooding uses flooding to propagate updates. The advantage of this propagation method is that it can be turbulent at the node. The update propagation process is effectively completed under the conditions of, and it has good node failure tolerance; but at the same time, the shortcomings of this method are also obvious. Storms and other issues [20]. In order to reduce data redundancy, other consistency maintenance methods adopt a structure-based consistency maintenance strategy. This type of method organizes the replica nodes into a special structure, so that the replicas in this structure. The node will only receive one update, thereby reducing data redundancy. However, the damage or departure of the node will destroy the structure and cause the update propagation to fail [21]. Structure-based consistency maintenance strategies can be further subdivided into push-based consistency maintenance strategies (Push-based), query-based consistency maintenance strategies (Pull-based), and prior information-based consistency maintenance strategies (Prior information-based). The push-based consistency maintenance strategy propagates updates through message push, and the replica node can only passively wait for the update; the query-based consistency maintenance strategy propagates the update through the replica node inquiry, that is, the node that needs to update receives the update , To a certain extent, reduce the overhead and the occupancy rate of network resources; the consistency maintenance strategy based on a priori information builds a certain structure by collecting certain information (such as geographic location information, interests, etc.) to disseminate updates. In this way, more consideration can be given to the node's own factors in terms of building structure and distributing messages.

Wang et al. [22] et al. used trust management to build a two-layer blockchain for data sharing to ensure the security of data transmission and proposed relevant incentives to encourage information sharing between nodes. Similarly, others assigned trust values to vehicles and judged information based on this. False situation and use node trust value to motivate vehicles to perform well; on the premise of ensuring data security when transmitting and storing data, through smart contracts and machine learning, shared data can be allocated reasonably.

Ha and Shim [23] use the You Only Look Once (YOLO) algorithm, which guesses the type and location of objects, to detect intrusions by using artificial intelligence techniques to determine the presence of wildlife in images captured by webcams. Although this study is significant in that it attempted to apply the latest technology, it has the disadvantage that a server-class computer is required for high-volume transmission communication and image processing for images, that there is an error probability of the analysis results, and that areas outside the field of view of the webcam cannot be detected.

Keum and Ko [24] presented a distributed transmission technique that uses the Q-learning result to prioritise the reliability of mission-critical data while taking energy, QoS, and trustworthiness into account. When data is transferred via a single path, network performance might suffer. This technique can fix this issue. By giving mission-critical data the greatest priority and sending it along the way with the highest MAX-Q value, the proposed distributed transmission technique maintains dependability while sending data with comparatively lower priority along the less-than-ideal path

RESEARCH ARTICLE

that fulfils all requirements. While guaranteeing the accuracy of the most crucial data first, this approach may serve the needs of all mission-critical data. Additionally, by suggesting flexible weights that take energy into account, it is feasible to run devices with limited resources using technology appropriate for mission-critical wireless sensor network operating conditions. To efficiently detect malicious nodes, a configurable threshold taking into account the connection condition was proposed. Effectively detecting malicious nodes is achievable based on data occurrence and attack conditions.

This study's main goal is to create a secure optimization routing method for MANET. The Bacteria for Aging Optimization Algorithm (BFOA) [25] algorithm serves as its foundation. The cluster head selection and intrusion node detection are key components of the secure iterative routing method. The indirect, direct, and most recent trust values with the highest values are used to determine the cluster head. For effective and observable routing, the intrusive node is identified using the threshold value concept. Moving forward requires selecting the cluster heads from the MANETS natural environment that have the highest value of recent, indirect, and direct trust. After all productive routing, which the BFOA may access, an intrusion detection technique is then used to identify intruded nodes and guarantee that their packets are successfully delivered from origin to destination. The capacity, connectivity, and capabilities of the path determine how well the path fulfils its stated purpose. The mining and modification stages of the algorithm can be balanced well even though the suggested approach makes use of the benefits of the BFOA. Further in Table 1 methodologies proposed by various researchers and their limitations are tabulated.

Table 1 Pros and Cons of Various Methods

Author(s)	Methodology Proposed	Limitations
Pathan et al [1]	Trust based Routing Scheme with Pattern Discovery	When the topology is dynamic and nodes are in motion then the trust score evaluation is not capable.
Singh et al [3]	Bilingual distribution-based trust-management system	Possible only to the one hop neighbour nodes in the wireless body area network.
Ferdous et al. [4]	The Dynamic Trust-Based Resources (DyTR) system	System applicable only to the selective topology.
Am et al. [7]	Considers ditch ratio as the primary social trust component between nodes.	Estimation of trust value between node is not sufficient and energy consumption is also high, when node falls in attack.
Sheikh et al [9]	Proposed a protocol based on the social structures was implemented	Even though it is powerful trust-based technique. Some limitations such as limited information about the nodes is not accessible.
Vaseer et al [10]	Distributed trust-based security scheme	Resistive only to selective attacks and even not secured to gray hole and black hole attacks.
Wadhwani et al. [11]	Proposed a revocation technique based on trust threshold.	The trust calculation for the attacked nodes are not reliable. Even sometime gives worst trust value.
Attkan and Ranga et al. [21]	Structure-based consistency maintenance strategy is proposed.	Departure of the node will destroy the structure and cause the update propagation to fail.

2.1. Problem Statement

As a result of the study, the reviewed approach can have an easy trust-based mechanism, which suggests that security flaws can be removed using hard security parameters. The trust thresholding is carried out throughout the routing protocol, which tends to minimize the issues in the CTPKM technique. As a result, the proposed work provides a trusted and secure routing protocol that is constructed by merging social and QoS trust in a QoS routing scheme. This combination will reduce the activeness of the harmful nodes within the network structure.

3. TRUST-BASED QOS ROUTING

This section explains the algorithm flow of the proposed work which implies in the reduction of harmful nodes with the routing protocol. The methodology discusses the proposed model structure which forms the secured routing protocol and the variations from the other existing algorithms. As routing protocols suffers mainly by the harmful nodes, the elimination of that harmful node will be

RESEARCH ARTICLE

real task. Various techniques have been adopted to eliminate the harmful nodes which would be explained below.

3.1. Ad-Hoc On-Demand Distance Vector Routing Protocol (AODV)

The protocol assumes that the IP addresses of source and destination process will be known in advance. The objective of the protocol is to determine the path of the nodes to communicate the required information to other nodes since the source and destination are known. By this can be affected by the harmful nodes which tends to change the path of communication and the trust of neighbour nodes will calculated using equation (1).

$$Neighbor_{Trust} = (Hop\ Count \times w1) + (Route\ Trust \times w2) \quad (1)$$

Where, w1 will be the 40% of the hop count and w2 will be the 60% hop count, Route Trust accessed from RREP control packets. By carrying the Neighbor trust in the AODV it will reduce the harmful nodes but the demerits lie in the calculation as the routing process from the identified trust will tend to implemented with the longer delay. This delayed process may lead to higher bandwidth and higher energy consumption.

3.2. Enhanced Trusted Routing scheme with Pattern Discovery (ETRS-PD)

In a routing procedure, the sender assesses a neighbour node's distrust by monitoring the actions taken by that neighbour. This routing system is designed to limit the attackers' desire to engage in various kinds of packet-forwarding failures by integrating an enhanced trust-based model and a technique for discovering attack patterns. The following equation (2) is used to determine the neighbour trust:

$$Neighbor_{trust}(t) = w1 \times CDR(t) + w2 \times DDR(t) + w3 \times EC(t) + w4 \times DTR(t) \quad (2)$$

Where CDR is Control Dropping Ratio, DDR is Ditch Ratio, EC is Energy Consumption and DTR is Ditch Ratio and the weights w1 to w4 must be a positive value greater than zero and the total sum of weights must be 1. DDR is defined as the ratio of the number of times a neighbor node is found to be distrusted to the total number of nodes. The key drawbacks of this routing mechanism are that it does not rely on any strategy to disseminate information about the hostile hub, therefore the chances of an impact are quite slim. To address these issues, a new routing protocol has been developed, based on the Adversary model, which is implemented in the proposed work.

3.3. The Adversary Model

In the proposed study, an adversarial model for packet dropping is established. By frequently monitoring the harmful nodes, this may bring about changes in the harmful nodes. The sequence number is based on the detrimental node's highest recorded value. The harmful node responds to a Route Request (RREQ) during the routing process with the highest possible value of the destination sequence number and the lowest hop count, which is 1. A trustworthy source node may readily circumvent the adversary utilizing the AODV protocol, even in the absence of a fully functioning channel for the compromised node. After that, the attacker spends half of his time trying to drop packets. Attacks known as packet dropping happen when data packets are being routed. The design of secure routing will be built on the adversarial concept. The trustworthy creation of the routing protocol initiates this process.

4. PROPOSED DESIGN FOR SECURE AND TRUST-BASED QOS ROUTING (PROPOSEDTRS)

The proposed design for secure and Trust-based QoS Routing includes the path allocation of the intermediate nodes. The implemented technique consists of following steps to undergo trust management.

- Trust-Recommendation.
- Trust-Update
- A secure QoS routing technique based on trust.

4.1. Trust Recommendation

The major processing of Trust Recommendations is as follows:

a. Finding the starting trust value for newly added node, to analyze whether other nodes can trust the new node or not.

b. Regular observation/updating the trust value of all nodes with the certain time interval.

c. Communicate the newly developed node with the other node with the lesser number of overheads.

Trust Recommendation is mostly concerned with multivariable environmental circumstances, in which the parameters must be adjusted in order for the nodes to operate better. The Ad-Hoc On-Demand Distance Vector Routing Protocol (AODV) transmits the majority of the data used to assess network connectivity. The memory of each node may be used to make better routing decisions. Better communication will be achieved by collecting information about surrounding nodes.

As part of the recommended routing strategy to obtain QoS trust recommendations, messages are exchanged. Based on parameters like residual energy, channel quality, link quality and neighbouring nodes may use this approach to assess the features of other nodes. The network collapses when these elements are coupled with more hazardous and harmful nodes. If a sending node is a trusted node, the intimacy with that

RESEARCH ARTICLE

node is calculated, recorded, and used to create an appropriate routing path. The volume of interaction with a transmitting node is determined by the total number of direct contacts.

4.2. Trust Update

The trust-based paradigm is primarily concerned with network transmission. The trust value decays over time as the interaction between the neighborhood nodes is calculated. Because nodal points are mobile, interactions between nodes and other members may be reduced. Disconnection due to unsuccessful connections to a node, scheduled disconnection (for power management), and unexpected disconnection are some examples of this (battery about to die and cable disconnection). The drawbacks of each node demonstrate resource-constrained MANETs. The sender assesses the trustworthiness of the nearest node based on connections with its neighbours throughout the routing process. To identify all the nodes that function poorly, calculate historical trust consistently in our proposed trust-based architecture after a predetermined time period known as a trust update. The neighbour trust value is calculated using the following factors (a to g):

4.2.1. Data Packets Forwarding Ratio (DFR)

The DFR is the proportion of all data packets successfully transported by a node to all data packets that should be forwarded. The trust value is then calculated using the remaining variables once this criterion has been evaluated for each level.

4.2.2. Control Packets Forwarding Ratio (CFR)

By dividing the total number of packets sent that are intended for forwarding by the quantity of control packets, CFR is calculated. For indications of potentially harmful node behaviour, the total number of packets and the restricted packets are continuously monitored.

4.2.3. Intimacy Level

The degree of closeness displays the distance between the two nodes as well as other facets of their interaction. The intimacy with a transmitting node is computed, recorded, and used to create the best routing path if that node is a trusted node. The volume of direct connection with a transmitting node determines the level of engagement.

4.2.4. Residual Energy

Energy required by the packets of data to undergo the transmitting and receiving process when the traffic takes place. It is calculated as in the equation (3),

$$Ec(n) = \left[P_t \times \frac{Ds}{Dr} - G_t \times \frac{Ds}{Dr}\right] + nPo \qquad (3)$$

Ec(n) denotes the energy consumed by the node, Pt the power required to transmit signals, Ds the size of the data packet, Dr the transmission speed, Pr the power used to receive signals, and Po the power consumed while neighbouring nodes are being overheard.

4.2.5. Link Quality

The connection time between two nodes is used to compute it. Network failure and harmful nodes are reduced as link quality improves. The duration of a link between nodes may be computed using the following formula. To begin, we must determine the distance between nodes as well as their relative velocity. In the event that a connection joins nodes A and B, let D stand in for the distance between them. It might be calculated with equation (4):

$$D = x = \sqrt{((x2 - x1)^2 + (y2 - y1))^2} \qquad (4)$$

Where the x1, x2, y1, y2 represents the coordinates of nodes A and B.

4.2.6. Channel Quality

Channel quality reveals the existence of channels at the time of transmission and reception. By analyzing the channel quality, one can detect the transmission's interference. The channel quality permits secure communication while reducing the end-to-end latency of the communication process. It is derived as in the equation (5):

$$H = G_t \times G_r \left(\frac{\lambda}{4\pi d}\right)^2 \qquad (5)$$

Where l stands for the signal wavelength, Gt stands for transmitter gain, Gr stands for receiver gain, and d stands for the distance between the source and the destination.

4.2.7. Signal Strength

If the signal intensity is weak, the closest node is excluded. The distance between nodes with smaller values is taken into consideration as transmission power is inversely proportional to node distance. It may be calculated using the equation (6):

$$Pr = Pt * (1 / d) n \qquad (6)$$

Where d is the distance between the nodes and n is the environmental factor.

The following equation (7) is used to get the total neighbour trust value:

$Neighbor_{Trust}$ = (*w1* x DFR) + (*w2* x CFR) + (*w3* x Intimacy level) + (*w4* x Energy (Remaining)) + (*w5* x LinkQuality) + (w6 x ChannelQuality) + (w7 x Signal *Strength)* (7)

Where *w1 to w7* are the weights assigned for the QoS parameters mentioned and it must be a positive value between 0 and 1. The total sum of w1 to w7 must be 1. As the activity of nearby nodes varies over time, so does the value of trust. Malicious nodes are distinguished from benign nodes using the trust threshold value for the nodes. When the node's signal

RESEARCH ARTICLE

strength increases, the vulnerable node will be eliminated in accordance with the trusted value. The value of neighbour trust, which typically maintains a constant weight, is increased through this procedure. As we assess the other procedures, the Neighbor trust gains significance as the other parametric values rise. The action increased the neighbour trust quantity, which raised the trustworthiness of other nodes.

4.3. A Secure QoS Routing Technique Based on Trust

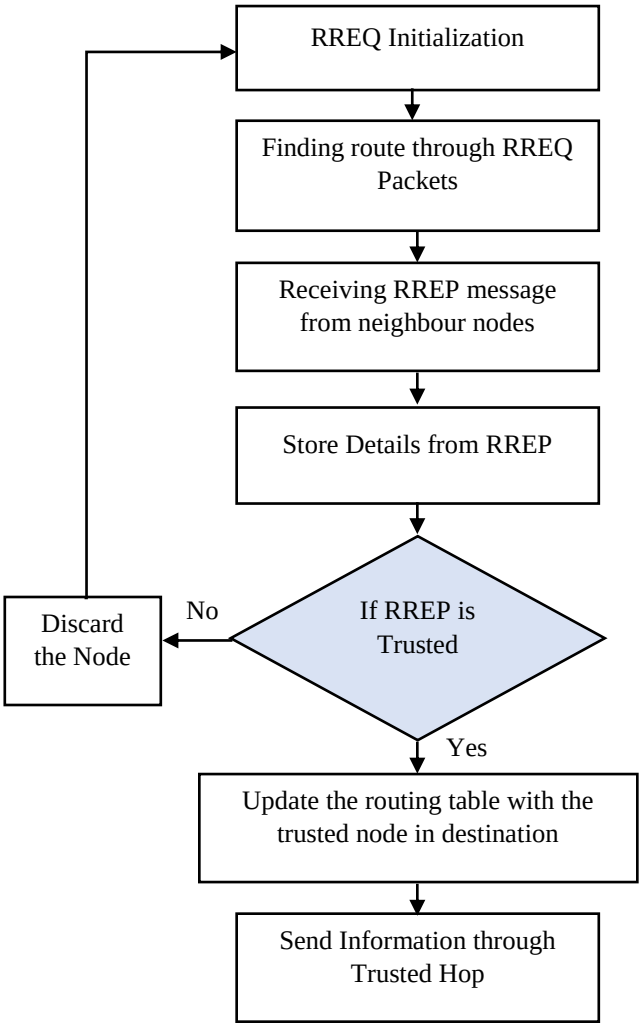

Figure 1 Proposed Trust Based Secure Quality of Service (QoS) Routing Strategy

Security and trust go hand in hand. In trust-based security, access rights for security protection are increased as trust levels rise. According to "the closeness of the relationships between entities that engage in a protocol exchange," trust in MANETs may be evaluated. There are two different kinds of trust: social trust and quality of service (QoS) trust. While social trust is based on interpersonal relationships such as friendship, honesty, privacy, and intimacy, QoS trust is based on knowledge, dependability, expertise, the quantity of packets delivered, and other factors. For securing the routing process in MANETs, a few recommendations have already been made. Even though cryptographic techniques are frequently used in routing to prevent interference from the adversary, such an approach may not be feasible for real MANETs due to high computational overhead and the inability to detect attacking nodes given the high mobility of MANETs, where nodes continuously enter and exit the networks. Nodes can effectively track and forecast neighbouring nodes' behaviour when "trust" is introduced into such a hostile environment. When nodes are dependent on one another to achieve their shared objectives in a highly dynamic system, the concept of trust is extremely helpful. By identifying and isolating untrusted nodes, trust-based routing has been viewed as a successful defence against security issues brought on by malicious nodes in MANETs.

All nodes, including the source, intermediates, and destination, are involved in the route discovery process. Figure 1 shows how to isolate a malicious node, and Algorithms 1 go into more detail about the process. All nodes, including the source, intermediates, and destination, are involved in the route discovery process. The procedure for sending data to the target is as outlined in Algorithm 1: The source node first looks for the entry for the destination node in its routing database before starting data transmission. Data is sent to the destination through a trusted hop if such an entry is present.

```
//Actions by the Source Node for RREQ (Route //Request)
IF (received RREQ not specific to the attacked node) then
Ignore received RREQ;
    InitializeDestSeqno to Null or zero;
    DestSeqno= RREQ;
    DesSeqno=DestSeqno + Rand (1:10);
    Set HopCount to 1;
    Evaluate the neighbor trust score using eq (7);
    Resend the forged response RREP to source node;
ELSE
    RREP = Seqno;
    Set HopCount to 1;
    Evaluate the neighbor trust score using eq (7);
    Drop RREQ;
    Resend genuine route response RREP to the source;
END IF
```

RESEARCH ARTICLE

// Actions by the Malicious Node for Route //Response (RREP)

IF (datapacket is not for attacked node) then

IF (time1>=CurrentTime<=time2)

Evaluate the neighbor trust score using eq (7);

Drop the received packets from the source;

ELSE

If (ValidPath)

Forward Data packets to the valid path;

End If

END If

ELSE

Data Packet Received by the node;

END IF

Algorithm 1 Proposed Secure Trust Based QoS Routing (Proposed TRS)

In order to find a route to the destination, the source node engages in route discovery by flooding the network with Route Request (RREQ) packets. Before beginning data transmission, the source node first looks for the destination node's record in its routing database.

5. EXPERIMENTAL RESULTS

The Proposed Trust based Secured QoS Routing Scheme (Proposed TRS) design was implemented using the NS-2 (ver. 2.34) simulator system. The performance of our suggested design is evaluated using parametric calculations like Packet Drop Ratio (PDR), Routing Overhead (RO), Energy Consumption (EC) and Packet Drop Ratio (PDR %). The table 2 shows the simulation parameters used for the evaluation.

Table 2 Initial Parameters in Ns2 Simulation

Parameter	**Value**
Simulator	NS 2.34
Routing Protocol	AODV, ETRS-PD, PROPOSED TRS.
Scenario Size	1000 x 1000 m^2
Simulation Time	240 s
Number of Nodes	50
Misbehaving Nodes	0 – 40%
Numberof Connections	15
Pause Time	5s
Traffic Type	CBR/UDP

5.1. Packet Delivery Ratio (PDR)

Performance of the proposed work can be increased by the changes in the mobility of the harmful nodes. The overall analysis of harmful nodes is about 10%.Packet Delivery Ratio (PDR) of the implemented work tends to be 75% to 50%.

When the problematic nodes are eliminated, the network's execution speed rises and linkage failures and packet loss decreases. Figure 2 compares the Ad Hoc On Demand Distance Vector Routing Protocol (AODV) and ETRS-PD with the Proposed TRS Routing scheme with Pattern Discovery to illustrate the Packet Delivery Ratio (PDR) against harmful nodes (Proposed TRS).

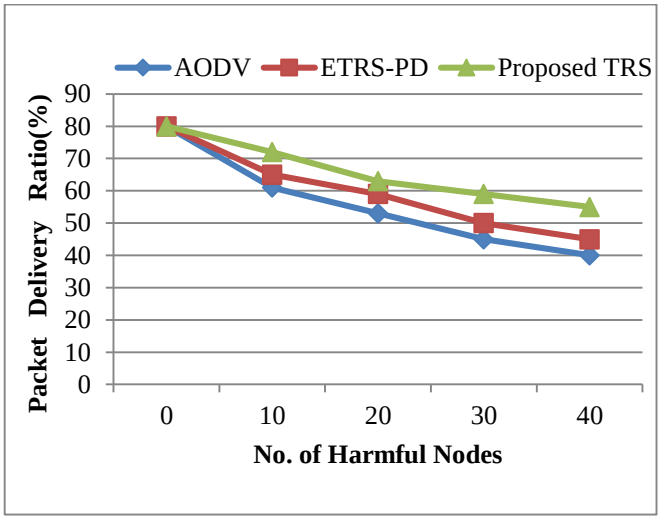

Figure 2 Packet Delivery Ratio (PDR) Against Harmful Nodes

The fraction of malicious nodes will rise, which will result in an increase in packet loss. When the existing algorithms are compared, ETRS-PD tends to drop by 58% while AODV tends to decline by 35% of detrimental nodes. As the harmful nodes are removed based on their trust value, the suggested approach proposed TRS improves by 67%.

5.2. Routing Overhead (RO)

The Figure 3 represents the Routing overhead analysis of the proposed work. As the comparison obtained between the various techniques the proposed protocol tends to have the improvement between 4.03 to 6.2. The RO range of the AODV protocol tends to be 4.8 to 9.9 range whereas the ETRS-PD ranges from 4.8 to 6.5. Since the proposed work

RESEARCH ARTICLE

have the lesser number of harmful nodes the link quality between the nodes will be high which lead toward the lesser Routing Overhead. Routing Overhead is further improved by the proposed TRS (RO). It is evident that the ease with which malicious nodes may inflict harmful node increases. There are fewer route failures because Proposed TRS only chooses secure nodes with strong links, which necessitates re-routing fewer control packets for route formation.

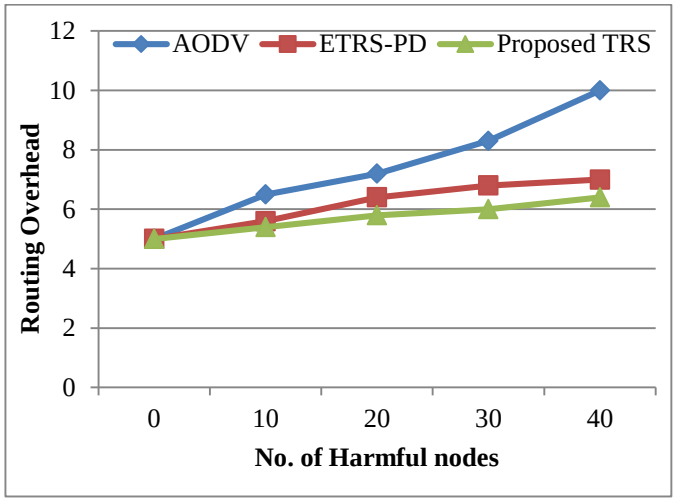

Figure 3 Routing Overhead of Harmful Nodes

5.3. Energy Consumption (EC)

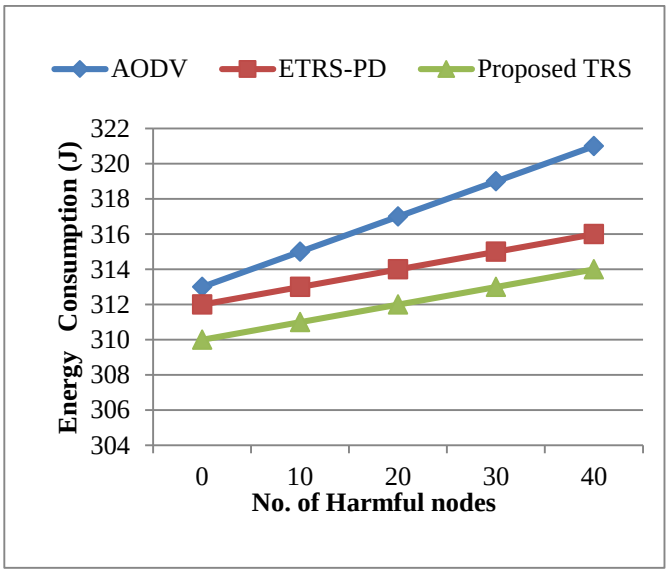

Figure 4 Energy Consumption (EC) Against Harmful Nodes

The proposed protocol consumes lesser amount of energy when number of harmful node increases. While AODV and ETRS-PD protocols consumes too high energy when rise in number of harmful nodes. A plot has been made for Number of harmful nodes and energy consumption and is shown in Figure 4. From the various observations of the AODV and ETRS-PD protocols, it is cleared that the energy consumption of AODV and the ETRS-PD protocols lies between 311.96 to 313.5 J whereas the proposed TRS technique consists of Energy Consumption between 309.24 J to 310.10 J. This will be useful to eliminate the route failure due to the harmful nodes. Thus, the proposed work yields the certain accuracy range as there was a reduction in the harmful nodes.

5.4. Packet Drop Ratio (%)

The packet loss ratio represents the ratio of the number of lost packets to the total number of sent packets. It is measured between the packet dropped and malicious nodes. The observed values are plotted in Figure 5.

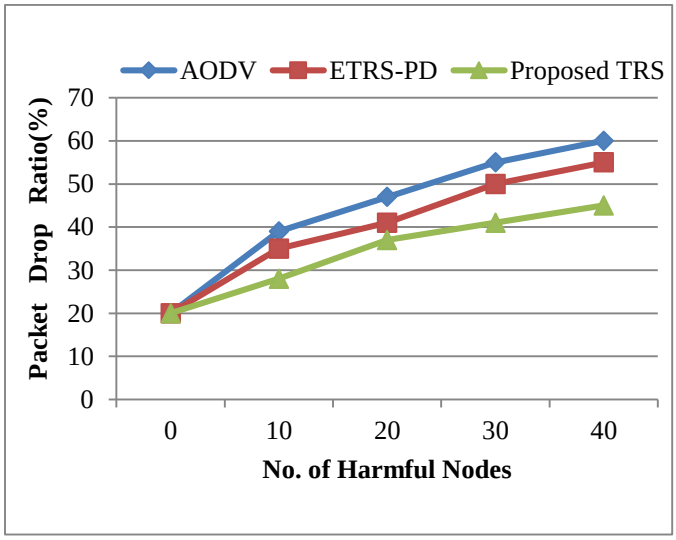

Figure 5 Packet Drop Ratio (PDR %) Against Harmful Nodes

It is observed that from the Figure 5 when the number malicious node increases then the packet drop rate is also increases and the performances of the networks are highly affected. The fraction of malicious nodes will rise, which will result in an increase in packet loss. When the existing algorithms are compared, AODV tends to drop by 60% while ETRS-PD tends to decreased by 55%. As the malicious nodes are removed based on their trust value, the suggested approach proposed TRS improves by 55%. The proposed TRS gives best results because it eliminates the malicious nodes during the communication.

6. CONCLUSION

Based on the simulation results, the proposed research reveals that combining QoS trust with social trust can improve routing analysis results in MANET networks and other types of ad-hoc networks. This will enhance the network's quality and security during source-to-destination transmission. The channel quality, link residual life, residual energy, CFR, DFR, intimacy level, and honesty level routing processes are all

RESEARCH ARTICLE

improved by this newly developed routing protocol. Due to enhancements made to the routing procedure and the addition of additional trust components, Proposed TRS can regularly outperform ETRS-PD and AODV in terms of packet delivery ratio, routing overhead, and energy consumption. When certain parameters are taken into consideration, routing errors are decreased and network communication speed is raised. The reduction of harmful nodes in the network is one of the main advantages of the recommended approach. As a further step of research, the same scheme can be implemented in decentralized networks such as like blockchain and IoT applications.

REFERENCES

[1] Pathan, Muhammad Salman, Nafei Zhu, Jingsha He, Zulfiqar Ali Zardari, Muhammad Qasim Memon, and Muhammad Iftikhar Hussain. 2018. "An Efficient Trust-Based Scheme for Secure and Quality of Service Routing in MANETs" Future Internet 10, no. 2: 16. https://doi.org/10.3390/fi10020016.

[2] Kumar, M., Bhandari, R., Rupani, A., & Ansari, J. H. (2018, June). Trust-based Performance Evaluation of Routing Protocol Design with Security and QoS over MANET. In 2018 International Conference on Advances in Computing and Communication Engineering (ICACCE) (pp. 139-142). IEEE

[3] Singh, S., Chawla, M., Prasad, D., Anand, D., Alharbi, A., & Alosaimi, W. An Improved Binomial Distribution-Based Trust Management Algorithm for Remote Patient Monitoring in WBANs. Sustainability, 14(4), 2141, 2022.

[4] R. Ferdous, V. Muthukumarasamy, and A. Sattar. A Node-based Trust Management Scheme forMobile Ad-Hoc Networks. Proceedings of the 4thInternationalConference on Network and SystemSecurity (NSS), pp. 275–280, 2010

[5] Lwin, M. T., Yim, J., & Ko, Y. B. (2020). Blockchain-based lightweight trust management in mobile ad-hoc networks. Sensors, 20(3), 698.

[6] Harold Robinson, Y., & Golden Julie, E. (2019). MTPKM: Multipart trust based public key management technique to reduce security vulnerability in mobile ad-hoc networks. Wireless Personal Communications, 109(2), 739-760.

[7] Am, A. B. (2021). High energy efficient lifetime management system and trust management framework for manet using self-configurable cluster mechanism. Peer-to-Peer Networking and Applications, 14(3), 1229-1241.

[8] Gayathri, D., & Raman, S. J. (2017, January). Pltrust AODV: Physical logical factor estimated trust embedded AODV for optimised routing in Manets. In 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS) (pp. 1-5). IEEE.

[9] Sheikh MS, Liang J, Wang W. Security and privacy in vehicular ad hoc network and vehicle cloud computing: a survey. Wireless Communications and Mobile Computing. 2020 Jan 17;2020.

[10] Vaseer, G., Ghai, G., &Ghai, D. (2018, December). Distributed Trust-Based Multiple Attack Prevention for Secure MANETs. In 2018 IEEE International Symposium on Smart Electronic Systems (iSES) (Formerly iNiS) (pp. 108-113). IEEE.

[11] Wadhwani, G. K., Khatri, S. K., & Mutto, S. K. (2020). Trust framework for attack resilience in MANET using AODV. Journal of Discrete Mathematical Sciences and Cryptography, 23(1), 209-220.

[12] Rajkumar, B., & Narsimha, G. (2016). Trust based certificate revocation for secure routing in MANET. Procedia Computer Science, 92, 431-441.

[13] Rahmani M, Benchaiba M. A comparative study of replication schemes for structured P2P networks[C]. Proc of the 9th Int Conf on Internet and Web Applications and Services. Lisbon, 2014: 147-158.

[14] Lu, K. D., Zeng, G. Q., Luo, X., Weng, J., Zhang, Y., & Li, M. (2020). An adaptive resilient load frequency controller for smart grids with DoS attacks. IEEE Transactions on Vehicular Technology, 69(5), 4689-4699.

[15] De la Rocha, A., Dias, D., & Psaras, Y. (2021). Accelerating Content Routing with Bitswap: A multi-path file transfer protocol in IPFS and Filecoin.

[16] Elbreiki W, Hassan S, Habbal A, et al. A Comparative study of chord and pastry for the name resolution system implementation in information centric networks[C]. The 4th Int Conf on Internet Applications, Protocols and Services. Kuala Lumpur: IEEE, 2015: 359-367.

[17] Naik, A. R., & Keshavamurthy, B. N. (2020). Next level peer-to-peer overlay networks under high churns: a survey. Peer-to-Peer Networking and Applications, 13(3), 905-931.

[18] Djellabi, B., Amad, M., & Baadache, A. (2022). Handfan: A flexible peer-to-peer service discovery system for internet of things applications. Journal of King Saud University-Computer and Information Sciences.

[19] Seddiki M, Benchaïba M. SWS: A smart walk mechanism for resources search in unstructured mobile P2P networks[C]. The 1st Int Conf on New Technologies of Information and Communication. Cairo: IEEE, 2015: 1-6.

[20] An, N., Liang, X., Zheng, X., Yuan, S., Wang, X., & Guan, Z. (2022, May). Achieving Secure and Efficient P2P Data Trading based on Blockchain for Internet of Things. In Proceedings of the Fourth ACM International Symposium on Blockchain and Secure Critical Infrastructure (pp. 139-144).

[21] Attkan, A., & Ranga, V. (2022). Cyber-physical security for IoT networks: a comprehensive review on traditional, blockchain and artificial intelligence based key-security. Complex & Intelligent Systems, 1-33.

[22] Wang S M, Ye D D, Huang X M, et al. Consortium blockchain for secure resource sharing in vehicular edge computing: a contract-based approach. IEEE Transactions on Network Science and Engineering, 2021, 8(2): 1189-1201.

[23] Y. S. Ha, J. C. Shim. "Wild Animal Repellent System for Prevention of Crop Damage by Wild Boars," Journal of Korea Multimedia Society, Vol. 24, No. 2, pp. 215-221, February 2021.

[24] Keum, D., & Ko, Y. B. (2022). Trust-Based Intelligent Routing Protocol with Q-Learning for Mission-Critical Wireless Sensor Networks. Sensors, 22(11), 3975.

[25] Srilakshmi, U., Alghamdi, S. A., Vuyyuru, V. A., Veeraiah, N., & Alotaibi, Y. (2022). A secure optimization routing algorithm for mobile ad hoc networks. IEEE Access, 10, 14260-14269.

Authors

G. Sripriya received her master degree in Computer Science from Madurai Kamaraj University, Madurai in 2001 and completed her M.Phil Computer Science in 2004. She is currently working as Assistant Professor in the department of Computer Science at KSG College of Arts and Science, Coimbatore. She is pursuing the Ph.D degree at GRD College of Science, Coimbatore. Her research interests include Mobile Ad hoc Network, Artificial Intelligence, and Network Security.

Dr. Santha T received her Post Graduation from P.S.G. College of Arts and Science, Coimbatore in 1987 and M. Phil. from Bharathiar University in 1991. She also completed her PhD in Computer Science from Bharathiar University during 2012. She is presently working as Principal of Dr. G.R.D. College of Science, Coimbatore. She has more than two decades of teaching and research experience. Her research interests on Computer Applications and Optimization Techniques, Multimodal Transportation, Image processing and Computer Simulation.

RESEARCH ARTICLE

How to cite this article:

G. Sripriya, T. Santha, "A Trust-Based Design for Secure and Quality of Service Routing in Mobile Ad Hoc Networks", International Journal of Computer Networks and Applications (IJCNA), 9(5), PP: 522-532, 2022, DOI: 10.22247/ijcna/2022/215913.