Computer Systems
Science and Engineering

Tech Science Press

DOI: 10.32604/csse.2023.033326
Article

Energy Based Random Repeat Trust Computation in Delay Tolerant Network

S. Dheenathayalan* and B. Paramasivan

National Engineering College, Kovilpatti, 628503, India
*Corresponding Author: S. Dheenathayalan. Email: dheenathayalansphd@gmail.com
Received: 14 June 2022; Accepted: 08 October 2022

Abstract: As the use of mobile devices continues to rise, trust administration will significantly improve security in routing the guaranteed quality of service (QoS) supply in Mobile Ad Hoc Networks (MANET) due to the mobility of the nodes. There is no continuance of network communication between nodes in a delay-tolerant network (DTN). DTN is designed to complete recurring connections between nodes. This approach proposes a dynamic source routing protocol (DSR) based on a feed-forward neural network (FFNN) and energy-based random repetition trust calculation in DTN. If another node is looking for a node that swerved off of its path in this situation, routing will fail since it won't recognize it. However, in the suggested strategy, nodes do not stray from their pathways for routing. It is only likely that the message will reach the destination node if the nodes encounter their destination or an appropriate transitional node on their default mobility route, based on their pattern of mobility. The EBRRTC-DTN algorithm (Energy based random repeat trust computation) is based on the time that has passed since nodes last encountered the destination node. Compared to other existing techniques, simulation results show that this process makes the best decision and expertly determines the best and most appropriate route to send messages to the destination node, which improves routing performance, increases the number of delivered messages, and decreases delivery delay. Therefore, the suggested method is better at providing better QoS (Quality of Service) and increasing network lifetime, tolerating network system latency.

Keywords: MANETs; energy competent dynamic source routing protocol; delay tolerant network; energy-based random repeat trust computation; quality of service; network lifetime routing

1 Introduction

A crucial duty is now performed by the mobile and its connected utilities, and it also regulates human beings for their needs. The progression in wireless communications has offered essential advantages. People can communicate with each other in both city homes and offices and rural areas. The wireless applications enhancement necessity and competently supervise network traffic, jamming, and data transmission, and should not collision requests and network performance. The

data transmission for a severe situation or necessity must attach to the QoS promise for the application requires on the accessible resources of the network and its respective routing protocols. The MANET routing formation is highly dynamic, and source dependent. Here, the several senders battle for link bandwidth and the most favorable route to attain the throughput performance. MANET is an autonomous structure of supple hosts linked with isolated links that have lesser establishments. The hosts are permitted to progress around as frequently as possible. The MANET routing protocols must be energetic to receive the routing choice energetically in the network at all times or else, packet loss will happen. Such systems are sound in military and other deliberate requests. MANETs are valid in cases where infrastructure for communication never exists, or infrastructure is expensive or intricate to carry out. Mobile Ad hoc networking allows the network devices to construct and maintains connections to the network. The transmission of data over error-prone MANET is essential as these networks are mainly deployed. The MANET communication includes two phases consisting of 1. Route Discovery and 2. Data transmission is calculating the optimum route from a sender node to a destination node using a grouping of transmitting or receiving devices. The extra routing protocols organized for MANETs execute convinced jobs for data transmission. The topologies modification, network partition, bandwidth, superior error rates, intrusion, power restraints, and conflict are the network control issues for superior level protocols design that entails routing and executing applications via the Quality of service (QoS). The energy utilization reduction gets managed by power transmission, which consequently products in successful data transmission and extends the network lifetime. Power conservation is an essential task in MANET. It needs fewer infrastructures and network communication. Supplementary, the variable communication link also enhances the possibility of packet drops and retransmission events. The utility factor of various packet forwarding policies will lead down and also influence the MANET performance like Energy and throughput. From a security perspective, the supporting packet forwarding policies need to be strong and adaptable enough to deal with every possible route transform while also maintaining the communication protocol pathways without complying with QoS and energy limitations. The built-in MANET features use a large number of mobile nodes overall, and limited flooding may significantly increase the cost of data transmission. Also, the Mobile nodes are employed as buyers and transform locations frequently, which may acquire recurrent data retrieval failures in the mobile nodes. Quality-of-service (QoS) routing must believe the diverse necessities along with the End-to-End consistency, Quality, Delay, and Energy efficiency constraints. There are several issues to be found in the MANET's data transmission. In order to increase QoS, energy-based random repetition trust computation in a delay-tolerant network is used in this work. The results of the simulation show how the routing protocol boosts node confidence. The proposed work makes a contribution by skillfully identifying the best and most suitable path for messages to take in order to reach the target node. For the trusted node classification, an approach of authentic node prediction via energy-based random repetition trust computation is adopted. The suggested approach is preferable because it offers greater QoS and increased routing performance while tolerating network system delays. The following list outlines the paper's overall structure: The relevant works about data transmission in MANET are presented in Section 2 from various authors' perspectives. A thorough explanation of the suggested methodology and how it functions is given in Section 3. In a comparable fashion, Section 4 describes the performance analysis of the proposed work with the current methodologies. The paper is concluded in Section 5 with a strong description.

2 Related Works

The Ad-hoc Routing (T2AR) proposed trust-aware protocol evaluated trust levels between MANET nodes and enabled safe data transfer between nodes. Based on energy, mobility, and received

signal strength indicator (RSSI) distance assessment, it forecasts a trust value. This Protocol offers nearby information about packet transmission performance and failure rates [1]. The confidence-based architecture is combined with a discovery method for attack models and the Adhoc On-Demand Distance Vectors (AODVs) Routing Protocol is expanded to lessen the capacity of adversaries to engage in various packets forwarding misbehavior [2]. For the Internet of Things (IoT)-MANET, a recently developed computational belief model has been assessed. The models are included in both main and indirect confidence judgments to calculate a node's ultimate trust score [3]. The Telecommunication Service Request (TSR), a contemporary trust-based unicast routing protocol for MANETs, provides a realistic and adaptable way to choose the shortest routing path for packet transfer [4]. In DTN situations, a protocol has been proposed for the security of the dynamic trust of well-balanced, self-centered, and malicious nodes. Planning and validation have gone into our new model-based strategy for evaluating and simulating our belief procedure. We will also employ a complicated trust management strategy in response to the constantly changing network conditions in order to minimize confidence, increase the functionality of routing hardware, and assess and enforce the ideal operating configuration in real time [5]. It advises using the revised Protocol. In addition to increasing communication integrity and reducing packet loss, the enhanced Protocol would also increase knots' service life [6]. The multi-objective fractional search method in a cluster head for an energy-efficient protocol is suggested in this paper. To maximize the node length, a fractional gravitational search algorithm (FGSA) is provided with an iterative IoT network architecture. The FGSA (MOFGSA), which determines the cluster head node for health care, uses a variety of metrics to determine its selection, including size, duration, longevity, and capital [7]. This article aims to talk about fundamental issues with cloud sensors, energy storage, data security, and the preservation of applications that are later improved by service quality (QoS). A secure Energy Efficiency Framework (SEEF) has been developed for efficient data transmission and maintenance. It includes a crosscutting for power and traffic management, a safety node and route investigation, and integrated dynamic routing to improve QoS using a fluid pollination algorithm. An intelligent service cycle planning protocol aims to maximize network performance by preventing data synchronization, trading conflicts, traffic disputes, and the removal of network resources [8]. In order to reduce energy consumption under cluster-headed nodes throughout the system, the Improving Low-energy Adaptive Clustering Hierarchy (LEACH) protocol, a cluster routing strategy, is proposed here [9]. A dependent method on Ant Colony Optimization (ACO) was anticipated for this issue. In order to speed up routing discovery and relieve network congestion, the terminal intersection concept was also proposed. Additionally, Local QoS Models (LQM) for assessing the entire and real QoS of urban route segments was introduced in order to reduce network overhead. The simulation's outcomes validate the LQM-derived models and demonstrate the usefulness of the AQRV [10]. A unique Cognitive Radio Ad Hoc Network (CRAHN) routing system that depends on multipath routing for QoS protocol and is generally known as route stability (SMQRP). The proposed protocol identifies the most advantageous primary and additional paths among the SU source, an SU destination that in turn ensures the best primary use with additional channels and paths. In the suggested technique, a stated metric of routing was used to support channel and path decisions [11]. The main goal has been to develop an optimal path mechanism to lessen the possibility of connection failures and cut down on network node energy consumption. The improved optimum course, along which the nodes were in the cluster shape, was the goal of the method proposed for this article. Under the Location Aided Routing (LAR) protocol, the Mobility Prediction technique was employed to maintain network stability and the two-tier system to reduce energy usage [12]. An attempt was made to provide information on the security and routing protocol aspects of the wireless ad hoc network technology. Multiple MANET attacks have also described various routing protocol security measures [13]. A brand-new, in-depth

investigation of trust was conducted on the massive Wireless Sensor Network (WSN), which uses clustering to foster cooperation, security, and reliability [14]. The energy and transit-conscious sleep-galactic (ETASA) system is a proposed hybrid technique for enhancing energy efficiency and load balancing in the heterogeneous network sensor situation. Contrary to earlier systems, in ETA SA connected nodes alternate between the sleep and alarm phases according to the node's energy and traffic volume. Additionally, we looked at the SEED conventional Time Division Multiple Access (TDMA) schedules to assign one slot to each pair in a series. This is meant to manage problems with passive listening so that tension is decreased [15]. A new cluster being formed In IoT-based WSNs, the FBCFP routing protocol has been suggested for neuro-fuzzy-based regulation [16]. This research proposes a novel and efficient clustering of Service Networks (SN) based on Eigen Values (EV) and Spectral Graph Theory. The spectral clustering theory in this article makes use of the Laplacian matrix. The autonomous values of the Laplacian matrix and its associated function are used for the grouping of the WSN nodes, and CH is selected using smooth reasoning, energy and distance limitations. A comparison between this study's appraisal of the outcomes and LEACH and Hybrid, Energy-Efficient, Distributed (HEED) is made [17]. To enable a range of applications, examine energy-intensive algorithms and network performance on WSN. One of the hierarchical protocols for routing between SN and sinks is clustering, which uses a Cluster Head (CH). Several algorithms are available to select the best Communications House (CH) and localize cluster memberships with fuzzy logic classification parameters to prevent regular clusters from consuming too much energy. We have also used the neural network learn [18]. Presents a scenario energy model and suggests using TEAR, or traffic and energy-sensitive routing, to support stability [19]. Here is a brand-new, energy-efficient solution. The Fuzzy Logic Cluster Formation Protocol (FLCFP) protocol is largely what drives this emphasis on the cluster creation process. A comparison between the suggested model and the well-liked hierarchical clustering approach to low-energy adaptation is made. Test findings demonstrate that the new protocol has increased Network Life [20,21]. It was suggested to use fuzzy cluster head choice logic. The proposed approach assesses each node's likelihood of becoming a CH using five criteria [22]. It is suggested to use a novel Fuzzy Logic-based Greedy Routing (FLGR). For the assessment of the following forwarding node, there are also suggested selection criteria and requirements. The FLGR protocol allows the target node's fuzzy position to be used to select the subsequent forward node [23]. The system predicts a benefit reliant on the matrix to maximize network security and dependability [24]. The Eigen Trust was used to design a non-cooperative game model that tracks a node's egoism when it doesn't provide MANET data packets [25]. To eliminate node emotions and directly diffuse messages in the relay node, a routing algorithm based on rewards is created using the Selfishness-Enhanced Effective Forwarding (SERF) theory. Through messages that the relief node receives, this method determines the most likely use of the sender node's resources. By adjusting the copy threshold for the source node resource consumption, the buffer control is maintained concurrently with message generation. The findings show that, in terms of performance indicators like the distribution ratio, the average time delay is larger than the already used techniques [26]. This study offers a revolutionary FANET routing system using a modified Ant Hoc Net. Ant colony optimization approaches, or metaheuristics, in general, have shown improved dependability and performance compared to other conventional optimal path selection algorithms [27]. The progress of wireless communication technology was thoroughly compared and evaluated for various parameter configurations in this research study [28]. The architecture, optimization techniques, mobility models, heuristic calculations, and routing protocols used in flying ad hoc networks were all explicitly covered in the introduction [29]. This study covered the issue of energy conservation for flying IoT. A unique DSDV routing scheme for the Internet of Flying Vehicles was presented in this study [30].

3 Problem Statement

Some of the challenges and issues faced in MANETs cause difficulties in the communication process. It is impossible to build methods that aid in communication among MANETs unless these difficulties are recognized and anticipated. Some of the most important things to think about when deploying MANETs are listed below. Nodes are subject to limitations such as limited processing power, battery life, and storage space. In the context of a scalable dynamic network, the overhead is a crucially difficult operation that is used to maintain topology. This ultimately has an impact on the network's Quality of Service (QoS).

4 Proposed Work

This section contains a thorough description of the suggested structure. The key to guaranteeing a secure data exchange with this network infrastructure is secure data communications. The technology suggested is, therefore, best for the security of records, privacy, and policy. The following is the general flow of the suggested system.

4.1 System Model

Initially, two general models were presented to suggest the transformation of information among mobile nodes. According to the reference region model of group mobility, it was believed that there were N mobile nodes travelling across a certain distance. The model's whole nodes have a transmission range that is equivalent. Each node has the ability to send information to its neighbors. Here, the channel and the user can both be initialized initially. Any data point has a field of interest. Maintaining data is necessary in this sector (some nodes in this region should be established). The source node sends information and specifics down to the area in question. It is possible to define the challenge of choosing the node as,

$$D_{cn} = \sum_{i=1}^{i=m-1} OP\,(S_i, S_{i+1})\,\frac{1}{m}.\,(m-1)\,C \tag{1}$$

where, S_i is the node for the data carrier, C is the channel, l is the number of data carrier nodes used by the entire time domain, and OP (S_i, S_{i+1}) is the network link between S_i and S_{i+1}. The data in the network is S, and the contact time between S_i and S_{i+1} is $P\,(S_i, S_{i+1})$. D here is the center of interest's distance from S to l. M is the node size. First, it is important to consider the delay between the present data carrier node and the nearby node as low-throwing connections that lengthen the duration for channel transmission.

4.2 Node Initialization

The initialization of the node is done first, then node deployment. Each network node is deployed by the network. Consideration was given to the situation in which there were two categories of non-cooperating users, known as SUs (Secondary Users) and Pus (Primary Users). The wireless spectrum quantity is being allowed for devices including portable units (PUs), mobile phones, wireless microphones, and televisions (TVs). The SUs, on the other hand, were those without pre-assigned wireless spectrum. On the other side, the SUs can broadcast their packet by taking advantage of the chance that presents itself when the PUs fails to use the authorized wireless spectrum. In this, the wireless spectrum that is available to the SUs has been further divided into a number of channels, each with a specific amount of frequency bandwidth. The energy-efficient reactive routing technology known as Electronic Communication-Data Subject Request (EC-DSR) establishes on-demand routes by providing less connection-phase delay. The nodes that were included in the dynamic communication

can choose the routes for a new destination with ease. Both multicast and unicast routing are approved. We select the shortest paths without loops. In the proposed EC-DSR protocol, the source node floods all of its neighbors with (RREQ) route request packets in order to reach the destination node. Seven fields make up RREQ, including the packet lifespan, request ID, source and destination addresses, and their serial numbers, which serve as a unique identification. The higher serial number of the node makes it easier to identify any new information coming from it. The source node continues this process until the destination node is located. If the neighbor node is the destination or in the condition that it knows the path for the destination, then the RREP packet is sent to the source node for acknowledgment.

4.3 Energy Model

The nodes in mobile ad hoc networks are battery-powered. We just consider energy consumption. In transmission, the overall energy consumption can be split into two parts: Energy generated and Energy absorbed, as seen in Eq. (2),

$$EN\,(k,n) = Energy_{consumption}\,(k) + Energy_{Transmission}(k,n) \tag{2}$$

where, *EN(k, n)* is the cumulative transmission power for n-bit data transmission over distance. k, n distance Means energy usage to transfer data n bit. A model would be used based on the distance between the source node and the target node.

$$EN\,(n) = E_t\,(k) = n^* \tag{3}$$

where, $EN\,(n)$ represents the consumed Energy for transmission, $E_t\,(k)$ represents the Energy needed for transmission, $n^*\ T_n$ represents the time needed.

$$\text{Remaining energy} = \text{Available energy} - \text{Consumer energy} \tag{4}$$

Prediction of the channel availability:

The residual power between each node and its bandwidth size can be calculated in this regard. Mobile network scheduling is one of the most important concerns. The mobile node is always monitoring the bandwidth. Any mobile node can control the channel during idle times in shared wireless media. If $T_{idle}\ (S)$ is the total idle periods during measurement time Ts of node s, then B_s, the available bandwidth of node s could be easily calculated as

$$B_s = (T_{idle}\,(S)\,/T_S)\ * \text{Channel capacity} \tag{5}$$

The Mobile Node will also track neighboring packets and gather information relating to bandwidth, such as packet size, explosives, etc. The Mobile Node could measure the bandwidth available for itself using this information:

$$\text{Local available bandwidth} = \text{Channel capacity} - \text{Sum (All neighbor throughputs)} \tag{6}$$

The MANET node may use this information internally or may share it with other nodes, as shown in Fig. 1. It determines when and how quickly data is transmitted. It is advised to track the entire communication network numerous times per second in order to evaluate the communication environment. The complete contact network should be tracked once, and in some situations, in a single second, in order to evaluate the communication structure. The history of proper channel utilization may be provided by the ongoing monitoring of spectrum contact. If the relevant use history is provided, prognostic methods may be used to select the current channel. Secondary users are those who opportunistically use the bandwidth for interaction. Owners who had received a frequency band license were the first users. Once the key user exits and enters the secondary user's channel, the secondary user

must leave the so-called termination channel. Thus, the secondary recipient is compelled to utilize several open platforms. Additionally, this form of modification may cause contact disruptions. This issue can be solved using the secondary user's ability to foresee when the primary user channel will be open. The secondary user number has been provided as a result of the channel's availability for secondary users, and it varies according to the volume of basic user traffic.

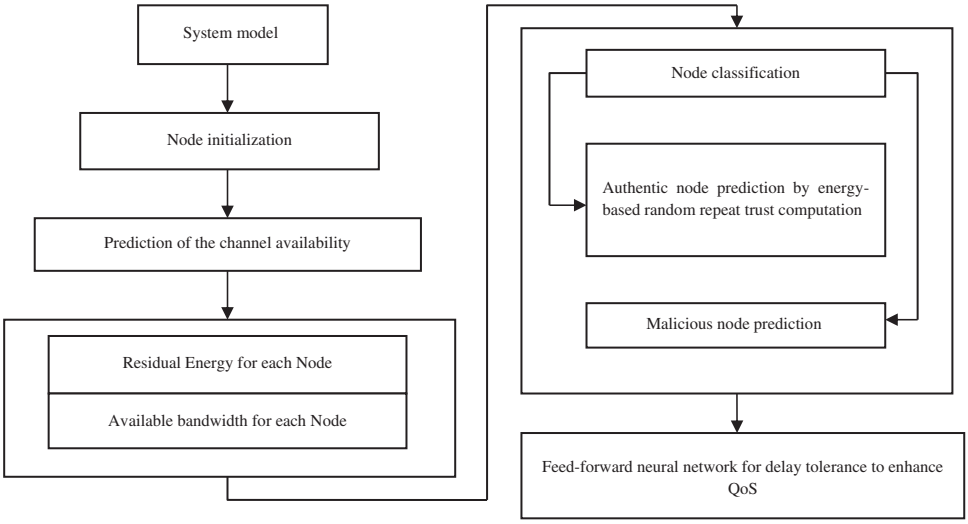

Figure 1: Schematic representation of the suggested methodology

4.4 Energy-Based Random Repeat Trust Computation

Finding the reliable neighbor node made it possible to use the entire strategy. Both the hop-based pause and the data transmission packets were impacted. The time varies depending on how many hops there are between the source and the destination. The delay at the packet's end is inversely proportional to the path length. The end-to-end packet delay will likewise rise as the route length does. The routing period and packet delay are over if there is a significant binding between them. The weighted distance and the shortest path measurement from each node's source are calculated in the suggested approach to trust end-to-end delay. The true, close-proximity nearest node is thin and trustworthy. Packets are sent directly to the destination node after node information. Time is saved, and energy is conserved as a result. This particular node sends the message to the network on a regular basis. As messages arrive, each node updates its local tables. The target node periodically modifies the table of its near neighbors in accordance with the messages it receives from its neighbors. Similar data was used to describe the relationship between neighboring nodes and their estimated bandwidth. Once the shortest traffic path has been found, the data shall pass directly from the source node to the destination node.

$$Trust_{(neighbor)} = Energy_{(node)} + Trust_{(neighbor)} \tag{7}$$

where,

$$Energy_{(node)} = \frac{\sum(PR + PF)}{Node_{iton}} \tag{8}$$

Here, PR and PF represent the packet received and the packet forwarded, respectively.

The flow chart of trusted node computation is shown in Fig. 2

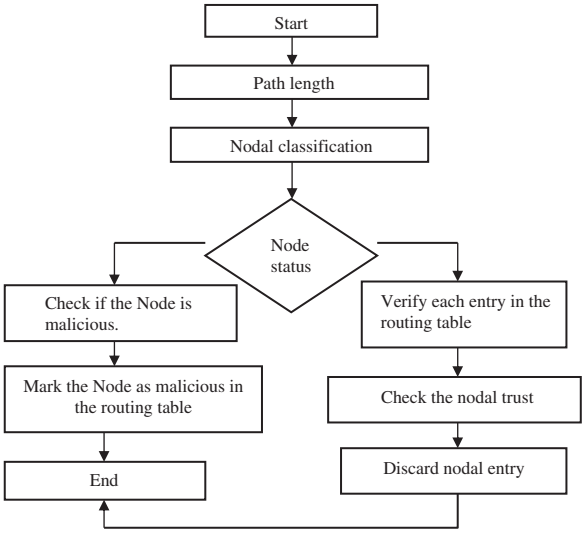

Figure 2: Flow chart of trust node computation

For calculating the trusted classified value, the distance is to be calculated.

$$Distance\,(i,j) = \sqrt{\left(W_{n_{fea}}\,(i,1) - W_{n_{fea}}\,(i,1)\right) + \left(W_{n_{fea}}\,(i,1) - W_{n_{fea}}\,(i,1)\right)^2} \tag{9}$$

The prototypes were trained on typical node behavior and its attributes. As a result, the proposed repeat trust mechanism can assess the nodes' attributes and distinguish between the legitimate nodes and malicious nodes. The malicious node's anomalous value was then determined.

$$A_{Mv} = (W_{n_{fea}} dist) \tag{10}$$

where, A_{Mv} represents the abnormal malicious value of the Mobile Node. The trusted value determines which node is an authentic one. The total value of the nearest trust is calculated based on the following equation:

$$Neighbor_T = W_1 CFR + W_2 DFR + W_3 Residual_{Energy} + W_4 Channel_{Quality} \tag{11}$$

CFR represents the forwarding ratio of the control packet, and DFR represents the transmission ratio of the data packet. In Eq. (11), CFR illustrates the number of packets sent from the source node to the destination node in the network, and DFR illustrates the number of received packets by the receiver to the number of packets sent by the source.

4.5 Feed-Forward Neural Network for Delay Tolerance to Enhance QoS

The Node, the neighbor, or the third party measures confidence. A node is calculating its own service-based Trust Score. There are several perceptrons in the multi-layer perceptron (MLP). It should be structured multi-layer experiences known as the layers. Fig. 3 The following input layer, a number (Possibly zero), and the output layer is in this FFNN. The following layers for this FFNN are. In the diagram, the input layer is layer 0, layer 1 is hidden, layer 2 is open, and input layer 2 is secret.

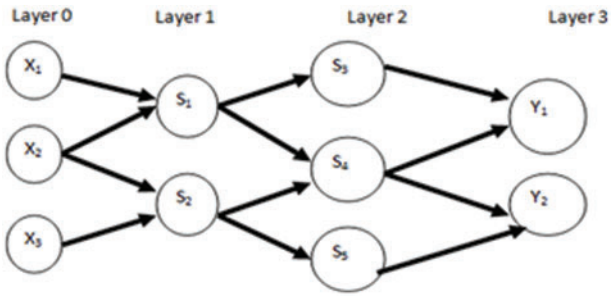

Figure 3: Feed-forward artificial neural network architecture

After selecting the trusted nodal value, the trusted route can be established. The weights W1, W2, W3, and W4 are those where 0Wn1. n = 1, 2, 3, 4, etc. Only the observed method was used to define the weight values. By implementing MANET and QoS constraints, they are simultaneously compressed for the goal of a high-priority customer. The significance of confidence, meanwhile, changes over time in accordance with the actions of nearby nodes. The confidence threshold then distinguished the beneficial path from the harmful path. The threshold (0.4) may be determined for malevolent roads. There are any connectivity failures or instances of malicious nodes that exceed the aforementioned threshold value when weighed against the reliable value discovered. The QoS trust transmits trustworthy information or messages to the intended recipient as the most likely Contact Network Node. The energy nodes will then decide on the QoS confidence level. The QoS Confidence energy level is then determined using the simple routing technique and preprocessing. Data will be provided over the journey once the optimum route has been chosen. Along the cluster path to the sink node, the transferred data is gathered in CH. Data from the sink node can be recovered using the provided method. This facilitates the detection of data capture and recovery. The fundamental goal of matrix filling is to collect all of the data using a minimal amount of packages that are processed as rapidly as feasible to minimize energy usage. The principle of the Feed-forward neural network shows,

$$(F\hat{}2) = x_{ij} = M_{ij}(ij)\varepsilon\varphi \tag{12}$$

where, F represents the Feed forward neural network, x represents the rank of the matrix, φ represents a set of known elements, and M_{ij} represents the sum of known elements. ε represents the summation.

4.5.1 Reduce Energy Consumption

Packet delivery is the key explanation for energy use. Primarily data transfer use and optimization of resources can be accomplished by

$$\min(E) = \min\left(E^T - E^i\right) \tag{13}$$

where, E^T represents the energy transfer and E^i represents the energy loss.

4.5.2 Reduce the Delay

The period when a node completes data collection is known as a delay here. Two factors decide mainly the pause in node A. Then, the packets are stored in a cluster. The timing and length of the packet that other CH nodes send to A are accompanied by,

To reduce the delay,

$$Min(D) = min(D_{CM}, D_{SN}) + \min(D_i) \tag{14}$$

where D_{CM} represents the delay of a cluster member, D_{SN} represents the delay of a sink node, and D_i represents the delay reduction. That is, the data processing in the cluster is finished as soon as feasible, and the inter-cluster transmission is accomplished.

Algorithm 1: Random repeat trust feed-forward neural network

Input: Node features $W_{n_{fea}}$, Node_coordinate W_c
Output: classified trust node and route dc_v To compute trust value,
For i = 1: size ($W_{n_{fea}}$, 1)
For j = 1: size ($W_{n_{fea}}$, 1)
$Distance\,(i,j) = \sqrt{\left(W_{n_{fea}}\,(i,1) - W_{n_{fea}}\,(i,1)\right) + \left(W_{n_{fea}}\,(i,1) - W_{n_{fea}}\,(i,1)\right)^2}$ End
End
Node features
To compute, trust value $A_{Mv} = (W_{n_{fea}} dist)$
Class label = unique (target)
K = length (class label)
For i = 1: k
Temp= total class mean (I :)
W (i, j) = −0.5 ∗ Delay∗ total class mean + log (i) (a delay of 0.5 ms can be produced)
W (I, 2: end) = delay
End

5 Performance Analysis

This section deals with the deliberation of the mechanism's performance analysis. In this section, some of the novel methodologies used in work in existing work are briefly introduced. The experimental analysis was simulated using ONE simulator.

5.1 Packet Delivery Ratio to BS

Collectively, this refers to the number of packets that are transferable by the sender and received by the recipient at the base station.

$$P = (P_r/P_s) * 100 \tag{15}$$

P is the transmission ratio of the packet, Pr is the sum of packets obtained, and Ps is the volume of packets forwarded.

5.2 Average End-To-End Delay

That's the length of the transmission process, regardless of the amount of time it takes to transmit the signals.

$$AD = (P_s - P_r)/P_r \tag{16}$$

Here Ps is the time taken to the sent packet, and Pr is the overall time consumed.

Fig. 4 above indicates a better example of the suggested mechanism proposed. The suggested procedure will increase communication above existing practices while also increasing BS efficiency. This procedure extends the suggested method's network life.

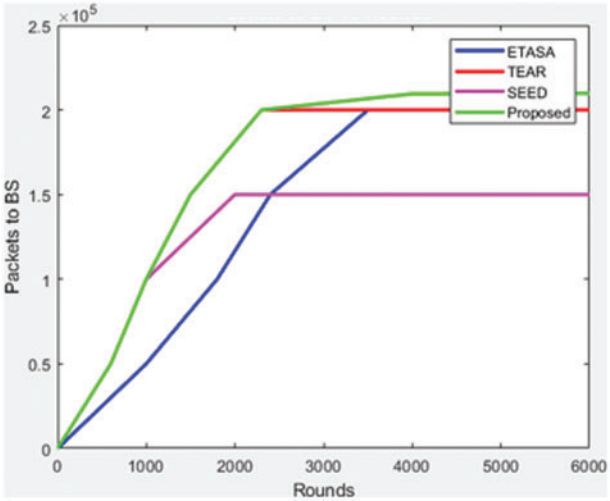

Figure 4: Rounds *vs*. Packets to the base station (BS)

The analysis of network life for different node numbers is seen in Fig. 5. This is due to the development of the cluster. The remaining capacity, distance, and present cluster scale are incorporated into each Node in our proposed research. It enables load balancing throughout the CH device, extending the network's lifespan by preventing the loss of the first node.

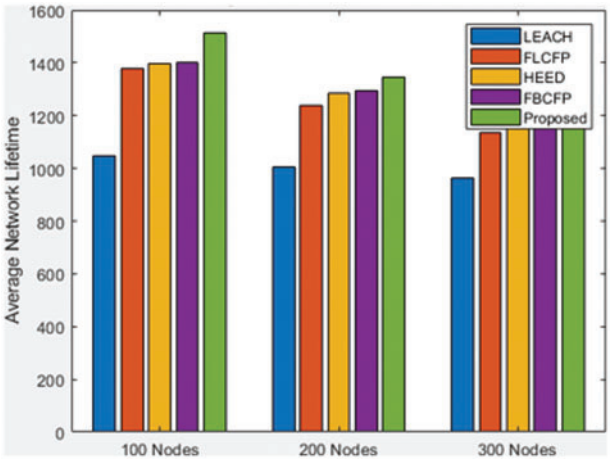

Figure 5: Nodes *vs*. Average network lifetime

The research demonstrates that the proposed method has a lower rate of delay than the existing mechanism, as shown in Fig. 6.

Fig. 7 demonstrates that there are far less dead nodes in the implemented approach than there are in the existing methodologies, indicating that the number of dead nodes in the latter methodology appears to be excessive.

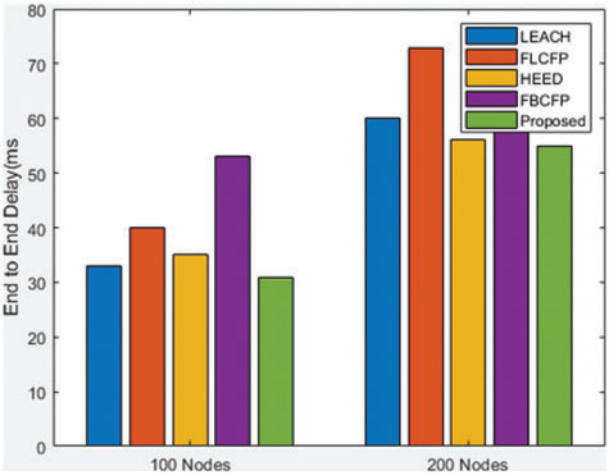

Figure 6: Nodes *vs*. End-to-end delay

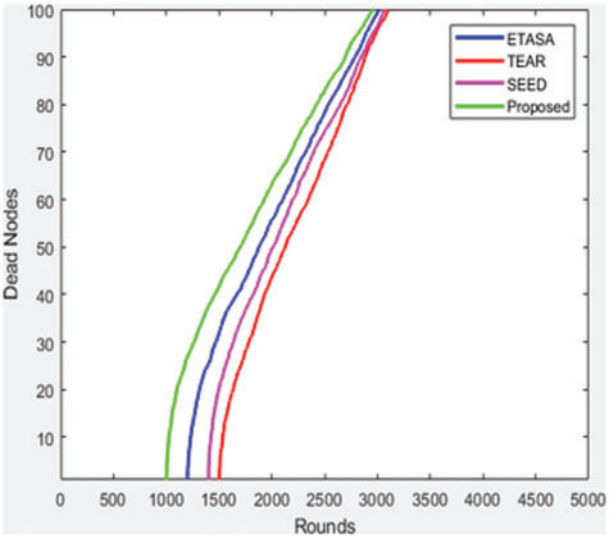

Figure 7: Rounds *vs*. Dead nodes

As seen in Fig. 8, the number of live nodes could increase the network's existence using the proposed technique. Compared to the approach suggested, SEED, TEAR, and ETASA have had less network life.

The results of current approaches are, however, insufficient and less efficient. According to the proposed simulated performance, data transfer in MANET is effective, has steady connectivity, and increases network life with improved QoS.

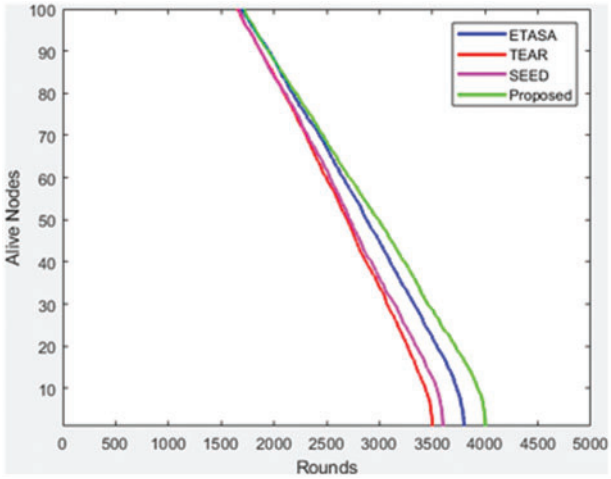

Figure 8: Rounds *vs*. Alive nodes

6 Conclusions

This method presents a computation for energy-based random repeat trust utilizing a feed-forward neural network (FFNN) in a DTN. The experimental analysis was simulated using the ONE simulator. The presented method demonstrates that it will improve BS efficiency and communication over current techniques. Through this methodology, the suggested method is enhanced to have a longer network life. The research of network longevity for various node counts is shown in Fig. 5. This is as a result of the cluster's development. The remaining capacity, distance, and current cluster scale are all taken into account by each node in our proposed research. It allows load balancing throughout the CH device, which really helps to increase the network's lifespan by preventing the death of the initial node. According to the research, the suggested method, as seen in Fig. 6, has a lower rate of delay than the existing system. Fig. 7 shows that there are substantially fewer dead nodes in the implemented approach than there are in the existing methodologies, indicating that there are a lot of dead nodes in the current methodology. The suggested method might increase the number of active nodes, as depicted in Fig. 8, which would strengthen the network's viability. When compared to the suggested technique, SEED, TEAR, and ETASA have a shorter network life. However, the results of the current tactics are inadequate and less efficient. Data transfer in MANET is efficient, reliable connectivity has extended network life, and QoS has improved based on the suggested simulated performance. In comparison to other existing techniques, simulation results show that this process makes the best decision and expertly determines the best and most appropriate route to send messages to the destination node, which improves routing performance, increases the number of delivered messages, and decreases delivery delay. As a result, the suggested method is better at providing improved QoS while tolerating network system delays. By employing an effective technique to apply the paradigm in the real-time setting while still meeting privacy and security criteria, this study may be developed in the future.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] G. Dhananjayan and J. Subbiah, "T2AR: Trust-aware ad-hoc routing protocol for MANET," *Springer Plus*, vol. 5, no. 1, pp. 995, 2016.

[2] R. Kumar and S. Shekhar, "Trust-based fuzzy bat optimization algorithm for attack detection in manet," In: *Smart Innovations in Communication and Computational Sciences*, vol. 1164. Springer, pp. 3–12, 2016.

[3] S. Sharma and A. J. V. C. Kaul, "A survey on intrusion detection systems and honeypot based proactive security mechanisms in VANETs and VANET Cloud," *Vehicular Communications*, vol. 12, pp. 138–164, 2018.

[4] A. Rajeswari, K. Kulothungan, S. Ganapathy and A. J. P. N. Kannan, "A trusted fuzzy based stable and secure routing algorithm for effective communication in mobile adhoc networks," *Peer-to-Peer Networking and Applications*, vol. 12, no. 5, pp. 1076–1096, 2019.

[5] I. R. Chen, "Hierarchical trust management of COI in heterogeneous mobile networks," *Virginia Polytechnic Institute and State University Blacksburg United States*, vol. 19, 2017. https://apps.dtic.mil/sti/citations/AD1050668

[6] F. Ullah and S. Babar, "Architectural tactics for big data cybersecurity analytics systems: A review," *Journal of Systems and Software*, vol. 151, no. 1, pp. 81–118, 2019.

[7] A. V. Dhumane and R. S. Prasad, "Multi-objective fractional gravitational search algorithm for energy efficient routing in IoT," *Wireless networks*, vol. 25, no. 1, pp. 399–413, 2019.

[8] S. Subashini and P. Mathiyalagan, "A cross layer design and flower pollination optimization algorithm for secured energy efficient framework in wireless sensor network," *Wireless Personal Communications*, vol. 112, no. 3, pp. 1601–1628, 2020.

[9] A. O. A. Salem and N. Shudifat, "Enhanced LEACH protocol for increasing a lifetime of WSNs," *Personal and Ubiquitous Computing*, vol. 23, no. 5–6, pp. 901–907, 2019.

[10] G. Li, L. Boukhatem and J. Wu, "Adaptive quality-of-service-based routing for vehicular ad hoc networks with ant colony optimization," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 4, pp. 3249–3264, 2016.

[11] S. AlQahtani and A. Alotaibi, "A route stability-based multipath QoS routing protocol in cognitive radio ad hoc networks," *Wireless Networks*, vol. 25, no. 5, pp. 2931–2951, 2019.

[12] U. Agballa, A. Obiniyi and B. Ayeni, "Design of an improved energy efficient routing protocol in VANET using a modified route-optimal path algorithm," *International Journal of Applied Information Systems*, vol. 12, no. 18, pp. 1–4, 2019.

[13] K. Abhilash and K. Shivaprakasha, "Secure routing protocol for MANET: A survey," In: *Advances in Communication, Signal Processing, VLSI, and Embedded Systems*. Springer, pp. 263–277, 2020.

[14] T. Khan, K. Singh, M. Abdel Basset, H. V. Long and S. P. Singh, "A novel and comprehensive trust estimation clustering based approach for large scale wireless sensor networks," *IEEE Access*, vol. 7, pp. 58221–58240, 2019.

[15] N. M. Shagari, M. Y. I. Idris, R. B. Salleh, I. Ahmedy and G. Murtaza, "Heterogeneous energy and traffic aware sleep-awake cluster-based routing protocol for wireless sensor network," *IEEE Access*, vol. 8, pp. 12232–12252, 2020.

[16] K. Thangaramya, K. Kulothungan, R. Logambigai, M. Selvi and S. Ganapathy, "Energy aware cluster and neuro-fuzzy based routing algorithm for wireless sensor networks in IoT," *Computer Networks*, vol. 151, no. 12, pp. 211–223, 2019.

[17] S. Lata, S. Mehfuz, S. Urooj and F. Alrowais, "Fuzzy clustering algorithm for enhancing reliability and network lifetime of wireless sensor networks," *IEEE Access*, vol. 8, pp. 66013–66024, 2020.

[18] M. Ali and F. Gared, "Energy optimization of wireless sensor network using neuro-fuzzy algorithms," *Ethiopian Journal of Science and Technology*, vol. 12, no. 2, pp. 167–183, 2019.

[19] D. Sharma and A. P. Bhondekar, "Traffic and energy aware routing for heterogeneous wireless sensor networks," *IEEE Communications Letters*, vol. 22, no. 8, pp. 1608–1611, 2018.

[20] M. Toloueiashtian and H. Motameni, "A new clustering approach in wireless sensor networks using fuzzy system," *The Journal of Supercomputing*, vol. 74, no. 2, pp. 717–737, 2018.

[21] P. Srinivasan, "Fuzzy sets based cluster routing protocol for internet of things," *International Journal of Fuzzy System Applications*, vol. 8, pp. 70–93, 2019.

[22] A. Hamzah, M. Shurman, O. Jarrah and E. Taqieddin, "Energy-efficient fuzzy-logic-based clustering technique for hierarchical routing protocols in wireless sensor networks," *Sensors*, vol. 19, no. 3, pp. 561, 2019.

[23] X. Hu, L. Ma, Y. Ding, J. Xu, Y. Li *et al.,* "Fuzzy logic-based geographic routing protocol for dynamic wireless sensor networks," *Sensors*, vol. 19, no. 1, pp. 196, 2019.

[24] J. Sengathir and R. Manoharan, "Exponential reliability coefficient based reputation mechanism for isolating selfish nodes in MANETs," *Egyptian Informatics Journal*, vol. 16, no. 2, pp. 231–241, 2015.

[25] S. Subbaraj and P. Savarimuthu, "Eigen Trust-based non-cooperative game model assisting ACO look-ahead secure routing against selfishness," *EURASIP Journal on Wireless Communications and Networking*, vol. 2014, no. 1, pp. 78, 2014.

[26] S. Dheenathayalan and B. Paramasivan, "A comprehensive approach to avoid node selfishness and data redundancy," *Journal of Intelligent & Fuzzy Systems*, vol. 39, no. 1, pp. 407–419, 2020.

[27] I. U. Khan, I. M. Qureshi, M. A. Aziz, T. A. Cheema and S. B. H. Shah, "Smart IoT control-based nature inspired energy efficient routing protocol for flying ad hoc network (FANET)," *IEEE Access*, vol. 8, pp. 56371–56378, 2020.

[28] I. U. Khan, S. Z. N. Zukhraf, A. Abdollahi, S. A. Imran, I. M. Qureshi *et al.,* "Reinforce based optimization in wireless communication technologies and routing techniques using internet of flying vehicles," in *Proc. of Int. Conf. on Future Networks and Distributed Systems (ICFNDS)*, New York, NY, USA, pp. 1–6, 2020.

[29] I. U. Khan, A. Jamin, A. Abdollahi, B. Baig, F. Subhan *et al.,* "A novel design of FANET routing protocol aided 5G communication using IoT," *5G and A Vision of 6G*, vol. 18, no. 5, pp. 1333–1354, 2022.

[30] I. U. Khan, M. A. Hassan, M. Fayaz, J. Gwak and M. A. Aziz, "Improved sequencing heuristic DSDV protocol using nomadic mobility model for FANETs," *Computers, Materials & Continua*, vol. 70, no. 2, pp. 3653–3666, 2022.