Computer Science • 26(1) 2025 https://doi.org/10.7494/csci.2025.26.1.5135

Veeramani R.
R. MadhanMohan
C. Mahesh

ENERGY EFFICIENT AND QoS AWARE TRUSTWORTHY ROUTING PROTOCOL FOR MANET USING HYBRID OPTIMIZATION ALGORITHMS

Abstract *The security challenges in MANETs are particularly difficult to address. To assess the reliability of each mobile node, factors such as location, mobility speed, energy usage, transmission count, and neighbor list are considered. This research proposes the Intelligent Dynamic Trust (IDT) paradigm to enhance security in wireless networks. For secure routing, IDT combines beta reputation trust with dynamic trust. Performance analysis was conducted using Network Simulator 3.36, with metrics such as throughput, energy consumption, packet delivery ratio, jitter, end-to-end delay, packet loss rate, detection rate, and routing overhead. The results show that the proposed approach outperforms existing methods.*

Keywords MANET, levy flight centred shuffled shepherd dynamic source routing, firefly, whale optimization, energy consumption, secure routing, network simulator

Citation Computer Science 26(1) 2025: 101–131

1. Introduction

The usage of mobile computing has seen an enormous increase in popularity over the years due to the development of new technologies and the desire for flexibility and simplicity in the workplace. A dynamic multi-hop wireless ad hoc communication network called a mobile ad hoc network (MANET) enables people and objects to easily connect without the need for any pre-existing infrastructure. Finding a route between the communication endpoints is the main issue in this type of network, which is made more difficult by node mobility, resource limitations, and channel access competition [9, 40]. To connect nodes that are unable to interact with one another directly, a routing protocol would be crucial in MANET. Quality of Service (QoS) indicators should be accessible in MANETs to provide prompt and reliable transmission of information and multimedia material. The absence of central administration, internal errors, and outside interferences all contributed to the difficulties in ensuring QoS. Connection breakdowns, high traffic rates, battery failures, process failures, and packet retransmissions are examples of internal problems [16]. A QoS-assured Mobility-Aware Routing (QMAR AODV) protocol based on AODV was proposed in [26]. It is essential to present an effective routing protocol in MANTs and demands an ideal QoS mechanism. There have been several types of research on routing optimization and communication models in MANETs, most of which undervalue the importance of mobility and its impact on QoS. In connection failures that result in packet loss and subsequent data retransmissions, node mobility is a crucial factor. In addition, route failures result in error packets, take additional time for network convergence, and need a new route discovery procedure if no alternative viable pathways exist. As a result, there is a corresponding increase in delivery latency and a corresponding decline in data quality [38].

Energy-efficient routing protocol

With new series of developing technologies, solutions have recently been offered in intelligent transportation systems, smart agriculture, retail utilities, and intelligent cities, to serve mankind. These solutions incorporate IoT networks, MANET, and other emerging technologies. These appliances will use a significant quantity of electricity. Saving energy is thus very important for MANET-IoT networks. Due to frequent changes in network architecture and the constrained energy resources of network nodes, route stability and mobile node energy capacity are the two most difficult problems in MANETs. Due to network congestion brought on by excessive duplicated traffic and connection failures, routing systems perform worse and use more energy. As a result, many strategies are being examined to address the problems caused by node mobility and energy failures in MANETs. To resolve these problems, a new routing algorithm of ant colony optimization (ACO) with ad hoc on-demand vector (AODV) [1] and MANET routing protocol [23] is proposed. Therefore, in the highly dynamic MANET environment, developing a plan that promotes energy efficiency is essential. Based on effective route failure detection [13], recommends the Energy Effi-

cient Routing (EER) protocol. A new routing method was proposed to reduce failed communication in MANET. To maintain the least energy-consuming routes, a genetic algorithm-based AOMDV routing protocol is suggested in [30]. To extend the lifespan of the network and improve system performance, a delay-based energy-saving routing protocol for MANETs is presented in [39].

Data security in MANET

In the lack of infrastructure, mobile nodes wander within or outside the network. Security attacks including the grey-hole attack, Sybil attack, black-hole attack, jamming assault, and rushed attack might affect MANET. The effectiveness of the entire network is decreased by these attacks. Packets are lost or the link connection breaks when many assaults take place on the route. It results in less security and more power usage. A Hybrid Secure Aware Routing Protocol (HSARP) was presented to satisfy the QoS criteria. It encourages the proper distribution of power and security [21]. A novel GEO-TAODV routing protocol is utilized in MANETs [15] for data transmission. This method employs the GEO approach, a multiple-objective Meta heuristic optimization technique. Therefore, the protocol offers a stable and trustworthy method for data transfer in addition to an efficient one. In [11], the ANFIS idea with the Group Teaching Optimization Algorithm (GTA) is suggested for the evaluation of the neighbour's trust value for the trust-aware routing protocol. The mobility of nodes makes it challenging to maintain the proper QoS in the network due to frequent connection failures and high error rates. BAT optimization [27] and the improved animal migration optimization (IAMO) algorithm [18] were also used to increase the quality of service during data transmission to protect the MANET network.

Existing methods cannot be transferred to MANETS without being modified to carry out these protocols in various circumstances due to the basic differences between MANETS and wired networks. To ensure QoS in MANET, some new challenges specific to MANETS must be overcome, including node mobility, a lack of infrastructure, a lack of a centralised authority, multiple node functionality, energy limitations, erroneous link-state information, and constrained bandwidth. To create the route in various scenarios, there was intense cooperation between nodes. Routing optimization is a widely used technique to decrease the distance of data transmission and enhance the quality of service (QoS) of MANET applications. The data transmission channel from the source node to the destination node is referred to as routing. The most effective routing is a crucial problem in MANET since there are typically numerous options for the routing method. The clustering process, which causes the nodes to consume the least amount of energy for data connection, is one of the strategies that have been proposed for obtaining the best design. A trade-based strategy is required to solve the challenge of energy efficiency, either by compromising on energy use or other QoS metrics like delay, rate of transmission, or distance. Minimising the trade-offs as the network's population grows requires an optimised approach. Here, a hybrid strategy is set forth for energy optimization with little loss of other QoS factors. There is a significant chance that a packet will get dropped during communication, which

can cause many security problems like confidentiality and privacy loss. The nodes might trick other nodes by sending misleading signals. As a result, the idea of trust management is born, which refers to building node reliability (i.e., trust). Devices are created with little computational and processing power due to the constrained power supply they operate on, consuming less energy. They are not required to adhere to all the security protocols for a strong secure network due to the limited power supply. Therefore, by selecting the optimum route for routing information, this problem can be solved. The DSR-optimized LF-SSO algorithm is employed in the study for the energy-efficient trust-based routing protocol.

2. Literature survey

The performance of QoS for users is directly impacted by the frequent changes in network architecture that the mobility of nodes in MANETs produces. To develop effective routing optimization techniques for a variety of traffic flows, network operators are essential. Khan et al. [20] proposed an algorithm that increases the reliable delivery of critical BAN data at the destination. We have performed extensive simulations in the OMNeT++-based simulator Castalia 3.2 to demonstrate the better performance of the proposed QoS-based routing protocol for reliability sensitive data in terms of lower network routing traffic (Hello packets) overhead, fewer reliability packets dropped, lower end-to-end delay (latency), fewer packets dropped due to media access control (MAC) buffer overflow and higher throughput in both stationary and movable patient scenarios. The scalability of the protocol is demonstrated by using two cases that simulate a 24-bed and a 46 beds real hospital environment with 49 and 93 nodes, respectively. El Dien et al. [6] proposed an energy-efficient and QoS-aware framework for transmitting multimedia content over WSN (EQWSN) is presented, where packet, queue and path schedules were introduced. It adapts the application layer parameter of the video encoder to the current wireless channel state and drops less important packets in case of network congestion according to the packet type. Finally, the path scheduling differentiates packet types/priorities and routes them through different paths with different QoS considering network lifetime. Simulation results show that the new scheme EQWSN transmits video quality with QoS guarantees in addition to prolonging network lifetime.

Muhammad Amjad et al. [2] proposed an energy-efficient routing protocol for heterogeneous WSNs to support delay-sensitive, bandwidth-hungry, time-critical, and QoS-aware applications. The proposed QoS-aware and heterogeneously clustered routing (QHCR) protocol not only conserves the energy in the network but also provides dedicated paths for real-time and delay-sensitive applications. The inclusion of different energy levels for the heterogeneous WSNs also provides the stability in the networks while minimizing the delay for the delay-sensitive applications. Extensive simulations have been performed to validate the effectiveness of our proposed scheme. The proposed routing scheme outperforms other state-of-the-art schemes in terms of delay performance. Faheem et al. [7] proposed the dynamic clustering-based

energy efficient and quality-of-service (QoS)-aware routing protocol (called EQRP), which is inspired by the real behaviour of the birds mating optimization (BMO), has been proposed. The proposed distributed scheme improves network reliability significantly and reduces excessive packet retransmissions for WSN-based SG applications. Performance results show that the proposed protocol has successfully reduced the end-to-end delay and has improved packet delivery ratio, memory utilization, residual energy, and throughput.

Manisha Rathee et al. [35] proposed an ant colony optimization-based QoS aware energy balancing secure routing (QEBSR) algorithm for WSNs is proposed in this article. Improved heuristics for calculating the end-to-end delay of transmission and the trust factor of the nodes on the routing path are proposed. The proposed algorithm is compared with two existing algorithms: distributed energy-balanced routing and energy-efficient routing with node-compromised resistance. Simulation results show that the proposed QEBSR algorithm performed comparatively better than the other two algorithms. Kaur et al. [19] proposed an Optimized Energy Efficient and Quality-of-Service aware Routing Protocol (OEEQR) to achieve a longer network lifetime, energy efficiency, lower delay and high throughput. In the proposed protocol, the cost function with residual energy, distance and path loss as its parameters is optimized using the Particle Swarm Optimization (PSO) technique. The proposed cost function determines the best feasible next hop to send the data to the sink.

The QoS-aware routing optimization technique (QoS-ROA) was then introduced by Jiang et al. [14] to effectively handle the issue. The connection quality at the next instant is initially predicted using a wavelet neural network (WNN). Then utilize differential search (DS) to solve the proposed route optimization issue after converting it into a 0-1 knapsack problem. In Kalpana et al. [17], End-to-End Delay and bandwidth characteristics are tested with a Channel Aware AOMDV to offer QoS to the application layer. The Average Non-Fading Duration and Average Fading Duration will be used in the proposed strategy to analyze the channel fading. A QoS-aware routing with bandwidth and end-to-end delay is presented to decrease the control overhead. Different optimization-based MANET routing protocols have been put out for each of them to take into account various metrics and address certain issues. According to requirements for energy, stability, traffic, and hop count, Nabati et al. [28] presented a genetically based ad hoc on-demand distance vector mechanism. The ideal path is chosen using the Genetic Algorithm (GA) and Learning Automata (LA).

Multipath routing has been employed recently in WSN to provide scalable and dependable data transport. Even though several multipath routing methods have been put out, relatively few routing protocols have been specifically designed to provide QoS. The hybrid Particle Swarm Optimization and Cuckoo Search Optimization technique are used to cluster sensor nodes in Mohanadevi et al. [25] for a QoS-aware, multipath routing protocol. Using the cluster heads and multi-hop communication, the proposed protocol then selects several reliable pathways to send data. A novel protocol for sender-based responsive strategies on energy, mobility, and efficient routing

for WSN is suggested by Dhanalakshmi et al. [4]. It covers a variety of issues in WSN communication, including energy optimization, energy balance, and packet routing in particular. This key goal is to suggest a safe and resource-conserving routing protocol that makes use of fuzzy rules and a node's trust values.

Dynamic topology, hidden terminal, multi-hop routing, exposed terminal issues, packet loss, mobility, and security threats are just a few of the difficulties faced by MANET. The set of instructions used to direct data packets from one node to another is known as a routing protocol. In Choudhary et al. [3], a flooding mechanism is used to broadcast the packet to determine the potential paths from the source to the destination nodes without affecting network conditions like energy, bandwidth, and link quality. In the reactive AOMDV protocol, an existing path fails when a node along the way moves out of range or becomes unreachable owing to low energy. The packet delivery ratio is also impacted by malicious node behaviour or outside noise interference. For packet transmission through numerous paths from source to destination, Saravanan et al. [36] presented trusted optimum path selection using channel and node-aware routing as a solution to this problem. To find numerous routes from source to destination, the AOMDV reactive routing protocol is employed. Then, either the many best paths are used to route packets from source to destination, or the delay factors associated with the multiple best paths are calculated, and the optimal path with the lowest delay factor is chosen for packet transmission. To improve path selection and energy efficiency, a new hybrid Zone-based Hierarchical Routing Protocol (ZHRP) based on the Dynamic Cuckoo Search (DCS) algorithm has been presented by Gopalan et al. [10]. A dynamic switching parameter has been used in the DCS algorithm to maintain the harmony between the global and local random walks.

By keeping numerous channels open between the communication nodes, MANET routing overhead can be minimized. In this manner, an alternative path can be easily adopted when one path fails without requiring a new route discovery. The link-disjoint, loop-free multipath AOMDV protocol is ideal for MANET. A node can monitor the strength of the received signal and take required action when the signal strength drops below a threshold level rather than waiting until a link fails. The reliable energy and link AOMDV proposed routing protocol takes into account both of these factors during route discovery and maintenance in Dsouza et al. [5]. Additionally, MANETs' dispersed operating model, which does not rely on centralized hardware like base stations, makes the guarantee QoS problem one of their biggest difficulties. Therefore, Quy (2022) [31] proposed a QoS-aware on-demand routing protocol (QoS-ADRP) for urban-MANET applications. The suggested protocol can operate in both adaptive and admission modes to increase the viability of the solution.

3. Methods

Mobile routers connected through a wireless link self-configure MANETs, which are wireless networks with an absolute topology. Due to its dynamic nature, routing is now seen to be the key issue with MANET. For effective routing in MANET, route dis-

covery and the best route selection from a variety of routes are established. The main goal of this study is to choose the best route for MANET packet delivery. The mobility and resource limitations of nodes have a significant impact on the performance of mobile ad hoc networks (MANET). The development of a routing protocol that supports quality of service (QoS) in MANET is highly challenging since node mobility will affect connecting stability and node resource restrictions would cause congestion. It is necessary to develop the MANET protocol routing that can be adjusted for changes in the networking architecture to support QoS because, in particular, the frequent interrupting connection may decrease QoS performance in the high-speed node drive scenario. The suggested work's flow diagram is shown in Figure 1.

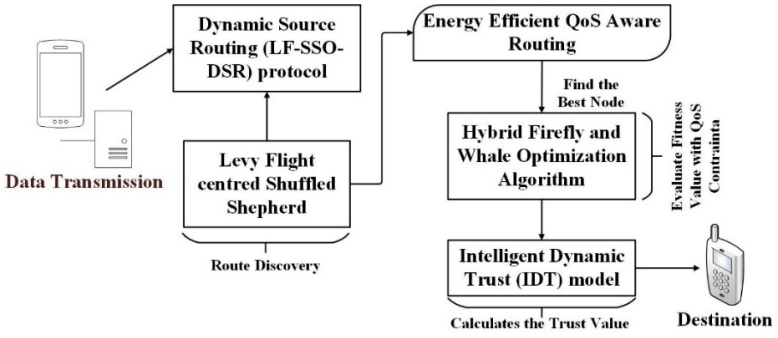

Figure 1. Flow diagram of the proposed work

The approach first identifies all possible paths between any source and any destination. Multiple routes are discovered using the route discovery scheme. With the use of the Levy Flight-centred Shuffled Shepherd Dynamic Source Routing (LF-SSO-DSR) protocol, which is used to apply an optimal path out of the multipath chosen based on QoS metrics, the transmission's best froute is chosen. Additionally, it has a high energy usage. Ad hoc network energy consumption is a constant challenge, which is what motivated the researchers to make use of bio-inspired algorithms and their fitness functions to assess node energy throughout the path-finding stage. To obtain the ideal values/fitness function for the objective parameter, hybrid firefly and whale optimization techniques also handle high energy consumption (i.e., energy). Somehow, there has been some exploration of the studies for resource limitations. The security challenges in MANETS present the most difficult assignment. The system and its linked consumer may be impacted by the adaptation of harmful elements, which causes communication issues. The reliability of each mobile node is assessed by taking into account factors such as the node's location, mobility speed, energy use, number of involved transmissions, neighbour list, etc. The research project then suggested the Intelligent Dynamic Trust (IDT) paradigm as a means of supplying security in wireless networks. For secure routing in mobile ad hoc networks, this paradigm combines beta reputation trust and dynamic trust.

3.1. Network model

The suggested system takes into account the network environment, which is organised and decentralized. The network's nodes can send and receive packets through many indirect hops. Assume there are N identical mobile nodes in the MANET network. The source node and destination node are allotted based on their respective distances, their ability to make linkages, and their routing paths. Each node can connect with its neighbouring nodes using a link l, while the nodes are separated by distance d and energy e. If the node i is the neighbour node of the node j, then the distance between these two nodes can be formulated as $d(i, j)$ and must be about the maximum transmission range of the node i, given as $d(i, j) < TR(i)$. Finding the best route while meeting QoS requirements and minimising energy consumption is known as QoS routing. Five evaluation factors are typically utilised as QoS limitations in IWSNs during actual factory production. They are bandwidth, cost, delay, delay jitter, cost, and packet loss rate. It is based on the supposition that neither the source nor the destination is malicious. Evil nodes do not cooperate among themselves, and all communication linkages are two-way. Additionally, the communication path is safe.

3.2. DSR routing mechanism

The routing pathways are determined at the time a source transmits a packet to the destination, making DSR the purest on-demand source routing system. Reactive routing protocol, or DSR, was specifically designed for use with multi-hop Adhoc networks of mobile nodes and allows the networks to function entirely on their own without centralised infrastructure. Each node in this style of routing stores the route data for recently taken routes by that node in cache memory. Route discovery and route maintenance are DSR routing's two key processes. A source node always verifies its route cache before attempting to send a packet to a destination node. The source node sends the packet along the available path if the route is open to the required destination node. Otherwise, the source node starts a route discovery process by implementing the LF-SSO method, which is done to give the nodes access to recognise and maintain the source routes to the destination nodes.

3.2.1. Optimal routing path discovery

To find a better link-quality path to transmit data from the SN to the DN, an optimal routing path discovery is used. The LF-SSO algorithm is used in this study to derive the best pathways from the chosen paths. The unique population-centred meta-heuristic LF-SSO method mimics the herding behaviour of shepherds. Shepherds put horses or other animals together to use their instincts to choose the finest pastures. The horses and lambs are chosen at random during the SSO algorithm's step size calculating process. Poor optimization is the result of this random selection. The proposed work substitutes a levy flight selection for a random selection to get over this problem. The LF-SSO algorithm is the term given to this algorithm.

First, a set of potential solutions is created, including sheep among other elements. The set of created potential solutions is expressed as in Equation (1):

$$\psi_j = \{\psi_1, \psi_2, \psi_3, \ldots, \psi_m\} \tag{1}$$

Herein, ψ_j signifies the candidate solution set; m implies the number of sheep ($m = h \times s$); h signifies the number of groups and s implies the number of sheep in every group. Then, jth sheep's initial position in the f-dimension is articulated as in Equation (2):

$$\psi_j^0 = \psi_{\min} + \hat{r} \circ (\psi_{\max} - \psi_{\min}) \tag{2}$$

Herein, ψ_j^0 represents j^{th} sheep's initial solution, $\psi_{\min}$ and $\psi_{\max}$are bound by design variables, $\circ$ implies the element-by-element multiplication and $\hat{r}$ is the random vector ($\hat{r} \in [0, 1]$). The fitness of each solution is then listed; here, the solutions of each candidate are taken into consideration as potential paths. As a result, the fitness of any solution is defined as the maximisation of path trust, minimization of EC, and minimization of path distance as expressed in Equation (3):

$$F_{opt} = \begin{cases} \max\left(\sum_{n=1}^{d} PT\left(N_n, N_{n+1}\right)\right) \\ \max\left(\frac{1}{N_n} \sum E_{res_n}\right) \\ \min\left(\sum_{n=1}^{d} dist\left(N_n, N_{n+1}\right)\right) \end{cases} \tag{3}$$

Where, $PT\left(N_s, N_{s+1}\right)$ and $dist\left(N_n, N_{n+1}\right)$ signify the path's trust and path's distance betwixt node N_n and N_{n+1}, correspondingly; $n = 1$ implies SN; d signifies the DN; E_{res_n}implies the node's residual energy. The solutions are arranged in ascending order based on the fitness values. To form the groupings, distribute the sheep to the group. The sheep are assigned to each group in descending order. The chosen sheep are known as shepherds, while the sheep that are well-fit and common in a herd are known as horses. Every shepherd's step-size $\left(S_{s_j}\right)$ is computed by choosing one amidst the horse and sheep as in Equations (4) and (5):

$$S_{s_j} = \omega \cdot L^y \circ (\psi_d - \psi_j) + \varpi \cdot L^y \circ (\psi_k - \psi_j) \tag{4}$$

$$L^y = t\left(-y\right), \quad 1 < y < 3 \tag{5}$$

Herein, ψ_d and ψ_k signify the horse and sheep chosen. L^y implies the levy flight distribution; $\omega$and ϖ imply the factors utilized to manage exploration and exploitation, correspondingly. These factors are enumerated in (6) and (7):

$$\omega = \omega_0 + \frac{\omega_{\max} - \omega_0}{I_{\max}} \cdot I \tag{6}$$

$$\varpi = \varpi_0 + \frac{\varpi_0}{I_{\max}} \cdot I \tag{7}$$

Herein, I implies the iteration; $I_{\max}$ signifies the maximal iteration.

The pseudo-code for the LF-SSO method, which is intended to find the best path, is shown in Algorithm 1. To achieve effective optimization, this algorithm executes good exploration in the initial iterations and better exploitation in the last rounds. Next, ψ_j the new position is enumerated as in Equation (8):

$$\psi_j'' = \psi_j^0 + S_{s_j} \tag{8}$$

If the fitness value ψ_j'' isn't worse analogized to ψ_j^0 fitness value, ψ_j's position is updated. Similarly, the fitness value of each path is assessed and compared to the corresponding old path. Repeating this process will continue until the best course is found.

Algorithm 1 Route Discovery with Optimum Routing Using LF-SSO

Input: Selected Routing Paths
Output: Optimal Routing path
Initialize the candidate solution ψ_j randomly
Determine the initial position using
$\psi_j^0 = \psi_{\min} + \hat{r} \circ (\psi_{\max} - \psi_{\min})$
Evaluate fitness
while ($I = 0$ to $I_{\max}$) **do**
    Sort the solutions in ascending order // F_{opt} and form group
    Determine step size
    $S_{s_j} = \omega * L^y \circ (\psi_d - \psi_j) + \bar{\omega} * L^y \circ (\psi_k - \psi_j)$
    Generate new elements
    $\psi_j^n = \psi_j^0 + S_{s_j}$
    if $\left(F_{opt}\left(\psi_j^n\right) \geq F_{opt}\left(\psi_j^0\right)\right)$ **then**
        sheep position $= \psi_j^n$
    else
        sheep position ψ_j^0
    end if
end while
Return Optimal routing path

3.3. Energy consumption with QoS constraints

The inability of MANETs to support mobile networking devices due to a lack of adequate energy is a significant problem. The MANETs' packet forwarding is hampered by this deficit. The main issue with MANET has been identified as energy consumption, and it needs to be dealt with appropriately. Consequently, when the distance between nodes grows, so does the transmission power. When compared to when data is received, more energy is used during data transfer.

A node's energy consumption can be represented as in:

$$E_c = E_{TR} + E_R \tag{9}$$

Where the E_{TR} represents the transmission energy and the E_R represents the receiving energy. These energy values can be determined using the:

$$E_{TR} = D_t \cdot E_{ut} \cdot T_t \tag{10}$$

Where the D_t gives the rate in which the data is transmitted and the E_{ut}represents the total energy that is utilized for that particular transmission and T_t is the time taken for transmission.

$$E_{UR} = D_R \cdot e \cdot t_r \tag{11}$$

Where, E_{UR} is the total energy that has been utilized in the reception process and D_R is the rate of reception and t_r denotes the time of receiving the data. A MANET atmosphere with n the number of nodes in the set of $\{N\}$. All the nodes are considered to be connected with the nearest node through a link represented as L with a distance d. Nodes i and j are the nearest nodes and their distance is denoted by $d_{i,j}$ is considered to be lesser or equal to that of the range of transmission in node i as in (12):

$$d_{i,j} \leq T_{R(i)} \tag{12}$$

The total power applied at each link toward the path of data transmission from source to BS, which is evaluated by, is used to calculate the energy usage of a path:

$$E_{path_i} = \sum_{j=1}^{hop_i} E_{link_j} \tag{13}$$

For transmitting n bits of the data packet, energy application of a path E_{path} should be minimum when compared with essential lower energy E_{req}. Hence, the energy objective function f_E helps to reduce the overall power utilization on a path and is determined by:

$$f_E = \min \{E_{path_i}\} \tag{14}$$

Finding the path with the lowest energy consumption while also satisfying equations is the routing energy consumption optimization challenge for IWSNs. $C(e)$ can be represented by:

$$C(e) = E_c + E_R \tag{15}$$

In (11), $C(e)$ is the total energy consumption between two adjacent nodes, which is composed of E_c and E_b. E_c represents the energy consumption of data transmission, and E_b denotes the energy consumption of receiving information between two nodes.

3.3.1. Hybrid firefly and whale optimization algorithms

A unique hybrid firefly and whale optimization technique is developed to evaluate the node's energy through the path discovery stage with QOS restrictions to optimise the routing energy consumption of IWSNs with QoS constraints. In the subsequent stages of the algorithm, WOA does a local search instead of a global search, which can successfully find the routing path that complies with the QoS requirements.

Firefly algorithm for cluster head selection

The flickering lights of fireflies serve as the basis for firefly algorithm metaheuristics. A firefly swarm can be mapped to an optimal solution in the search space by moving to brighter and more desirable regions as a result of the intensity of the light. The firefly metaheuristic was chosen since it can offer the best solutions to multiobjective problems. This paper proposes and provides a novel fitness function that takes into account energy, end-to-end delay, and packet loss rate.

$$f(x) = \frac{(P_d/P_t) \cdot E_i^r/E_{init}}{\exp^{-e_d/e_m}} \tag{16}$$

Where, P_d is the number of dropped packets. P_t is the total number of packets sent. E_i^r is the remaining energy in the node i. E_{init} is the initial energy. The symbol e_d is the end-to-end delay and e_m is the maximum allowable delay.

Algorithm 2 Pseudocode for cluster formation and CH selection in firefly

```
Objective function f(x), x = (x_1, ..., x_d) T
Generate the initial population of fireflies x_i (i = 1, 2, ..., n)
Define light absorption coefficient γ
Determine the light intensity at each firefly position
while (t < MaxGeneration) do
   for i = 1 : n all n fireflies do
      for j = 1 : n all n fireflies do
         if (I_j < I_i) then
            Move firefly i towards j in d dimension
         end if
         Attractiveness varies with distance r via exp[−γr]
         Evaluate new solutions and update light intensity
      end for
   end for
   Rank the fireflies and find the best node as the cluster head
end while
```

The objective function of the firefly algorithm is embedded in the modulation of light intensity and the phrasing of the problem in terms of attraction. The preset light absorption coefficient and the light intensity are used to calculate the light intensity I can be computed based on distance r such that:

$$I = I_0 e^{-\gamma r} \tag{17}$$

Where, I_0 is the original light intensity. Approximating using Gaussian law we have:

$$I(r) = I_0 e^{-\gamma r^2} \tag{18}$$

The attractiveness $\beta$of a firefly is given in:

$$\beta(r) = \beta_0 e^{-\gamma r^2} \tag{19}$$

Where, β_0 is the attractiveness at $r = 0$. In two-dimensional space, the distance between two fireflies can be given by their Euclidean distance as $r_{ij} = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}$. A firefly i moves to a more attractive firefly j by:

$$x_i = x_i + \beta_0 e^{-\gamma r^2} (x_j - x_i) + \alpha \left(rand - \frac{1}{2} \right) \tag{20}$$

The nodes in each solution are represented in this work by binary values. The challenge in this type of encoding is between the real-valued vector space R^N and binary space $\{0,1\}^N$ and given by:

$$X_{ik} = \begin{cases} 1, & \text{if } rand() \leq \dfrac{1}{1 + \exp(-X_{ik})} \\ 0, & \text{Otherwise} \end{cases} \tag{21}$$

Where, $k = 1, \ldots, N$ and $rand() \sim U(0,1)$.

The best fireflies are chosen via tournament selection in the proposed firefly algorithm once the fireflies are ranked. As part of the WOA algorithm, the FA algorithm is used to update the whales' positions.

Whale optimization algorithm

The network lifetime of IWSNs can be efficiently extended for cost savings in the factory while maintaining QoS restrictions by utilising WOA to identify the optimal routing path with the least amount of energy consumption. A route's energy consumption is represented by the whale's fitness value in the routing energy consumption optimization problem with QoS restrictions. To determine the location of the leading whale, it is required to compute each individual's fitness before doing any additional CAWOA actions. Each person's fitness value is calculated using a formula (22). A fitness function is created to analyse the energy usage of routing, as demonstrated in:

$$fitness = \min \left\{ \frac{C(a) + DL(a) \cdot 1 + DJ(a) + PLR(a) \cdot PLC}{r \cdot B(a)} \right\} \tag{22}$$

In (14), $a = r(v_s, v_d)$ represents all routing paths that meet the QoS constraints from the node s to the node d in MANET. $C(a)$ is the energy consumption between two nodes, $DL(a)$ is the delay between two nodes, $DJ(a)$ is the delay jitter, $PLR(a)$ is the packet loss rate, PLC is the cost of packet loss, and $B(a)$ is the network bandwidth, r is the bandwidth factor. However, if a route does not adhere to the QoS requirements which include those for latency, delay jitter, bandwidth, packet loss rate, and cost it will be disregarded.

Secondly, the leading whale's position influences the update of each whale's position, and its formula is shown in:

$$W(gen + 1) = W(gen) - A.D \tag{23}$$

Where, A is another coefficient vector, which is calculated by:

$$A = \begin{cases} A_1 - \frac{(A_1 - A_2)(f_c - f_{avg})}{f_{\max} - f_{avg}} & f_c \geq f_{avg} \\ A_1 & f_c < f_{avg} \end{cases} \tag{24}$$

Where, f_c is the fitness value of the current whale, $f_{\max}$ is the fitness value of the leading whale. Accordingly, C_1 and C_2 are two constants and f_{avg} is the average fitness value of the population and A_1, A_2 are two constants. The inclusion of adaptive operators enables WOA to dynamically modify the parameters following the fitness value when the whale is feeding, hastening the algorithm's convergence.

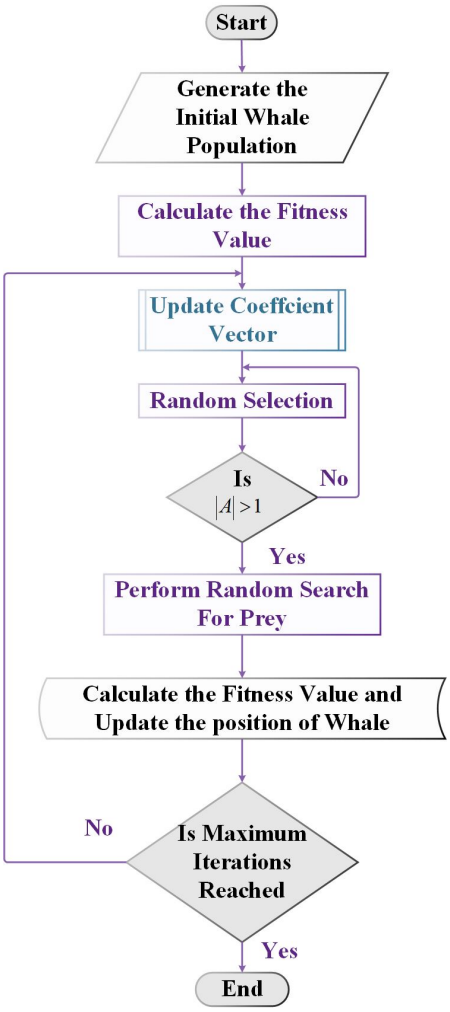

Figure 2. Flowchart of the whale optimization algorithm

The whale optimization algorithm's flowchart is shown in Figure 2. The location of the whale cannot always be updated by the position of the leading whale; occasionally, it must also be updated with the position of the partner to prevent hitting a local optimum when solving the MANET routing energy optimization issue under QoS restrictions. In particular, CAWOA's current mission is to conduct a random hunt for prey and determine the whale's future location. This operation is carried out while being influenced by the coefficient vector A. If $|A| > 1$, the random search behaviour of CAWOA increases the algorithm's capacity for global search, as demonstrated in:

$$D = |C \cdot W_r - W\,(gen)| \tag{25}$$

$$W\,(gen + 1) = W_r - A \cdot D \tag{26}$$

Where, W_r is the random position in the whale population. To simulate the trend of the algorithm for lowering routing energy consumption, algorithm convergence speed, and the percentage of energy consumption acquired after optimization in multipath routing MANET. Somehow, there has been some exploration of the studies for resource limitations. The security challenges in MANETS present the most difficult assignment. The system and its associated consumer may be impacted by the adaptation of harmful elements, which causes communication issues.

3.4. Intelligent dynamic trust (IDT) for secure routing

In this study, an intelligent trust paradigm for secure communication termed intelligent dynamic trust (IDT) is suggested. The beta distribution is a popular technique for converting observed data from the evidence space to the trust space. Let s and f represent the total amount of positive and negative feedback in the evidence space about the target entity, then the trustworthiness t of a subject node is then computed as:

$$t = \frac{s + 1}{f + s} \tag{27}$$

$$DT = Dynamic\ Trust\,(t, < t_1, t_2 >) \tag{28}$$

IDT is the combination of Dynamic Trust DT. The beta direct trust value is determined using intelligent agents and the Intelligent Dynamic Trust model. Here, the node trust is dynamically monitored by intelligent agents over a specific period. The suggested intelligent system presents each node's behaviour as a binary event. The distribution that is frequently used to represent the posterior probability of a binary event when using intelligent agents is utilised to model this binary event. Each node's dynamic trust model is assessed using the characteristics offered by the beta distribution that serves as a foundation. The family of probability density functions (PDFs) is a set of continuous functions indexed by two parameters α and β. In the beta reputation system, α is assigned as the number N_p of positive ratings plus 1 and β is assigned as the number N_n of negative ratings plus 1. Dynamic trust is

initially the anticipation of a node acting pleasantly. The trustworthiness value is determined through future interactions and is calculated as:

$$\frac{\alpha}{\alpha+\beta} = \frac{N_p+1}{N_p+N_n} + DT \tag{29}$$

Where, p indicates the decay factor of forgetting can be employed to give new ratings more weight while progressively reducing the weight of previous ratings. The following formula is used to calculate intelligent beta reputation and dynamic trust value:

$$I = \frac{s+1}{f+s+2} + \frac{ds+1}{df+ds} + DT \tag{30}$$

Algorithm 3 Intelligent dynamic trust algorithm

1: **Initialization:** Let $T_V\,(n_1, n_2, \ldots, n_m)$ // T_V indicate trust value, $n_1, n_2, \ldots, n_m$ are nodes

2: **Step 1:** Every node n_i is considered a source node at different time durations

3: **Step 2:** Every node $n_1, n_2, \ldots, n_m$ are considered a source node in a different time duration (t_1, t_2)

4: **Step 3:** Send messages to the neighbour nodes.

$$NC = NC + 1$$

5: **Step 5:** Start the Scheduler Class to execute the simulation.

6: **Step 6:** Verify that the node is the destination node if it got the request from neighbouring nodes. Otherwise, if it is a destination, it transmits the acknowledgement to the nodes next to it.

7: **Step 7:** Compute the trust score for all the nodes using

$$t = \frac{s+1}{f+s}$$

8: **Step 8:** Compute the dynamic trust score for all the nodes using

$$DT = Dynamic\ Trust\,(t, < t_1, t_2 >)$$

9: **Step 9:** Compute the overall trust score for all the nodes using Equation (3)

$$\frac{\alpha}{\alpha+\beta} = \frac{N_p+1}{N_p+N_n} + DT$$

10: **Step 10:** **if**$(Minimum\ Value < Threshold)$
then detect the malicious node
else update the routing table with the new node

11: **Step 11:** Perform routing performance

The combination of IDT and dynamic trust. The trust value is determined dynamically using the proposed intelligent beta reputation model. The proposed work comprises a three-phase trust-based secure routing algorithm that evaluates trust scores, sets thresholds, and routes traffic according to trust values. The crucial component of dynamic trust-based secure routing is the focus of the proposed work. The fundamental objective of this work is the trust-based secure routing method. The proposed secured routing Algorithm 3 follows these steps.

The trust value is determined dynamically by the proposed secure routing technique. For each participating node in the network scenario, the trust values are computed at various periods. By obtaining an acknowledgement for their messages, the participant nodes verified the correct destination node. Similarly, the trust score and dynamic trust score for each node have been determined using Equations (27) and (28). In a network situation, threshold values are set by intelligent agents and verified against the dynamic trust scores of every node. Any node that has a dynamic score below a threshold must be regarded as malicious and should not be used for routing if the dynamic score is below the threshold. All other nodes with dynamic scores over the threshold are then included in the routing process.

4. Results

To assess the performance of the MRLAM routing system, which is compared with E-RARP, EEC-HO, TAGA, EHO-ETQRP, ETOR, and the proposed routing schemes, utilising the varied speed of node scenarios, extensive simulations have been carried out using the Network Simulator 3.36 simulator. One of the key criteria in research evaluating routing methods in MANETs is node speed. The efficiency of the proposed strategies' mobility awareness was assessed by taking mobility-related factors into account. The maximum speed in the RWP model was adjusted from 0 m/s to 10 m/s to specify the maximum waypoint speed of nodes.

4.1. Evaluation criteria of the proposed work

In the suggested work, experiments were carried out using the above-mentioned QoS parameters. The study observes the following results with QoS parameters by simulating the scenario created for analysing the impact of mobility on mobile network QoS parameters (throughput, average jitter, average end-to-end delay). Through some time simulations, the percentage of dead nodes, network longevity, energy consumption per node, and a fraction of alive nodes are all examined. This large simulation's goal is to assess the effectiveness of the suggested routing strategy, and the following metric is used to accomplish with:

Energy Consumption. The total energy used by all nodes for key transmission during the simulation is what is meant by this term. After each simulation, the energy consumption of each node is calculated while accounting for its initial energy.

The data transmission energy usage formula is:

$$E_{consumption} = \frac{E_{Total}}{Number\ of\ Packets\ successfully\ Transmitted} \tag{31}$$

where, E_{Total} is the total energy of the node which is 3600 mAh in the simulation model.

Jitter. The jitter is the variance in the transmission of messages from beginning to end. In the case of jitter evaluation, the message transmission time is very brief. The transfer delay time must be less than the necessary point value in the case of the jitter value. The following calculation yields the average value of jitter:

$$Jitter = D - (Q_{rs} - Q_{st}) \tag{32}$$

Packet Delivery Ratio (PDR). The number of packets received by the sinks at the destination divided by the number of packets generated by the application layer is the ratio. The following equation is used to calculate the packet delivery ratio for the proposed KF-MAC protocol:

$$PDR = \frac{Q_{rx}}{Q_{st}} \tag{33}$$

where, Q_{rx} is the received packet and Q_{st} is the sent packet.

Throughput. The quantity of successful messages sent over MANET is the network's throughput. Throughput is used to analyse messages sent in a given amount of time. The following equation yields the network throughput analysis:

$$Throughput = \frac{size_B \cdot T_{message\ Transmitted}}{T_r\,(simulation)} \tag{34}$$

where, B is the bit message, T_r is the response time.

Figure 10 shows a comparison of the KF-MAC protocol's throughput with those of the existing E-RARP, EEC-HO, TAGA, EHO-ETQRP, and ETOR protocols.

Number of Dead Nodes (NoDN). The metric displays all dead nodes after the simulation period.

Energy Cost per Packet (ECP). This indicator displays the average energy consumption as a percentage of the number of packets that were successfully received at the destinations. It is calculated as shown in the equation below:

$$ECP = \frac{Average\ Energy\ Consumption}{Total\ Packets\ Received} \tag{35}$$

According to Figure 3, all routing protocols spend more energy as the number of mobile nodes rises, which results in a larger network size since the mobile nodes in the network must process all of the routing packets. Figure 3 shows that from 14 to 18 nodes, all proposed protocols' energy usage is very similar. However, when

the network size increases to 40 nodes, a noticeable change in energy consumption is apparent. Execution time is reduced by 3% in comparison to the current model, but energy usage is reduced by about 20%.

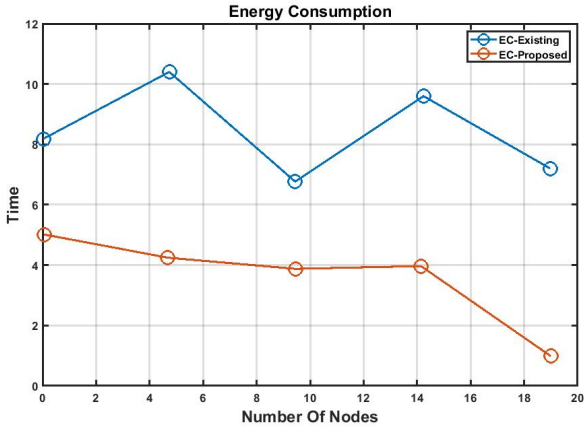

Figure 3. Energy of network nodes vs time

The graphs of the routing energy usage optimization are shown in Figure 4. This illustrates how the suggested optimization converges more quickly than the existing algorithms, which have slow convergence rates. While FFWHO gets the best routing solution with a 0.38 J energy consumption and a faster convergence speed, the suggested technique is locked in premature convergence. At the start of the iteration, this achieved lower routing energy usage than other algorithms, and this trend was maintained until the algorithm's termination.

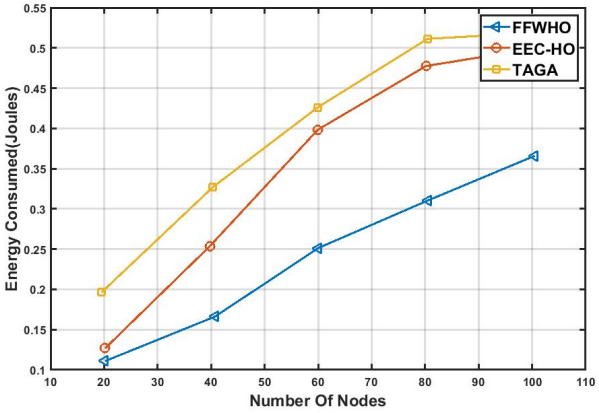

Figure 4. Energy consumption analysis

The end-to-end delay between the current and suggested algorithms, with the number of nodes, is represented by the plot in Figure 5. It has been determined that the suggested technique improved network performance and recorded the smallest end-to-end delay at time 0.0015. This authentication method causes a delay, which lasts longer in the event of an attack. In particular, it is the reason for attacks that perform poorly in terms of security once the path has been set.

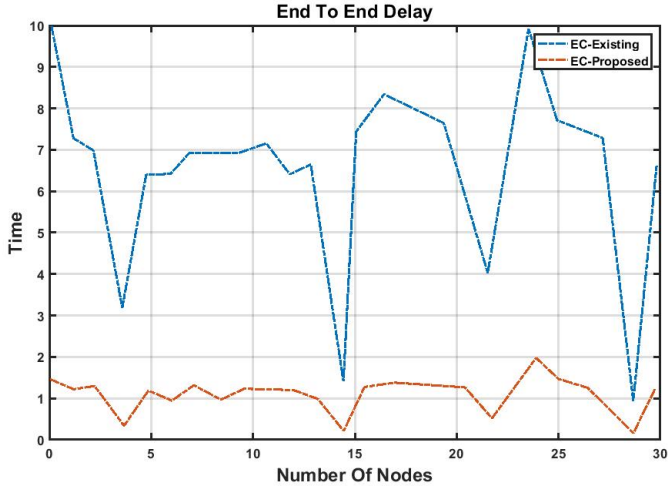

Figure 5. End-to-end delay vs time

The DSR application is connected between the two nodes in this example, node 9 is delivering packets to node 3. Delay is introduced during transmission, and the average end-to-end delay varies with the change in speed. Figure 6 displays the average end-to-end delay variation concerning speed. Figure 6 shows that the average end-to-end delay is very low while the speed is low, or 0.02926 s at the speed of 10 m/s, but it grows as the speed increases, becoming 0.11596 at the speed of 30 m/s. The movement of node 3 affects the average end-to-end delay since the mobility model is a random waypoint.

Figure 7 shows that the jitter is initially very low, or 0.01129 seconds when node 5 is moving at a speed of fewer than 10 m/s. As speed increases, however, the jitter likewise rises, reaching 0.06792 seconds at a speed of 15 m/s. The reason for this is that either the entire signal is broken up into chunks of data and conveyed to a receiving device for assembly, or the data is divided up into manageable "packets" with headers and footers that indicate the correct order of the data packets. Jitter makes synchronisation difficult and makes it challenging for the receiving unit to accurately assemble the incoming data stream. As a result, throughput is lower and jitter is greater at high speeds.

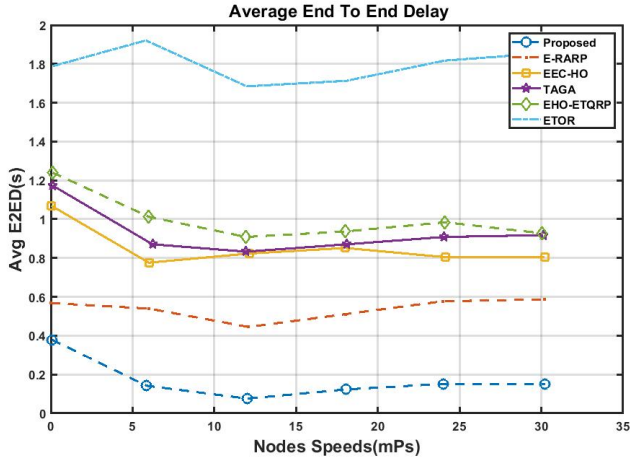

Figure 6. Average end-to-end delay

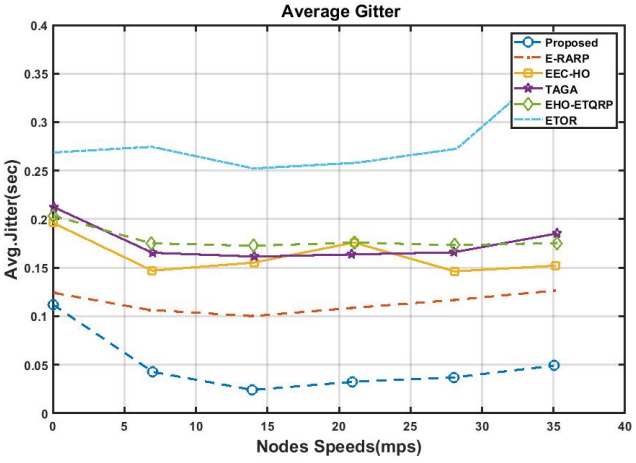

Figure 7. Average jitter vs nodes speed

The total packets dropped as a measure of packet loss and transmission failure is another QoS metric that is compared in this scenario and is shown in Figure 8. The findings show that the suggested reduces the overall number of packets dropped and achieves the lowest number of dropped packets across all scenarios. When compared to LS-SSO-DSR, which is obtained at 10 m/s, the suggested minimises the number of missed packets up to 329 packets. Using energy and mobility-aware approaches, the MBMA-OLSR outperformed the traditional scheme and reduced the number of packets missed, enabling it to successfully transfer the packets between source-destination pairs. The rising number of missed packets in LS-SSO-DSR is ascribed to the lack of mobility awareness support, which would have allowed users to choose the optimum paths, particularly in the event of a link failure brought on by node mobility.

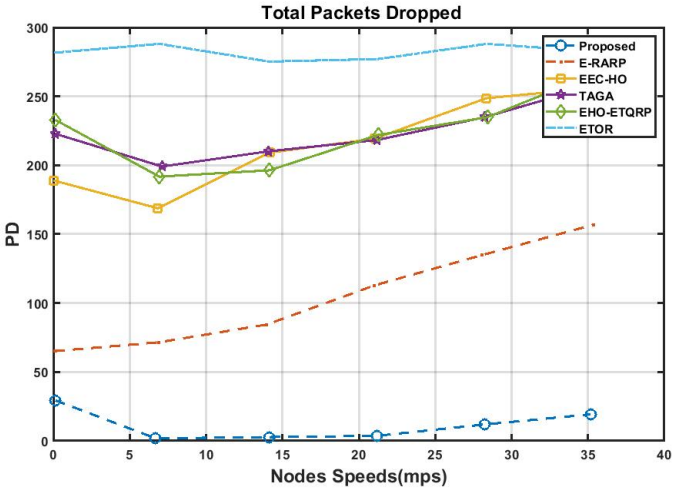

Figure 8. Packets drop vs nodes speed

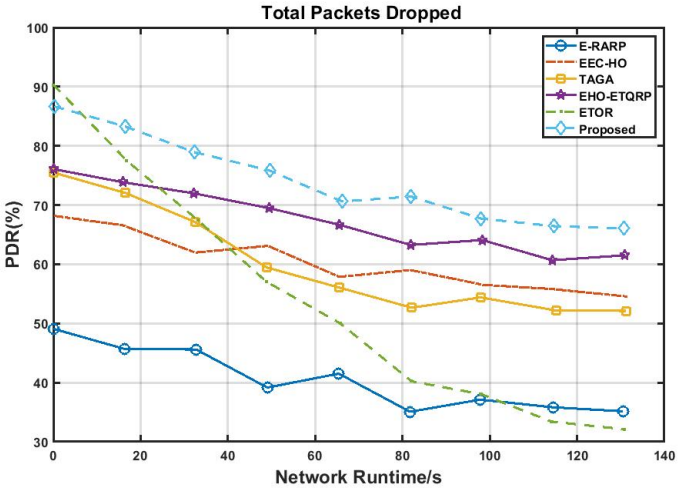

Figure 9. Packet delivery ratio vs network runtime

As the network size grows, the PDR of DSR gradually declines, as illustrated in Figure 9. Unlike other figures, this one compares the performance improvement brought on by the hybrid nature of LA-SSO-DSR by including graphs for reactive routing protocols E-RARP, EEC-HO, TAGA, EHO-ETQRP, and ETOR as examples. Regardless of network size, this surpasses all other approaches and successfully raises the PDR. Maintains a PDR of at least 83% as the desired level of quality of service for consistent data transmission. As a result, the routing protocol maintains a greater

PDR and lower delay than previous multipath systems by choosing nodes with high residual energy, low congestion levels, and lengthy idle times.

In terms of node speed and routed data packets, Figure 10 shows the throughput performance parameter of MANETs using E-RARP, EEC-HO, TAGA, EHO-ETQRP, and ETOR. Figure 3 shows that at 10 m/s (metre per second), throughput is 2 bits and that as speed increases, throughput decreases. For a 25 m/s node speed, the LA-SSO-DSR protocol outperformed EEC-HO by up to 14% in throughput. Finally, the outcome demonstrates that the suggested convention performs better.

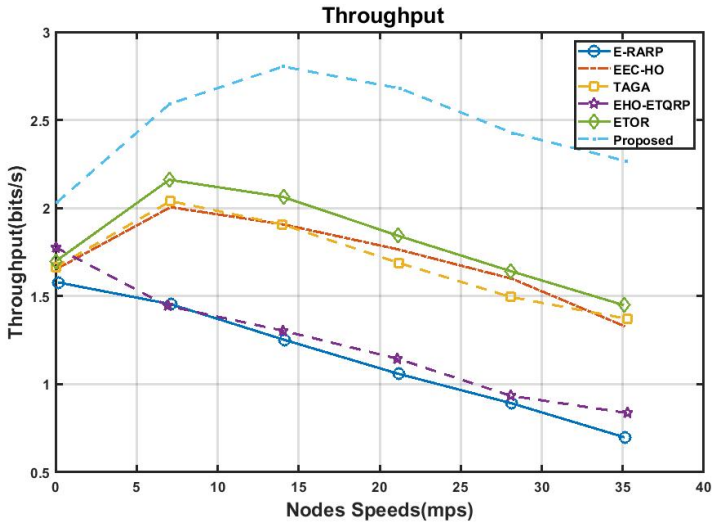

Figure 10. Throughput vs nodes speed

Figure 11 illustrates that there are very few interactions between nodes and that the impact of dynamic weight on integrated trust value is near $\phi = 0.1$. The trust value is more dependent on indirect trust when there are fewer interactions between nodes, and as interaction times increase, the effect of dynamic weight on integrated trust value gradually moves towards $\phi = 0.9$. This indicates that the integrated trust value metric measure is more dependent on direct trust as the number of contacts between nodes increases. The acquired results are consistent with the earlier theoretical study. The accuracy of trust measurement can be improved by dynamically adjusting the weight factor following the volume of node interactions.

Figure 12 illustrates how many dead nodes there are. This straightening results from duplicate pathways created by dying nodes close to the target. However, this straight line emerges much later in the figure for other approaches, indicating a longer lifetime. The chart makes it evident that the clustering with the gateway method has 50% of nodes still alive after 275 rounds, but 50% of nodes in both other schemes die considerably sooner due to significant energy consumption at roughly 65 rounds.

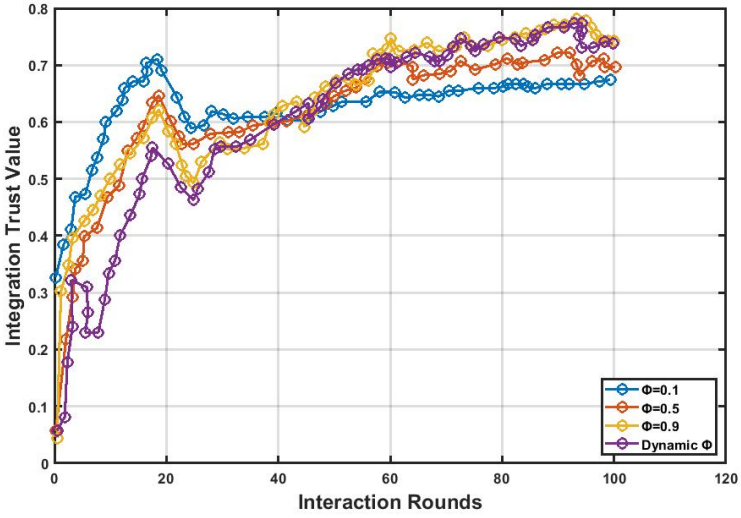

Figure 11. Effect of dynamic weights on integrated trust value

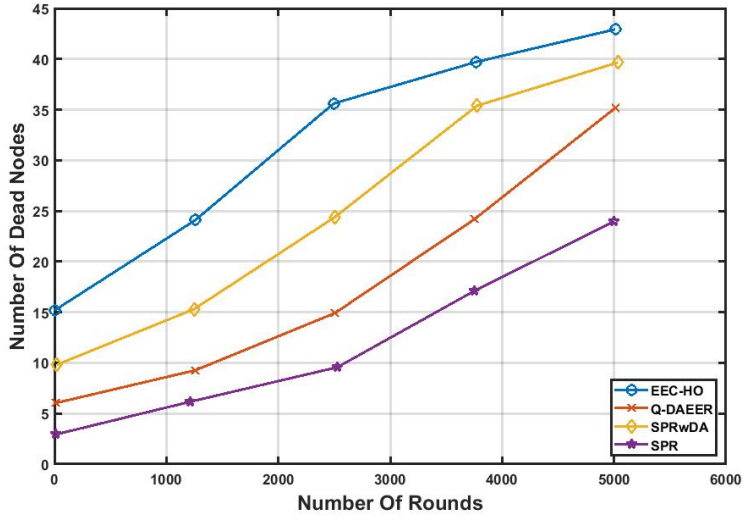

Figure 12. Number of dead nodes vs number of rounds

Figure 13 displays the detection rate for several trust models, and can see how the DTEM performed for Data 1, Data 2, and Data 3. Data 1 and 2 are subject to numerous attacks, therefore when the number of malicious nodes rises, the detection rate rapidly declines, however, data 3 maintains a high detection rate. As a result, the

IDT is a reliable trust evaluation model that can recognise many types of malicious nodes and may be dynamically altered to meet the unique needs of the network.

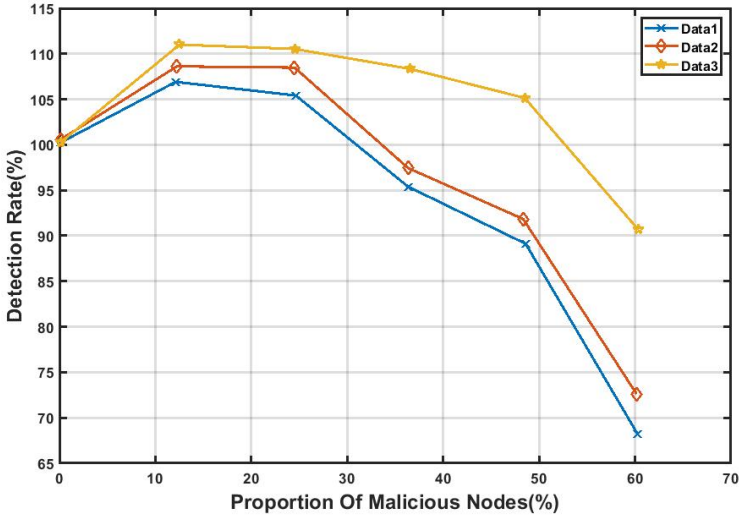

Figure 13. Proportion of malicious nodes

5. Discussion

The effectiveness of the optimised dynamic source routing protocol (DSR) for MANETs is examined in this article. The LF-SSO algorithm is used to modify the conventional DSR algorithm to determine the best routes between the communication nodes. In this work, the performance of the suggested technique is compared to the performance of the DSR protocol when there are malicious nodes present. Describes the variation in trust scores between the current and proposed systems. The proposed system outperforms the current system. This is because dynamic trust value calculation and a clever reputation system are used. In the initial deployment region of 1000 m $\times$ 1000 m, the network is clustered with 100 nodes. In terms of node speed and routed data packets, the article finds the throughput, energy consumption, jitter, packet delivery ratio, the number of dead nodes, and energy cost per packet performance parameter of MANETs is estimated using comparison techniques of E-RARP, EEC-HO, TAGA, EHO-ETQRP, and ETOR. The proposed technique has a 25 m/s node speed for protocol also the technique outperformed EEC-HO by up to 14% in throughput.

Subbaiah et al. [37] provided a reliable and energy-efficient healthcare system routing technique to balance QoS and power consumption. Performance metrics include routing overhead, energy consumption, end-to-end latency, throughput, scala-

bility, and transmission error. According to testing, IBOLSR uses less energy and has a longer lifespan than OLSR, EAOLSR, and BOLSR. The simulation results demonstrate that the proposed algorithm outperforms other existing algorithms. In tests, the proposed work shows a 79% less Average End-to-End Delay compared to other existing algorithms. Rachna Jain et al. [12] study illustrates that the throughput of proposed LD-OLSR is increased by 13% over conventional OLSR with 120 s of simulation time.

Rama Rao [33] proposed FCS-based multipath selection shows that the proposed QoS aware routing protocol performs better than the existing routing protocol with a maximal energy of 99.1501 and minimal delay of 0.0554. Later, Kebebew Ababu Yitayih et al. [40] proposed quality of service (QoS) supporting the MPR selection approach and a new lower maintenance clustering approach for minimizing the overhead of the network. The study selects a minimum number of MPR, and it minimizes the number of retransmitted control packets of a network into 61.12. R. Lavanya et al. [22] proposed an energy-efficient and optimal QoS-aware multi-path routing protocol based on EHO (Elephant Herding Optimization) algorithm and trust called EHO-ETQRP for IoT. Based on the energy and trust update, the secure nodes are selected and which improves secure communication. The simulation result proves that the proposed routing protocol is used to increase the delivery ratio, energy efficiency and network lifetime, which are the network-related QoS parameters. Rajakumar Ramalingam et al. [34] proposed the ad hoc on-demand distance vector protocol (AODV) is used and analyzed based on MANET's QoS (Quality of Service) metrics. The QoS metrics for MANET depend on delay, bandwidth, memory capacity, network load, and packet drop. This proposed algorithm stagnates in a lifetime of 4 ms.

Mamatha et al. [24] took an algorithm that takes place from 210 to 230 bits/s with 25–175 time intervals. Veguru Gayatri et al. [8] overcome the limitations of slow convergence and premature resolution of Quality of Service using multicast routing problems particle swarm optimization algorithm (PSO) and genetic algorithm (GA). The value of BER decreased for all techniques as the node increased. The suggested work displays a BER of 8% at the outset. Mobile nodes dynamically enter and exit the network often, resulting in unstable network topology in MANET. As a result, maintaining a stable network becomes a challenging task. Path preservation, battery life, safety, dependability, and unexpected connection characteristics are the major issues in MANET.

Rajathi et al. [32] presented a cluster coordinator-based CH election mechanism (CCCH). The comparison result proves that the proposed algorithms' performance is far better than the others in all evaluation metrics, such as energy consumption, packet delivery ratio (PDR), and the number of CH changes. K. Nirmaladevi et al. [29] proposed Selfish Node aware Trustable and Optimized Clustering-based Routing (SN-TOCRP) follows hierarchical clustering for creating node clusters. This achieves improved results with a Packet delivery ratio of 96%, a loss ratio of 0.045%, an average delay of 0.325 ms with throughput is 76 Kbps, an end-to-end delay of 0.425 ms and

an energy consumption of 88 MJ. The comparison results prove that the proposed system performs better than the existing approaches in all evaluation metrics.

Limitations

The comparison highlights the design of efficient routing protocols satisfying specific QoS metrics for a specific application using a specific routing technique. Moreover, WSNs need to provide different levels of Quality of Service (QoS) based on the different demands of various types of applications. The proposed framework still outperforms the malicious node scenarios based on the stated performance metrics. However, the study does not undertake any attack-related results, this tends to improve the robustness of the study.

6. Conclusion and future scope

Due to the lack of centralised control, Mobile Adhoc Networks (MANET) experience more network disconnections as a result of energy depletion issues. The main difficulties that MANET networks encounter are their dynamic topologies, energy constraints, bandwidth limitations, varying links, higher loss rates, high delay, and jitter, as well as the lack of centralised control and their limited physical security. However, node information must be continuously maintained for routing. So, reactive routing protocols (also known as on-demand routing protocols) were used to overcome these constraints and improve the routing performance in MANETs. The majority of Adhoc networks favour these reactive protocols. As a result, the research suggested using the Levy Flight-centred Shuffled Shepherd Dynamic Source Routing (LF-SSO-DSR) protocol to choose the best path out of a group of paths that were chosen based on QoS parameters. The main and crucial problem with MANET, aside from the routing technology, is how it operates under energy constraints. The batteries' issue with energy depletion has a big impact on how well the network functions. Because of this, hybrid firefly and whale optimization methods (FFWHO) successfully find the routing path that complies with QoS requirements. The research project then suggested the Intelligent Dynamic Trust (IDT) paradigm as a means of supplying security in wireless networks. The simulation moves following the mass mobility model to evaluate the performance of the energy-efficient-based QoS-aware routing protocol. Performance analysis of QoS metrics is evaluated in Network Simulator 3.36 simulation. Several performance metrics, including throughput, energy consumption, packet delivery ratio, jitter, end-to-end delay, packet loss rate, detection rate, and routing overhead, are used to assess the suggested approach. This outcome shows that the suggested strategy works better than other cutting-edge approaches. The simulation results demonstrate that in terms of routing energy consumption, convergence speed, and optimization capability, the proposed routing algorithm based on the optimization algorithm outperforms existing methods. It follows that the adoption of LA-SSO-DSR with a hybrid optimization approach can successfully lower the MANET's routing energy consumption.

References

[1] Abdullah A.M., Ozen E., Bayramoglu H.: Energy Efficient MANET Routing Protocol Based on Ant Colony Optimization, *Adhoc & Sensor Wireless Networks*, vol. 47(1-4), pp. 73–96, 2020.

[2] Amjad M., Afzal M.K., Umer T., Kim B.S.: QoS-aware and heterogeneously clustered routing protocol for wireless sensor networks, *IEEE Access*, vol. 5, pp. 10250–10262, 2017. doi: 10.1109/access.2017.2712662.

[3] Choudhary S., Narayan V., Faiz M., Pramanik S.: Fuzzy Approach-Based Stable Energy-Efficient AODV Routing Protocol in Mobile Ad hoc Networks. In: *Software Defined Networking for Ad Hoc Networks*, pp. 125–139, Springer, Cham, 2022. doi: 10.1007/978-3-030-91149-2_6.

[4] Dhanalakshmi B., SaiRamesh L., Selvakumar K.: Intelligent energy-aware and secured QoS routing protocol with dynamic mobility estimation for wireless sensor networks, *Wireless Networks*, vol. 27(2), pp. 1503–1514, 2021. doi: 10.1007/s11276-020-02532-8.

[5] Dsouza M.B., Manjaiah D.H.: Improving the QoS of Multipath Routing in MANET by Considering Reliable Node and Stable Link. In: *Sustainable Communication Networks and Application*, pp. 535–546, Springer, Singapore, 2021. doi: 10.1007/978-981-15-8677-4_43.

[6] El Dien M.E., Youssif A.A.A., Ghalwash A.Z.: Energy efficient and QoS aware framework for video transmission over wireless sensor networks, *Wireless Sensor Network*, vol. 8(3), pp. 25–36, 2016. doi: 10.4236/wsn.2016.83003.

[7] Faheem M., Gungor V.C.: Energy efficient and QoS-aware routing protocol for wireless sensor network-based smart grid applications in the context of industry 4.0, *Applied Soft Computing*, vol. 68, pp. 910–922, 2018. doi: 10.1016/j.asoc.2017.07.045.

[8] Gayatri V., Kumaran M.S.: Energy Efficient Cluster based Multipath Routing Protocol in MANET using Genetic Particle Swarm Optimization Algorithm, *International Journal of Intelligent Systems and Applications in Engineering*, vol. 10(4), pp. 231–239, 2022.

[9] Ghaleb S.A.M., Varadharajan V.: Convergence Factor and Position Updating Improved Grey Wolf Optimization for Multi-constraint and Multipath QoS Aware Routing in Mobile Adhoc Networks, *International Journal of Intelligent Engineering and Systems*, vol. 13(4), 2020. doi: 10.22266/ijies2020.0831.40.

[10] Gopalan S.H.: ZHRP-DCSEI, a Novel Hybrid Routing Protocol for Mobile Ad-hoc Networks to Optimize Energy Using Dynamic Cuckoo Search Algorithm, *Wireless Personal Communications*, vol. 118(4), pp. 3289–3301, 2021. doi: 10.1007/s11277-021-08180-1.

[11] Hemalatha R., Umamaheswari R., Jothi S.: ANFIS Based Optimal Routing using Group Teaching and Adaptive Equilibrium Optimization based Trust Aware Routing Protocol in MANET, 2021. doi: 10.21203/rs.3.rs-355720/v1.

[12] Jain R., Kashyap I.: An QoS aware link defined OLSR (LD-OLSR) routing protocol for MANETs, *Wireless Personal Communications*, vol. 108(3), pp. 1745–1758, 2019. doi: 10.1007/s11277-019-06494-9.

[13] Jayalakshmi D.S., Hemanand D., Kumar G.M., Rani M.M.: An Efficient Route Failure Detection Mechanism with Energy Efficient Routing (EER) Protocol in MANET, *International Journal of Computer Network & Information Security*, vol. 13(2), 2021. doi: 10.5815/ijcnis.2021.02.02.

[14] Jiang L., Xia W., Yan F., Shen L., Zhang Y., Gao Y.: QoS-aware Routing Optimization Algorithm using Differential Search in SDN-based MANETs. In: *2021 IEEE Global Communications Conference (GLOBECOM)*, IEEE, 2021. doi: 10.1109/globecom46510.2021.9685327.

[15] Joshi S.S., R. B.S.: A Novel Golden Eagle Optimizer Based Trusted Ad Hoc On-Demand Distance Vector (GEO-TAODV) Routing Protocol, *International Journal of Computer Networks and Applications*, vol. 8(5), pp. 538–548, 2021. doi: 0.22247/ijcna/2021/209986.

[16] Kalidoss T., Rajasekaran L., Kanagasabai K., Sannasi G., Kannan A.: QoS aware trust-based routing algorithm for wireless sensor networks, *Wireless Personal Communications*, vol. 110(4), pp. 1637–1658, 2020. doi: 10.1007/s11277-019-06788-y.

[17] Kalpana V., Saravanan G., Noorul Julaiha A.G., Balamanigandan R.: An Intensify Manet Based Channel and QoS Conscious Routing Using AOMDV, *Turkish Journal of Physiotherapy and Rehabilitation*, vol. 32(3), pp. 35–48, 2022.

[18] Karthick K., Asokan R.: Mobility aware quality enhanced cluster-based routing protocol for mobile ad-hoc networks using hybrid optimization algorithm, *Wireless Personal Communications*, vol. 119(4), pp. 3063–3087, 2021. doi: 10.1007/s11277-021-08387-2.

[19] Kaur T., Kumar D.: MACO-QCR: multi-objective ACO-based QoS-aware cross-layer routing protocols in WSN, *IEEE Sensors Journal*, vol. 21(5), pp. 6775–6783, 2020. doi: 10.1109/jsen.2020.3038241.

[20] Khan Z.A., Sivakumar S.C., Phillips W.J., Robertson B.: QPRR: QoS-aware peering routing protocol for reliability sensitive data in body area network communication, *The Computer Journal*, vol. 58(8), pp. 1701–1716, 2015. doi: 10.1093/comjnl/bxu114.

[21] Kumar D.A., Nyamathulla S., Kirankumar M., Kumar K.V., Jayasankar T.: A Hybrid Secure Aware Routing Protocol for Authentication in MANET, *International Journal of Advanced Science and Technology*, vol. 29(3), pp. 8786–8794, 2020.

[22] Lavanyaa R., Shanmugapriya N.: Energy efficient with trust and QoS-aware optimal multipath routing protocol based on elephant herding optimization for IoT based wireless sensor networks, *Turkish Journal of Computer and Mathematics Education*, vol. 12(9), pp. 979–990, 2021.

[23] Malar A.C.J., Kowsigan M., Krishnamoorthy N., Karthick S., Prabhu E., Venkatachalam K.: Multi constraints applied energy efficient routing technique based on ant colony optimization used for disaster resilient location detection in mobile ad-hoc network, *Journal of Ambient Intelligence and Humanized Computing*, vol. 12(3), pp. 4007–4017, 2021. doi: 10.1007/s12652-020-01767-9.

[24] Mamatha C.R., Ramakrishna M.: An Energy Efficient Model for Node Ranking and Routing path Computation using Optimal Type-2 Fuzzy Logic Controller, 2023. doi: 10.21203/rs.3.rs-1652397/v1.

[25] Mohanadevi C., Selvakumar S.: A QoS-aware, hybrid particle swarm optimization-cuckoo search clustering based multipath routing in wireless sensor networks, *Wireless Personal Communications*, vol. 127, pp. 1985–2001, 2021. doi: 10.1007/s11277-021-08745-0.

[26] Mostafavi S., Hakami V., Paydar F.: A QoS-assured and mobility-aware routing protocol for MANETs, *JOIV: International Journal on Informatics Visualization*, vol. 4(1), pp. 1–9, 2020. https://joiv.org/index.php/joiv/article/view/343.

[27] Muthumayil K., Buvana M., Jayasankar T.: Secure and Energy Efficient Routing Protocols for MANET using BAT Optimization, *International Journal of Modern Agriculture*, vol. 10(2), pp. 1649–1656, 2021.

[28] Nabati M., Maadani M., Pourmina M.A.: AGEN-AODV: an intelligent energy-aware routing protocol for heterogeneous mobile ad-hoc networks, *Mobile Networks and Applications*, pp. 576–587, 2021. doi: 10.1007/s11036-021-01821-6.

[29] Nirmaladevi K., Prabha K.: A selfish node trust aware with Optimized Clustering for reliable routing protocol in Manet, *Measurement: Sensors*, vol. 26, 100680, 2023. doi: 10.1016/j.measen.2023.100680.

[30] Patel J., El-Ocla H.: Energy Efficient Routing Protocol in Sensor Networks Using Genetic Algorithm, *Sensors*, vol. 21(21), 7060, 2021. doi: 10.3390/s21217060.

[31] Quy N.M., Ban N.T., Quy V.K.: An Adaptive On-demand Routing Protocol with QoS Support for urban-MANETs, *IAENG International Journal of Computer Science*, vol. 49(1), pp. 252–259, 2022. https://www.iaeng.org/IJCS/issues_v49/issue_1/IJCS_49_1_26.pdf.

[32] Rajathi L.V., Ruba Soundar K.: An advancement in energy efficient clustering algorithm using cluster coordinator-based CH election mechanism (CCCH), *Measurement: Sensors*, vol. 25, 100623, 2023. doi: 10.1016/j.measen.2022.100623.

[33] Rama Rao A., Reddy S., Valli Kumari V.: Multi-path selection based on fractional cuckoo search algorithm for QoS aware routing in MANET, *Sensor Review*, vol. 39(2), pp. 218–232, 2019. doi: 10.1108/SR-08-2017-0170.

[34] Ramalingam R., Muniyan R., Dumka A., Singh D.P., Mohamed H.G., Singh R., Anand D., *et al.*: Routing Protocol for MANET Based on QoS-Aware Service Composition with Dynamic Secured Broker Selection, *Electronics*, vol. 11(17), 2637, 2022. doi: 10.3390/electronics11172637.

[35] Rathee M., Kumar S., Gandomi A.H., Dilip K., Balusamy B., Patan R.: Ant colony optimization based quality of service aware energy balancing secure routing algorithm for wireless sensor networks, *IEEE Transactions on Engineering Management*, vol. 68(1), pp. 170–182, 2019. doi: 10.1109/tem.2019.2953889.

[36] Saravanan M., Reddy K.L.K., Nadhan R.S., Kumar K.V., Sundaramurthy B., Karthik G.: Trusted Optimum Path Selection Using Channel and Node Aware Routing in Manet, *Nveo – Natural Volatiles & Essential Oils Journal*, pp. 15234–15247, 2021.

[37] Subbaiah C.V., Govinda K.: Implementing routing protocol for energy-aware mobile ad hoc networks for WBAN-based healthcare systems, *Soft Computing*, vol. 28, 469, 2023. doi: 10.1007/s00500-023-07975-7.

[38] Veeraiah N., Khalaf O.I., Prasad C.V.P.R., Alotaibi Y., Alsufyani A., Alghamdi S.S., Alsufyani N.: Trust aware secure energy efficient hybrid protocol for Manet, *IEEE Access*, vol. 9, pp. 120996–121005, 2021. doi: 10.1109/access.2021.3108807.

[39] Vu Q.K., Le N.A.: An Energy-Efficient Routing Protocol for MANET in Internet of Things Environment, *iJOE International Journal of Online and Biomedical Engineering*, vol. 17(07), pp. 88–99, 2021. doi: 10.3991/ijoe.v17i07.23273.

[40] Yitayih K.A., Libsie M.: Towards developing enhanced cluster-based QoS-aware routing in MANET, *Journal of Computer Networks and Communications*, vol. 2020, 5481916, 2020. doi: 10.1155/2020/5481916.

Affiliations

Veeramani R.
Annamalai University, Department of Computer Science and Engineering, Annamalai Nagar, Chidambaram, Tamil Nadu 608002, India, gvmani.r@gmail.com

R. MadhanMohan
Annamalai University, Department of Computer Science and Engineering, Annamalai Nagar, Chidambaram, Tamil Nadu 608002, India, madhanmohan_mithu@yahoo.com

C. Mahesh
Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Department of Information Technology Chennai, Tamil Nadu 600062, India chimahesh@gmail.com

Received: 18.12.2022
Revised: 6.02.2024
Accepted: 7.04.2024