

# Energy efficient secured-quality of service routing protocol for mobile ad hoc network using multi-objective optimization

Veeramani Ramasamy<sup>1</sup>, Madhan Mohan Ramalingam<sup>1</sup>, Mahesh Chitraivel<sup>2</sup>

<sup>1</sup>Department of Computer Science and Engineering, Annamalai University, Annamalai Nagar, India

<sup>2</sup>Department of Information Technology, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, India

## Article Info

### Article history:

Received Nov 10, 2022

Revised Mar 28, 2023

Accepted Apr 16, 2023

### Keywords:

Cluster head selection  
Energy efficient routing  
protocol  
Multi-path routing protocol  
MO-GWO  
Node authentication  
Quality of service

## ABSTRACT

This article proposed a hybrid energy-efficient secured quality of service (QoS) based multipath routing protocol. A modified crow search combined with the tunicate swarm butterfly optimisation algorithm (TSBO) with a density-based clustering technique strategy is proposed for the selection of cluster heads after the initial cluster formations. Among all the nodes, the cluster head is selected, and employing the collaborative trust-based approach (CTBA), which employs the trust factor for mobile ad hoc network (MANET) data transmission, a node's authentication is supplied. Finally, to implement the safe routing technique, this article suggested a hybrid multipath routing protocol combining multi-objective grey wolf optimisation (MO-GWO) with a fruit fly algorithm. The NS3 simulator is used to assess the proposed work. The packet delivery ratio metric performs 4% better than the current models. As a result, the suggested approach performs better for the end-to-end delay, energy consumption, packet delivery ratio (PDR), and throughput; it also uses less energy and has a shorter delay. Additionally, single-path nodes with the same energy value have lower throughput than multi-path nodes.

*This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.*



## Corresponding Author:

Veeramani Ramasamy

Department of Computer Science and Engineering, Annamalai University

Annamalai Nagar, Chidambaram, India

Email: gvmani.r@gmail.com

## 1. INTRODUCTION

Mobile ad hoc networks (MANET), the most recent generation of wireless networks, offer a variety of unmatched features, such as a topology that can vary dynamically, a range of transmission, a baseless network, reliability, and a routine method [1], [2]. The formation of a path between the recipient and initiator nodes is necessary for the communication of information between them, and intermediary nodes must be involved. However, an attacker may find it difficult to work on various offensive attack types and is more likely to decline participation in the MANET due to the lack of resources and the mutual presence of the transmission system [3], [4]. Energy efficiency is the key constraint on networks, hence the ad hoc protocol for networks should best combine the needs. The research community is currently focused on the discovery of the multipath to improve single-path difficulties [5]. However, there are no such techniques to improve the aforementioned multipath utilisation issues that are specific to on-demand routing protocols [6]. Networks are mostly constrained by energy conservation [7]. As a result, the ad hoc protocol for the network should balance the requirements. The truth is that the nodes have continued to be in the path even after communication has ended for there to be a connection between them, which indicates that both points of origin and destination are connected by intermediary stations [8]. The malicious node can attack the MANET in a variety of ways, such as by creating false routing information, repeatedly sending bogus messages, and disseminating false connections [9]. In ad hoc networks, the most serious threat is the black hole (BH) assault. A data packet is

directed to itself by using an attacking node during BH attacks when it either intercepts or discards them. Reliable security must be ensured when constructing an ad hoc network [10]. In a "black hole attack," a hostile node pretends to have the network's fastest route to the node being attacked by sending a bogus route response to the original node. Discarding the received packets, it might be handled as a denial of service (DoS) [11]. The secure routing mechanism based on the trust factor with quality of service (QoS) routing-based literature is stated in Table 1.

Table 1. Survey related to energy-efficient trust-based routing protocol

References	Objective	Trust factors	Simulation parameters	Findings	Limitation/future scope
Khan and Gite [12]	Countermeasures using responsive guiding in conjunction with the routing system	Considering the information package, the route request, and the route response, the trust value	Packet delivery ratio, throughputs, and end to end delay (EED)	In terms of throughput reduction, secure ad hoc on-demand distance vector (SAODV) outperforms AODV and the current protocol.	Limited to attacks like man-in-the-middle, eavesdropping, and black hole.
Yamini <i>et al.</i> [13]	Efficient trust establishment-based routing evidence scheme (ETERE)	Probabilistic node misbehaviour detection using I-Trust	Packet delivery ratio, throughputs, and end to end delay	ETERE system increases the network's packet delivery ratio (PDR) and throughput to a maximum of 28% and 34%, respectively.	Updating a secure route in protected routing conditions over a big, wide group of the surrounding area
Bondada <i>et al.</i> [14]	Secure and energy-efficient routing protocol using key cryptography.	Trust factors of MANET networks i.e., distribution key (DK) and calculator key (CK).	Average end-to-end delay, throughput, packet-delivery ratio routing overhead.	Energy use (3.6872%), EED (2.4597%), throughput (2.6246%) and PDR (2.178%) are the values.	Other types of wireless networks, such as vehicular ad hoc networks, can employ the suggested architecture.
Usha and Ravishankar [15]	Energy efficient trust aware routing (NETAR) for AODV traditional protocol	Estimating the rate of trust between neighbours and calculating bandwidth.	End-to-end latency, PDR, throughput and false positive are examples of network link lifetime (NLT) metrics.	PDR-36.53%, 2.15%, average delay is 36.23%, throughput-36.53%, 2.15%, and 23.33% higher.	Robotic prototype-checking techniques are used to verify the system.

To ensure the nodes' degree of trust, the research in [16] attempts to offer novel trust-aware routing in MANET. To address this, a brand-new approach to estimating trust rates according to node power and mobility is presented. To select the optimum trust-aware path for data transfer, the self-improved particle swarm optimisation (SI-PSO) algorithm is suggested. Several factors are taken into account when choosing the best route. A cluster-based algorithm (CBA) is shown in [17] to be more effective than earlier methods for identifying either within-band or out-of-band links. By doing calculations based on the round-trip time (RTT) and some sequences which are used to identify hybrid attacks through wormholes. To boost battery life and network security, the hybrid deep learning prediction (HDLP) wireless network model is presented in [18]. To evaluate the network's resistance to black hole attack, numerous simulated experiments are run. In addition to being simulated, the suggested model is contrasted with earlier models like deep multi-task learning (DMTL) and deep learning based defense mechanism (DLDM). By preventing hostile nodes from connecting during the authentication process and utilising the lightweight resistive mechanism for grey hole attack prediction (LRM-GHA), dependability in attack prediction is achieved [19] by merging the current low-energy adaptive clustering hierarchy (LEACH) with the resistive mechanism. Foreseeing malevolent nodes on the network under specific packet drop assaults requires the resistive mechanism against the grey hole attack.

To defend the network against black hole attacks, allow communication between nodes. Secure dynamic source routing (SEC-DSR), a compact approach that can be used when attackers are present, is provided in [20]. In the routing path, based on the collective wisdom of the participating nodes the host chooses a safe route without any black hole nodes. Nandi and Anusha [21], feature extraction and an ANFIS-based classification model are presented (adaptive neuro-fuzzy inference system). The retrieved feature is trained and then classified using an ANFIS classifier. This research also suggests an spinal muscular atrophy (SMA) integration with AODV protocol named SMA2AODV to identify flooding assaults for MANETs to combat flooding cum energy-conserving routing. Numerous simulated experiments are conducted to assess the network's defence against black hole attacks [22]. Accuracy in attacker detection can be achieved by combining the current LEACH with an additional resisting method. This prevents malicious nodes during the authorization procedure from connecting and using the LRM-GHA [23]. As a result, the multi-objective grey wolf

optimisation algorithm's hybrid multipath routing protocol is provided in the paper. The remaining section of the article is structured as; section 2 provides the recommended approach. Section 3 presents the experimental results and section 4 contains the conclusion.

## 2. METHOD

In the article, an energy-aware trust based multipath routing protocol (EA-TBMRP) based hybrid secure routing system was presented. This protocol makes use of neighbour trust information to select the best secure file transfer path. Several mechanisms evolved to achieve secure routing on MANET. But there is a challenge to satisfying all QoS parameters while achieving enhanced MANET performance. Most of the studies currently in existence lack a secured routing system for handling packet losses, and there is no suitable pre-set mechanism. As a result, a multipath safe trust-based routing system was suggested. The suggested work's block diagram is shown in Figure 1. It introduces the modified crow search strategy for selecting cluster heads as well as the tunicate swarm butterfly optimisation algorithm (TSBOA) density-based clustering technique for cluster creation. To improve network security, the multi-objective grey wolf optimisation (MO-GWO) with fruit fly technique multipath routing protocol is also developed. For node authentication, a cooperative trust-based approach is also recommended.

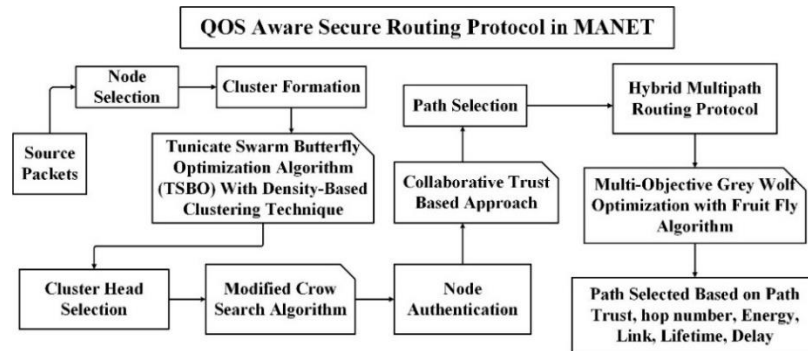


Figure 1. Flow diagram of the proposed work

### 2.1. Cluster formation and selection using TSBOA

This work seeks to build a productive CH selection method using the suggested modified crow search algorithm. However, the TSBOA, is incorporated into the suggested TSBOA density-based clustering technique. Due to the swarming aspect of the optimization process, it offers the ideal solution. The bio-inspired initiative is tunicate swarm algorithm (TSA) which mimics swarm activity and tunicate jet propulsion. It takes into account the two activities of navigation and foraging. All the individuals are grouped based on the gelatinous tunic which is presented in each tunicate. The solution encoding, which is a solution vector representation, uses the objective parameters to identify the cluster's ideal nodes. The CH is selected as the node with the energy, least amount and maximum distance of latency. Das *et al.* [24] for the algorithmic steps of TSBOA. By using parameters such as delay link lifetime, node energy, inter-cluster distance, intra-cluster distance and the projected energy as the objective factors, compute the fitness value which is determined in (1).

$$F = \frac{1}{6} [D^{intra} + (1 - D^{inter}) + G_{cons} + B + (1 - L) + G^p] \quad (1)$$

By selecting the best fitness value, the ideal solution might then be computed by a node with the lowest fitness value. Until the best solution is obtained, the above steps are repeated.

#### 2.1.1. Density-based clustering technique

This work suggested an approach to discovering clusters that exist within a cluster using the density-based clustering method (DBCT). By partitioning the network region into equal-sized layers, subdividing each layer into equal-sized clusters (sub-layers), and combining clusters with other neighbouring clusters, the network lifetime can be greatly extended. Further balancing the energy use among cluster members utilising

the density technique. Additionally, using an effective technique for selecting the cluster heads results in sorting cluster members in a list according to an efficient cluster head.

Pre-processing is an important step before applying the DBCT algorithm. Missing values should be handled in this procedure based on the data set objects, and noise should also be removed. Additionally, until the requirements for homogeneity are not met, the data is split into two or three pieces starting at the entire data set or the highest level. MinPts and Eps will start low and gradually increase throughout the subsequent rounds. Manhattan and Euclidian are the distance units that are employed.

Perform post-processing: this runs a series of iterations to combine these noise spots and combine clusters with the nearby connected cluster that is closest to them. The next objective is to enter the clusters and locate the sub-regions. Because the cluster produced by the first density-based spatial clustering of applications with noise (DBSCAN) is typically less significant, both MinPts and Eps are somewhat raised this time. If any segments are noisy, they can be made to join with their nearest neighbouring cluster.

### 2.1.2. Crow search optimization algorithm

The modified crow search technique is used for selecting the cluster head. The following describes the specific steps which make the proposed crow search optimization algorithms (CSOA's) working procedure in detail. The optimisation problem is identified in the first stage, together with the decision and constraints variables. The adjustable factor values' probability awareness are flight length ( $FL_{Length}$ ), fock size  $F_{Size}$ , and  $A_p$ , maximum iteration count ( $\max\_Iter$ )<sub>COUNT</sub> are also assigned and it is employed in the optimization problem. A two-dimensional size matrix is created in the second stage where,  $F_{Size}$ ,  $N_{Dec-var}$  and  $F_{Size} \times N_{Dec-var}$  relates to the number of crows (mobile nodes) and the number of decision variables (the dynamic variables that influence the choice of the cluster head).

The cumulative energy approach is used to determine the fitness function's value. A potential mobile node is selected randomly from the search space by the crow search agent (search process) in this case if the value is higher than the value of the randomly generated number. If not, from any crow flock  $C^f$  (clusters of sensor nodes) the search agent  $C^j$  randomly select the crow (mobile node). Additionally, the search agent is responsible for locating real nodes for sensors, that have the potential in all factors considered when selecting the cluster head, for pursuing  $C^f$ . Therefore, (2) is applied to determine the new location of the cluster's main sensor node.

$$C^{i+1,t+1} = C^{i,t} + rn_i * FL_{Length}^{i,t} * (C^{f,t} - C^{i,t}) \quad (2)$$

Where,  $rn$  and  $t$  related to the number of implementation iterations and the random quantity produced during the process. The fitness values of the mobile nodes placed in the recently modified location by (2) were calculated. As a result, the fitness indicator of the most recent update to the sensor node's position is contrasted with the health value of the sensor nodes' position that was first evaluated, and if the latter one is superior, the most recently maintained sensing node location is updated in memory for further iterations.

## 2.2. Node authentication with collaborative trust-based approach

Security is a significant issue for secure routing in MANE and delivering QoS since hostile nodes present in the network present all potential risks to that network. A collaborative trust based approach (CTBA) that leverages the trust factor by neighbour observations and combining directly to build the resultant combining trust provides node authentication before beginning the route discovery process for resulting in MANET data transmission. A malicious node gives the packet incorrect information in an attempt to insert itself into the path. The cooperation of its neighbours successfully isolates the rogue node. The data must first be decoded to make the appropriate changes to the original data, after which it must be recomputed. It cannot recompute the MAC because it is not aware of the private key for the accused node. Since no attempt has been made to alter the information. Since the nodes receiving the warning messages are unable to decode the MAC utilising the erroneous node's private key, malicious behaviors is discovered. Using its private key, a node deceives another by altering the data it received from the latter, and then recalculating the MAC. Since the neighbouring nodes get the alert messages which are unable to utilise the private key of the accused node, decrypt the MAC, additionally, behaviour is seen when a node accuses another node without proof and uses a different node's MAC than the one that is being accused. Direct, indirect, and overall trust ratings, which make up the three types of trust ratings in this study, are all beneficial for enhancing communication security. The required final way is selected based on hop number, path trust, and energy consumption, and a safe routing technique is then obtained as effectively as possible.

### 2.3. Hybrid multipath routing using multi-objective grey wolf optimization

To achieve QoS-conscious energy-efficient multi-path routing in MANET, the multi-objective grey wolf optimization (MO-GWO) with fruit fly algorithm (MO-GWFFA) is proposed in this work as a hybrid multipath routing protocol. The primary goal of this work is to formulate objective functions for route optimisation in MANET based on the energy, delay, lifetime, trust, and connection quality factors as multiple MO-GWO objectives. This hierarchy serves as the foundation for the optimisation process, which is developed based on the hunting habits of each wolf pack. Prey enrichment, hunting, prey hunting, and prey searching are all included in the mathematical models.

Encircling prey: grey wolves surround their prey when hunting, which can be stated mathematically as:

$$\vec{X}(K+1) = \vec{X}(K) - \vec{A} \cdot \vec{D}, \vec{D} = |\vec{C} \cdot \vec{X}_p(k) - \vec{X}(K)| \quad (3)$$

where  $(X)$  is a grey wolf's location vector and  $\vec{X}_p$  is the position vector of the prey. The equation in (4) and (5) can be used to determine the coefficient vectors, which are shown in  $\vec{A}$  and  $\vec{C}$ , respectively. The difference vector is denoted by  $D$ , and the current iteration is expressed by  $k$ .

Hunting: the positions of the prey are better known as alpha, beta, and delta. The search agents intended by the top three rankings after the other search agents have been updated. In (4) and (5) provide a statistical representation of the hunting behaviour.

$$\vec{D}_\alpha = |\vec{C}_1 \cdot \vec{X}_\alpha - \vec{X}| \quad \vec{D}_\beta = |\vec{C}_2 \cdot \vec{X}_\beta - \vec{X}| \quad \vec{D}_\delta = |\vec{C}_3 \cdot \vec{X}_\delta - \vec{X}| \quad (4)$$

$$\vec{X}_1 = \vec{X}_\alpha - \vec{A}_1 \cdot (\vec{D}_\alpha) \quad \vec{X}_2 = \vec{X}_\beta - \vec{A}_2 \cdot (\vec{D}_\beta) \quad \vec{X}_3 = \vec{X}_\delta - \vec{A}_3 \cdot (\vec{D}_\delta) \quad (5)$$

Here the  $\vec{X}_\alpha$ ,  $\vec{X}_\beta$ , and  $\vec{X}_\delta$  are the optimal position vectors of  $\vec{X}_1$ ,  $\vec{X}_2$ , and  $\vec{X}_3$  grey wolves respectively. The first component is preserved for storing and holding non-dominated Pareto optimisation results. Especially, a sort of storage called an archive allows users to keep or retrieve non-dominated Pareto optimal solutions. A leader selection is the second element method, which is in charge of determining the best three options (a, b, and d) as the leaders of the hunting process from the archive. The search space's least congested areas were selected using the leader selection component. A roulette-wheel approach, which can be stated as follows, is used to calculate the selection probability.

$$P_i = \frac{c}{N_i} \quad (6)$$

Where, a constant number ( $> 1$ ) is denoted by  $c$ , and the segment  $i$  is a number of the best optimal solution is  $N$ . The multi-objective GWO method is ideally combined with the fruit fly algorithm for QoS-aware routing in the proposed multi-objective GWFFA model to improve routing performance based on QoS parameters.

#### 2.3.1. Fruit fly optimization algorithm

This technique, which discovers the optimum path based on the fitness value (smell concentration) estimated between the nodes depending on the distance, is used for efficient data transportation. Initially, to choose the best route, the fewest number of hops paths are calculated, followed by the greatest overall fitness value along those paths. The shortest path (since the fitness value is based on the distance) is considered to select which best path, it minimizes energy consumption and it also improves the data delivery performance.

The following necessary steps are describing the fruit fly characteristics of searching for a source node which is described in [25]. The random initial position of a mobile sink is in (0, 0) coordinates such that,

$$Init X_{axis} = 0; Init Y_{axis} = 0 \quad (7)$$

the regulated direction of the mobile sink and the distance of the source search were determined by each CH individual's fitness score. The path that the mobile sink takes to gather data towards the spot and the best smell concentration value are both maintained using the fitness value. Enter into iterative optimization for every mobile sink's position, in a controlled manner, it moves along the sensor field. The suggested optimisation technique is fruit fly for optimal path selection (shortest path), based on the fitness value and hop count, improving the data delivery performance while minimising the delay as compared to the prior algorithms.

### 3. RESULTS AND DISCUSSION

The proposed research is simulated based on the Ns-3 simulator. The proposed optimization technique for multipath selection's experimental findings is presented in this section, along with a MANET simulation environment. This section also describes the analysis of the suggested algorithm and their comparison analysis based on performance metrics and in the selection of the weighted constants for the best network performance.

Table 2 represents the parameters of the simulation configuration. The proposed work is simulated using the Ns-3.33 tool, their simulation time is 8 seconds, and the number of nodes is 40. Accordingly, the simulation area for this work is 500\*500 meters, the mobility speed is 5 m/sec, and the transmission range is 27 m. However, the average end-to-end delay (E-to-E Delay), average delay, packet delivery fractions (PDF), and throughput are the parameters employed for evaluating performance and comparison results.

Table 2. NS3 simulation parameters

Simulation system configuration	
Simulation tools	Ns-3.33
Simulation time	8 seconds
Number of nodes	40
Simulation area	500*500 meter
Mobility speed	5 m/sec
Transmission range	27 meter

In terms of PDR and packet dropped ratio, the malicious nodes' proportions are depicted in Figure 2. Figure 2(a) depicts the PDR from the percentage of malicious nodes. In modified self-adaptive sailfish optimization (MSA-SFO), the PDR decreases from 88% to 40%, NETAR reduces from 80% to 32%, and ETERE (I-Trust) decreases from 78% to 29%. However, the proposed MO-GWFFA only decreases from 93% to 60%, due to a smaller drop ratio (using the strong link). Figure 2(b) shows the packet dropped comparison with existing methods. However, compared to this method, the proposed method has less packet drop percentage of 51%, respectively.

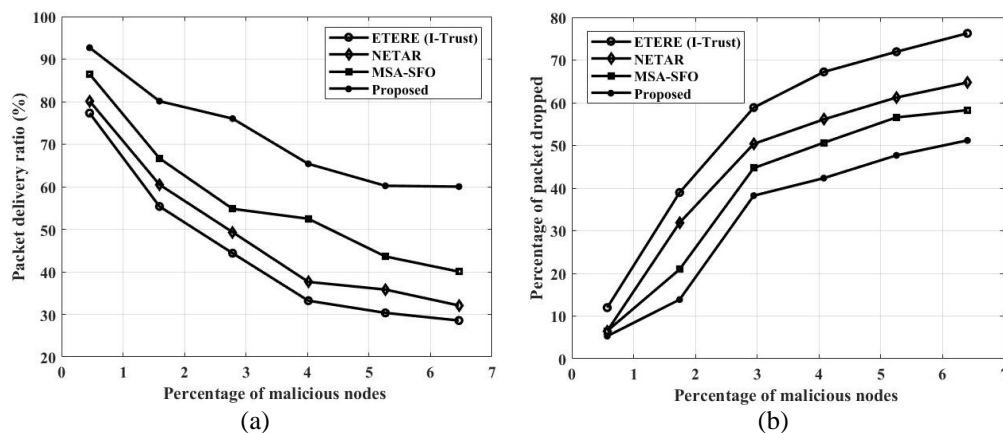


Figure 2. Existence of malicious nodes analyse (a) packet delivery and (b) packet dropped ratio

The performance and comparative analysis results for the presented MO-GWFFA are presented in Figure 3 in terms of E-to-E delay, which is compared with the existing routing models. Figure 3(a) illustrates the comparison graph with network size, here for node 120, the MO-GWFFA model attains the value of 1.89 s in terms of E-to-E delay, which is 4%, 4.1%, as well as 6% lower than existing models. Based on the low computation time in the shortest path selection, the efficiency of the work is improved by optimally reducing the delay. Figure 3(b) depicts the comparison results for E-to-E delay with malicious nodes. In the x-axis, the number of malicious nodes ranges from 0 to 9 and in the y-axis, the E-to-E delay metric is presented in seconds (s). Compare to the ETERE (I-Trust) model, the proposed model has 37% less E-to-E delay for malicious node 9. For providing optimal routing performance, the traffic is reduced and consequently, the delay is decreased by using the effective routes selection with balanced multi-path routing.

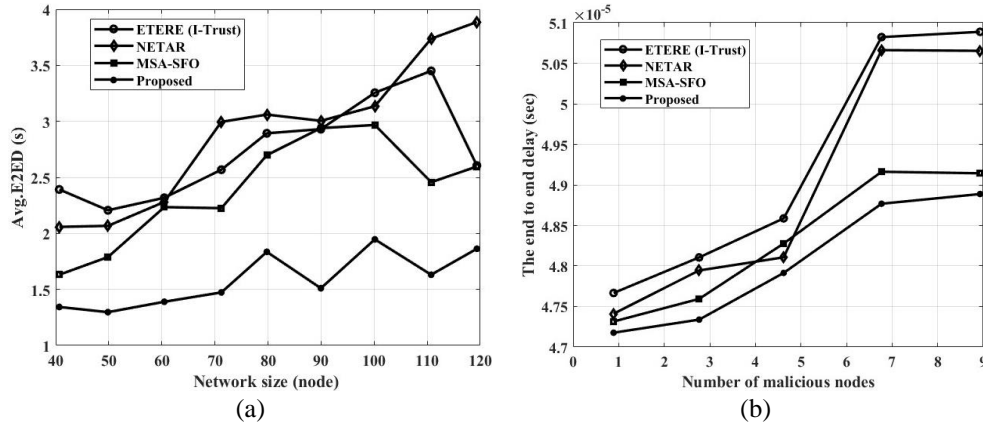


Figure 3. Average end-to-end delay analysis with (a) network size and (b) malicious nodes

Figure 4 reveals the comparative analysis of two energy-aware performance metrics. Figure 4(a) reveals the false positive analysis with existing techniques. The proposed method has less false positive values of 3.2, however, the other existing algorithm ETERE (I-Trust), NETAR, and MSA-SFO have 4.51, 4, and 3.2, respectively. Figure 4(b) depicts the throughput comparison in terms of network size. The simulation outcomes indicate that the maximum throughput of 0.94 kbps is attained by the suggested method than the existing techniques.

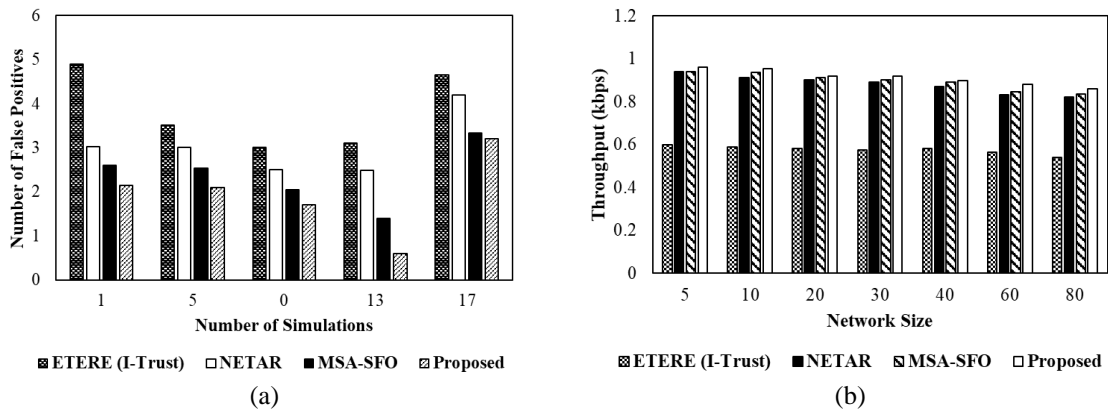


Figure 4. Comparison analysis graph for (a) false positive and (b) throughput

The values for PDR are presented in Table 3, it presents the existing ETERE (I-Trust), NETAR, MSA-SFO methods, and proposed method values. The existing technique analyses the packet ratio under various pause times (from 5 to 350 seconds). When compared to the other two techniques, ETERE (I-Trust) has the lowest packet ratio. Subsequently, for the proposed method, it obtained the highest packet ratio of 0.93. However, from this table, the proposed method values for PDR are approximately 4% higher than these existing methods.

Table 3. Comparison analysis of packet delivery ratio with pause time

Pause time (sec)	ETERE (I-Trust)	NETAR	MSA-SFO	Proposed
5	0.51	0.78	0.795	0.84
25	0.58	0.786	0.8	0.84
50	0.599	0.81	0.816	0.86
75	0.61	0.83	0.829	0.87
100	0.615	0.84	0.86	0.88
150	0.62	0.834	0.87	0.89
250	0.62	0.84	0.88	0.90
300	0.624	0.86	0.894	0.92
350	0.63	0.87	0.92	0.93

The comparative results for energy consumption performance parameters are portrayed in Figure 5. The relative study of energy consumption with previous techniques is presented in Figure 5(a). It portrayed that the suggested hybrid multipath routing protocol of MO-GWO with the fruit fly method achieves a lower energy consumption value than the other methods as 0.12 m joules. Figure 5(b) indicates the result of the jitter with various routing protocols. As MO-GWFFA gives an abrupt rise in delay as 40, it is less than the jitter values of the other methods and subsequently, because of the route changes in the network due to the breakage of the link, it provides a constant delay and this delay occurs because of the new route selection, respectively.

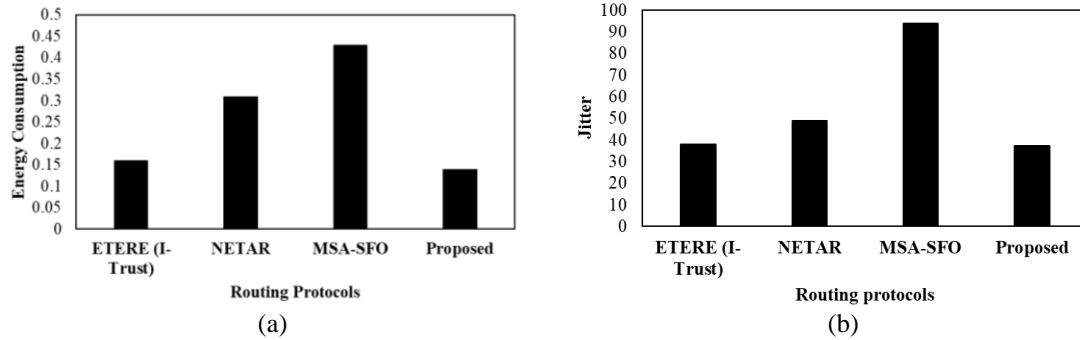


Figure 5. Comparison Analysis for (a) energy consumption and (b) Jitter

Figure 6 depicts the black hole attack analysis with the proposed technique. The control packet overhead graph for the black hole attack is presented in Figure 6(a). This figure depicted that the proposed method has less control packet overhead than the other existing ETERE (I-Trust), NETAR, and MSA-SFO. Accordingly, compared to these methods, the proposed method has approximately 7% higher than these existing methods, respectively. Figure 6(b) illustrates the attack impact on energy consumption in the proposed technique. This shows that by increasing the black hole attacks from 0 to 20, the proposed work gains lower consumption of energy than the other existing methods. The figure showed that the suggested method practices less control packet overhead and that the MO-GWFFA used 170 (J) less energy than the previous models by 3%, 4.5%, and 6% respectively.

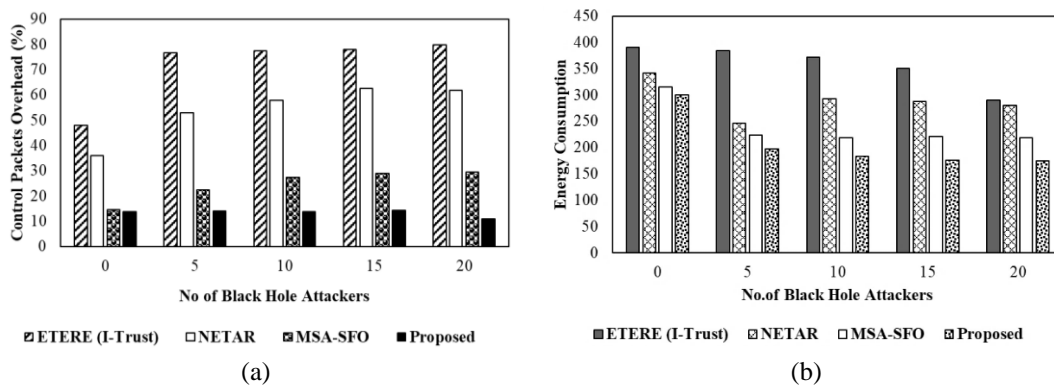


Figure 6. Performance analysis for black hole attackers (a) control packets overhead and (b) energy consumption

#### 4. CONCLUSION

The QoS-aware energy-efficient routing protocol is presented with MO-GWO fruit fly algorithm using multi-path trust-based routing. The suggested work was evaluated via simulations using the Ns-3 simulator. The findings outline that the proposed strategy beats others in terms of enhanced PDR, network security, and network lifetime. The results of the overall analysis showed that the recommended technique increases both the PDR and the trust level. Several performance metrics, including packet loss rate, PDR, energy consumption, jitter, E-to-E delay, routing overhead, throughput, and detection rate are used to evaluate the proposed approach. The suggested method performance is 3.5% and 5% high for PDR and E-to-E delay







when compared with the other previous techniques. However, PLR and energy consumption of the work are 2.5% and 7% higher than the existing methods. The outcome shows that the suggested strategy works better than other cutting-edge approaches. To discover node misbehaviour assaults like the black hole attack, the suggested approach employs the safe routing procedure. The suggested strategy also achieves a higher trust level and packet delivery ratio.





## REFERENCES

- [1] R. Thillaikarasi and S. M. S. Bhanu, "Adaptive DSR to mitigate packet dropping attacks in WMNs using cross layer metrics," *Journal of Ambient Intelligence and Humanized Computing*, Apr. 2021, doi: 10.1007/s12652-021-03233-6.
- [2] K. Ourouss, N. Naja, and A. Jamali, "Defending against smart grayhole attack within MANETs: a reputation-based ant colony optimization approach for secure route discovery in DSR protocol," *Wireless Personal Communications*, vol. 116, no. 1, pp. 207–226, Jan. 2021, doi: 10.1007/s11277-020-07711-6.
- [3] M. Thebiga and R. S. Pramila, "A new mathematical and correlation coefficient based approach to recognize and to obstruct the black hole attacks in manets using DSR routing," *Wireless Personal Communications*, vol. 114, no. 2, pp. 975–993, Sep. 2020, doi: 10.1007/s11277-020-07403-1.
- [4] S. Naveena, C. Senthilkumar, and T. Manikandan, "Analysis and countermeasures of black-hole attack in MANET by employing trust-based routing," in *2020 6th International Conference on Advanced Computing and Communication Systems, ICACCS 2020*, Mar. 2020, pp. 1222–1227, doi: 10.1109/ICACCS48705.2020.9074282.
- [5] F. H. Shajin and P. Rajesh, "Trusted secure geographic routing protocol: outsider attack detection in mobile ad hoc networks by adopting trusted secure geographic routing protocol," *International Journal of Pervasive Computing and Communications*, vol. 18, no. 5, pp. 603–621, Nov. 2022, doi: 10.1108/IJPC-09-2020-0136.
- [6] A. K. Bairwa and S. Joshi, "MLA-RPM: a machine learning approach to enhance trust for secure routing protocol in mobile ad hoc networks," *International Journal of Advanced Science and Technology*, vol. 29, no. 4, pp. 11265–11274, 2020.
- [7] V. Gomathy, N. Padhy, D. Samanta, M. Sivaram, V. Jain, and I. S. Amiri, "Malicious node detection using heterogeneous cluster based secure routing protocol (HCBS) in wireless adhoc sensor networks," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 11, pp. 4995–5001, Nov. 2020, doi: 10.1007/s12652-020-01797-3.
- [8] U. Hariharan, K. Rajkumar, and T. Akilan, "Detection of mischievous node in wireless ad-hoc sensor networks using HCBS routing protocol," in *Proceedings of the 3rd International Conference on Intelligent Sustainable Systems, ICISS 2020*, Dec. 2020, pp. 1131–1135, doi: 10.1109/ICISS49785.2020.9315952.
- [9] A. S., "Prevention of routing attacks using trust-based multipath protocol," *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 9, no. 3, pp. 4022–4029, Jun. 2020, doi: 10.30534/ijatcse/2020/227932020.
- [10] S. Nandgave-usturge, "Water spider monkey optimization algorithm for trust-based MANET secure routing in IoT," *International Journal of Scientific Research & Engineering Trends*, vol. 6, no. 2, pp. 980–984, 2020.
- [11] J. Lyu, C. Chen, and H. Tian, "Secure routing based on geographic location for resisting blackhole attack in three-dimensional VANETs," in *2020 IEEE/CIC International Conference on Communications in China, ICC 2020*, Aug. 2020, pp. 1168–1173, doi: 10.1109/ICCC49849.2020.9238997.
- [12] I. Khan and P. Gite, "Detecting and predicting malicious nodes in mobile ad-hoc networks using a secure technique," *International Journal of Computer Applications*, vol. 184, no. 3, pp. 15–19, 2022, doi: 10.5120/ijca2022921988.
- [13] K. A. P. Yamini, J. Stephy, K. Suthendran, and V. Ravi, "Improving routing disruption attack detection in MANETs using efficient trust establishment," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 5, 2022, doi: 10.1002/ett.4446.
- [14] P. Bondada, D. Samanta, M. Kaur, and H. N. Lee, "Data security-based routing in MANETs using key management mechanism," *Applied Sciences (Switzerland)*, vol. 12, no. 3, 2022, doi: 10.3390/app12031041.
- [15] M. S. Usha and K. C. Ravishankar, "Implementation of trust-based novel approach for security enhancements in MANETs," *SN Computer Science*, vol. 2, no. 4, p. 257, Jul. 2021, doi: 10.1007/s42979-021-00628-2.
- [16] S. Haridas and A. R. Prasath, "Trust aware secure routing model in MANET: self-improved particle swarm optimization for optimal route selection," *IFIP Advances in Information and Communication Technology*, vol. 651 IFIP, pp. 193–212, 2022, doi: 10.1007/978-3-031-11633-9\_15.
- [17] K. N. V. R. Kumar, R. Mahaveerakannan, C. M. Rao, P. N. Rao, and K. S. Rao, "Intrusive Detection of wormhole attack using cluster - based classification model in MANET," in *8th International Conference on Advanced Computing and Communication Systems, ICACCS 2022*, Mar. 2022, pp. 1869–1874, doi: 10.1109/ICACCS54159.2022.9785233.
- [18] D. Joon and K. Chopra, "Hybrid deep learning prediction model for blackhole attack protection in wireless communication," *Natural Volatiles and Essential Oils Journal (NVEO)*, vol. 8, no. 4, pp. 10228–10243, 2021.
- [19] C. Gowdham and S. Nithyanandam, "Modeling of an efficient lightweight resistive mechanism for gray hole attack prediction in wireless sensor networks," *NVEO-NATURAL VOLATILES & ESSENTIAL OILS Journal| NVEO*, vol. 8, no. 5, pp. 1821–1843, 2021.
- [20] M. Mohanapriya, N. Joshi, and M. Soni, "Secure dynamic source routing protocol for defending black hole attacks in mobile ad hoc networks," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 21, no. 1, pp. 582–590, Jan. 2021, doi: 10.11591/ijeecs.v21.i1.pp582-590.
- [21] M. Nandi and K. Anusha, "An optimized and hybrid energy aware routing model for effective detection of flooding attacks in a manet environment," *Wireless Personal Communications*, vol. 127, no. 3, pp. 2515–2533, Dec. 2022, doi: 10.1007/s11277-021-09079-7.
- [22] D. N. Tej and K. V. Ramana, "MSA-SFO-based secure and optimal energy routing protocol for MANET," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 6, pp. 306–313, 2022, doi: 10.14569/IJACSA.2022.0130638.
- [23] D. Ramachandran, V. R. Ratna, R. P. T. Vasanth, I. Garip, and K. Umamahesawari, "A low-latency and high-throughput multipath technique to overcome black hole attack in mobile ad hoc network (MTBD)," *Security and Communication Networks*, 2022, doi: 10.1155/2022/8067447.
- [24] A. Das, "Designing green IoT communication by adaptive spotted hyena tunicate swarm optimization-based cluster head selection," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 11, Nov. 2022, doi: 10.1002/ett.4595.
- [25] S. M. Darwish, A. Elmasry, and S. H. Ibrahim, "Optimal shortest path in mobile ad-hoc network based on fruit fly optimization algorithm," in *The International Conference on Advanced Machine Learning Technologies and Applications (AMLTA2019)*, vol. 921, 2020, pp. 91–101, doi: 10.1007/978-3-030-14118-9\_10.





**BIOGRAPHIES OF AUTHOR**

**Veeramani Ramasamy**     is a research scholar in the Department of Computer Science and Engineering at Annamalai University, Chidambaram Tamil Nadu. He completed her Bachelor of Engineering in Computer Science and Engineering from the University of Madras, Chennai and a Master of Engineering in Computer Science and Engineering from Annamalai University, Chidambaram. His research areas of interest include wireless networks, cloud computing, IoT, and artificial intelligence. Moreover, he is a member of the Indian Science Congress and the Association for Computing Machinery (ACM). He can be contacted at email: gvmani.r@gmail.com.



**Dr. Madhan Mohan Ramalingam**     is currently working as an Associate Professor in the Department of Computer Science and Engineering at Annamalai University, Chidambaram, Tamil Nadu. He received his B.E. from the University of Madras, Chennai and his M.E. from Annamalai University, Chidambaram. He obtained his Ph.D. from Annamalai University, Chidambaram. His research interests include networking routing, distributed computing and network security. He has published his research in many journals and conferences. He can be contacted at email: madhanmohan\_mithu@yahoo.com.



**Dr. Mahesh Chitraivel**     working as a Professor and Heading the Department of Information Technology, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, India. He has more than 22 years of experience as an academician and 12 years in research. His research areas are data mining, image processing, bio-informatics, and machine learning. He has produced six Ph.D. candidates and currently Guiding 8 research scholars. He has published more than 30 articles in various Scopus-indexed and SCI journals. He can be contacted at email: chimahesh@gmail.com.