Journal of Information Systems Engineering and Management
2025, 10(38s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Optimizing Manet Routing in Iot with Antlion Grey Wolf Hybrid Approach Enhancing Energy Efficiency, Trust, Stability, and Bandwidth

[1*]P. Yuvaraja and [2]Dr. P. Suganthi
[1]Research Scholar, Department of Computer Science, Namakkal Kavingnar Ramalingam Government Arts College for Women, Thillaipuram, Namakkal, Tamil Nadu 63700. India.*
Email: psyuvaraja.p@gmail.com
[2]Associate Professor and Head,
Department of Computer Science, Namakkal Kavingnar Ramalingam Government Arts College for Women, Thillaipuram, Namakkal, Tamil Nadu 63700. India.
Email: mail: kpsuganthi74@gmail.com
[1]Corresponding author mail: psyuvaraja.p@gmail.com*

ARTICLE INFO

Received: 18 Dec 2024

Revised: 10 Feb 2025

Accepted: 28 Feb 2025

ABSTRACT

Wireless Sensor Networks (WSN) act as a vital link between the physical and information networks in the Internet of Things (IoT). Energy efficiency and trustworthiness are key factors in ensuring reliable communication in these networks. During multicast routing, the Base Station (BS) is responsible for securely transmitting data to multiple destinations via intermediate nodes, which is a significant challenge in IoT and Mobile Ad-hoc Networks (MANET). An energy-conscious multicast routing system that combines Antlion Optimization (ALO) and Grey Wolf Optimization (GWO) is presented in this paper: the Antlion Grey Wolf Energy-Trust Pathway (ALGWO-ETP). It makes use of an objective function that assesses bandwidth, energy, trust, and link stability. In order to guarantee safe and effective node selection, routes are created and optimized using these parameters, with energy and trust levels updated following each transmission. To further enhance security and routing efficiency, the protocol is augmented with the Improved Salp Swarm Algorithm (ISSA) and Elliptic-curve Cryptography (ECC). The ISSA evaluates and selects the most secure and efficient multiple paths, optimizing routing decisions based on node energy and trustworthiness. Meanwhile, the ECC mechanism secures data transmission by validating node keys and shared codes, ensuring that only legitimate nodes participate in the network. This process enhances communication reliability and efficiency in the network. The proposed model was evaluated through extensive simulations in MATLAB, comparing its performance against existing techniques. The simulations, conducted with networks of 50 and 100 nodes, demonstrated significant improvements in minimal delay, maximum detection rate, energy efficiency, bandwidth utilization, and throughput.

Keywords: WSN; IoT; MANET; ALGWO-ETP; ALO; GWO.

1. INTRODUCTION

In the rapidly evolving landscape of the IoT, the integration of MANET has emerged as a significant advancement in enhancing connectivity and communication between various IoT devices. MANET are decentralized networks where nodes (devices) communicate directly with each other without relying on a fixed infrastructure [1, 2]. This characteristic makes MANETs particularly suitable for IoT applications, where devices often operate in dynamic, unpredictable environments and require flexible, self-organizing communication solutions [3, 4]. In the IoT, optimizing MANET routing is crucial due to the diverse and often challenging scenarios these networks encounter. IoT devices are frequently deployed in environments such as smart cities, industrial automation, healthcare, and environmental monitoring, where they must communicate effectively despite constraints like limited power, variable network density, and frequent node mobility [5]. The efficiency of routing protocols directly impacts the overall performance of the IoT network, influencing factors such as data transmission speed, energy consumption, and network reliability. Optimizing routing in MANETs involves addressing several intrinsic challenges [6].

First, the dynamic nature of MANET, characterized by the constant movement of nodes and fluctuating network topologies, can lead to frequent route changes and interruptions. Traditional routing protocols, designed for static or less mobile networks, may struggle to adapt to these conditions, resulting in increased latency, packet loss, and overall inefficiency [7]. Second, IoT devices often have limited computational resources and power constraints. Efficient routing protocols must balance the need for rapid, reliable data transmission with the energy consumption of the devices, as prolonged high energy expenditure can lead to reduced network longevity and device failures. Third, the scalability of routing protocols is another critical consideration [8]. As the number of devices in an IoT network grows, routing protocols must handle increased traffic and complexity without degrading performance. Scalability challenges can manifest as increased overhead, reduced throughput, or longer delay times [9]. Recent advancements in MANET routing for IoT focus on addressing these challenges through various optimization strategies. One approach is the development of adaptive routing protocols that dynamically adjust to changes in the network topology [10]. These protocols use real-time data to optimize route selection and minimize disruptions caused by node mobility. Another strategy involves leveraging machine learning and artificial intelligence to enhance routing efficiency [11]. Machine learning algorithms can analyze network conditions and predict optimal routes based on historical data and current network metrics. This proactive approach helps in anticipating potential issues and adapting routing decisions accordingly.

Additionally, energy-efficient routing protocols have been designed to minimize power consumption while maintaining network performance [12, 13]. These protocols prioritize routes that conserve energy and extend the operational life of IoT devices, balancing the trade-off between energy use and data transmission requirements. MANET, characterized by dynamic and autonomous node movement, face challenges in routing optimization for IoT applications [14]. Key concerns include energy efficiency due to battery limitations, ensuring trust in unreliable nodes, maintaining stability amidst frequent topology changes, and optimizing bandwidth usage. Addressing these issues requires innovative approaches, such as energy-aware protocols, trust-based models, stability-enhancing algorithms, and adaptive bandwidth management. Integrating these strategies helps develop robust routing solutions that improve performance, reliability, and efficiency in IoT networks [15]. Optimizing MANET routing in IoT is essential for enhancing the performance, reliability, and longevity of interconnected devices. Addressing the inherent challenges of dynamic topologies, resource constraints, and scalability requires innovative approaches and continuous advancements in routing protocols. As IoT applications continue to grow and evolve, the development of efficient and adaptive MANET routing solutions plays a pivotal role in ensuring seamless and effective communication across diverse and complex network environments.

The contributions of this paper are manifested below,

- This work introduces the ALGWO-ETP, a novel multicast routing protocol that combines ALO and GWO. This hybrid approach enhances routing efficiency and security in WSN and MANET.
- The ALGWO-ETP protocol incorporates an objective function that considers energy, trust, link stability, and bandwidth. This comprehensive evaluation ensures more balanced and effective routing decisions, improving overall network performance.
- The protocol dynamically updates nodes energy and trust levels during data transmission, ensuring that routing paths remain secure and efficient. This adaptive mechanism enhances communication reliability by selecting optimal nodes based on current network conditions.

This paper is further divided into the following sections. The part 2 presents both related works and problem statement. The suggested method is implemented and illustrated in the part 3. The result and discussion are then presented in the part 4, followed by the conclusion in the part 5.

2. LITERATURE REVIEW

In 2024, Naveen and Prathap [16] introduced a three-stage selection process for cluster heads (CH), clone CH (CCH), and direct nodes (DN) to optimize network performance. By considering multi-objective QoS constraints such as residual energy, latency, throughput, and distances the HCM-DSO algorithm demonstrates superior network lifetime and performance in extensive experiments compared to existing protocols. To maximize cluster selection in WBAN, Saleem et al. created a metaheuristic method in 2021 that uses the Ant Lion Optimizer (ALO). In terms of energy efficiency for routing protocols, ALO fared better than more conventional techniques like Ant Colony Optimization, Grasshopper Optimization, and Moth Flame Optimization. In order to improve safe routing in Vehicular Ad-hoc Networks (VANETs), Kaur and Kakkar presented a unique AI-based hybrid optimization technique in 2024 that combines Rider Optimization and Remora Optimization. Although trust-based security methods are more straightforward and economical, they frequently lack the variety and flexibility required in dynamic settings. By optimizing routing according to trust, energy, latency, and distance, the suggested method overcomes these difficulties.

Cluster-based routing protocols (CBRPs), created especially for Flying Ad-Hoc Networks (FANETs), were introduced by Abdulhae et al. in 2022. With an emphasis on topology, scalability, clustering techniques, and routing metrics, their thorough analysis assesses the advantages and disadvantages of 21 distinct CBRPs. The report identifies open issues and makes recommendations for future directions in UAV network routing protocol development. A new cluster head selection approach that improves network lifespan and energy efficiency was presented by Dattatraya and Rao (2022). Glowworm Swarm Optimization and Fruitfly Optimization are combined in their Fitness-based Glowworm Swarm with Fruitfly Algorithm (FGF). Comparisons with current techniques showed better results in terms of energy efficiency and node survival.

In 2024, Kaviarasan and Srinivasan presented a routing method for effective cluster head (CH) selection that makes use of the Adaptive Remora Optimization method (AROA). This technique improves network lifetime and lowers energy consumption in Wireless Sensor Networks (WSNs) by optimizing energy consumption, distance, throughput, Packet Delivery Ratio (PDR), and route loss. The Optimal Energy and Bandwidth-based Link Stability Routing (OEBLS) method was presented by Kothandaraman et al. (2022). It improves route stability by maximizing throughput and reducing error rates. The program evaluates routes by taking node distance, velocity, and residual energy into account, as well as link stability, energy, and bandwidth. A power management plan was created by Krishnan et al. (2022) to improve energy efficiency in mobile ad hoc networks (MANETs). By detecting and replacing unreliable cluster heads, this approach aims to enhance communication and data collecting. For efficient cluster head management, they suggested a self-configurable cluster mechanism based on the k-means algorithm. A multi-objective optimization technique was employed by Mishra et al. (2021) to improve WSN performance by reducing energy usage. Their two-step strategy uses a hybrid Particle Swarm Optimization (PSO) and Genetic Algorithm (GA) for route optimization after first choosing cluster heads using a trust concept. An adaptive Multipath Multichannel Energy Efficient (MMEE) routing technique was presented by Chandravanshi et al. (2022). It chooses routes by taking into account available bandwidth and predicted energy usage. MMEE reduces collisions and balances load by using numerous pathways and sub-channels.

2.1. Problem Statement

In WSN and MANET, multicast routing presents significant challenges, particularly in the IoT. These networks often consist of numerous battery-powered nodes that require efficient energy management to maintain longevity and performance. Additionally, nodes can exhibit varying degrees of trustworthiness, which affects the reliability and security of data transmission. The dynamic nature of node mobility and changes in network topology further complicates the routing process, leading to potential issues with route stability and bandwidth utilization. Traditional multicast routing protocols frequently overlook the complex interplay between energy efficiency, trust, stability, and bandwidth. This oversight can result in suboptimal performance, including excessive energy consumption, unreliable data paths, and inefficient bandwidth usage. Furthermore, existing solutions may not adequately address the real-time updates needed for maintaining optimal routes as network conditions change. Therefore, there is a pressing need for a robust multicast routing protocol that integrates energy-awareness and trust mechanisms while optimizing link stability and bandwidth utilization. Such a protocol must adapt to dynamic network conditions and ensure reliable, efficient communication across varying network sizes and topologies.

3. PROPOSED METHODOLOGY

The goal of multicast routing is to efficiently distribute data to multiple recipients. This article proposes the ALGWO-ETP optimization technique, which assesses mobile nodes in the IoT network based on their energy and trust levels. Secure nodes are identified, and the enhanced ALGWO-ETP method is applied to select the optimal routes. Data is transmitted over the chosen path, with the energy and trust levels of nodes updated after each transmission to ensure continuous selection of secure and efficient routes. This update ensures that secure node selection continues effectively for subsequent rounds, maintaining efficient routing. Key evaluations also include Link Stability and Bandwidth Assessment to further refine route selection. Fig. 1 depicts the overall proposed methodology.

3.1. Initialization

In the wireless network optimization, initialization is the critical first step where the network's nodes are evaluated and prepared for the routing process. This phase ensures that the network's resources are effectively utilized and that the routing paths selected are both efficient and reliable.

3.1.1. Node Assessment

Energy Levels: The initial energy levels of each node are evaluated to identify those with the highest remaining power. Nodes with higher energy levels are more desirable for routing because they are less likely to deplete their power reserves quickly, which helps extend the overall network lifespan.

Trust Scores: Trust scores are calculated for each node to assess their reliability. This score is based on historical data, including successful transmissions and the node's behavior in avoiding malicious activities. Nodes with higher trust scores are considered more secure, making them preferable for routing, as they help maintain the confidentiality and integrity of the data being transmitted.

Link Stability: The stability of the links between nodes is analyzed to determine which connections are less likely to break due to factors such as node mobility or environmental interference. Stable links are prioritized to ensure continuous and reliable communication, reducing the risk of data loss or transmission delays.

Bandwidth: The available bandwidth of each node is measured to ensure that the selected nodes can handle the expected data load without causing network congestion or delays. Nodes with higher bandwidth are preferred to support faster and more efficient data transmission.

3.1.2. Objective Function Setup

After assessing the nodes, an objective function is defined to guide the optimization process. This function integrates the metrics of energy levels, trust scores, link stability, and bandwidth. The objective function aims to balance these factors to identify the most optimal nodes for routing. Specifically:

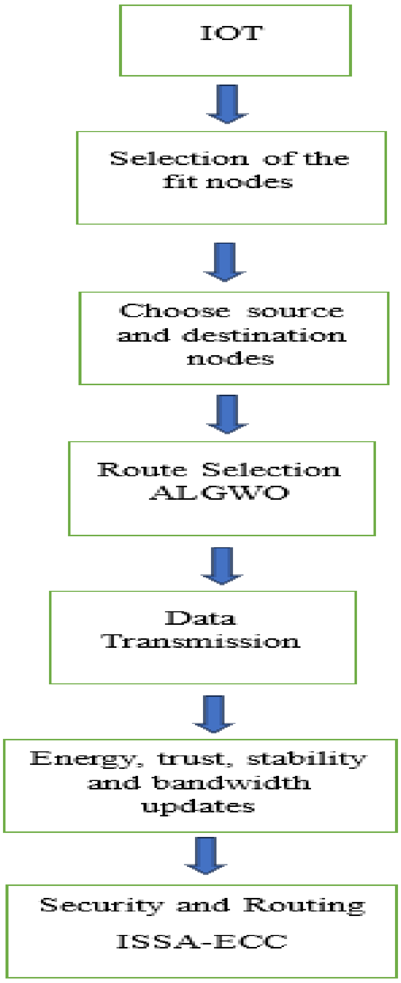

IOT
Selection of the fit nodes
Choose source and destination nodes
Route Selection ALGWO
Data Transmission
Energy, trust, stability and bandwidth updates
Security and Routing ISSA-ECC

Figure 1: Overall Proposed Model

Energy Efficiency: The function prioritizes nodes with higher energy to extend network life.

- Trustworthiness: It ensures data is routed through reliable, secure nodes.
- Stability: The function favours routes with stable links to minimize the risk of communication failures.
- Bandwidth Availability: It ensures nodes with sufficient bandwidth are selected to prevent congestion and delays.

This objective function drives the optimization process, enabling the selection of the most suitable nodes for efficient, secure, and reliable data transmission across the network.

3.2. Route Establishment

Finding and choosing the best paths from the Base Station (BS) to several locations within a wireless network is the aim of the route establishment phase. This involves evaluating nodes based on energy and trust levels, as well as assessing link stability and bandwidth. Each of these factors contributes to ensuring that the chosen routes are reliable, efficient, and capable of supporting data transmission effectively.

3.2.1. Energy Evaluation

To identify nodes with sufficient energy for routing, each node's energy level is assessed. Nodes with higher energy levels are preferred to avoid premature depletion and ensure sustained operation. The energy of a node i at time t can be represented as per Eq. (1).

$$e_i(t) = e_i(t-1) - e_{dist}(i) \quad (1)$$

Where, $e_{dist}(i)$ is the energy dissipated during data transmission.

3.2.2. Trust Evaluation

Trust is computed based on several factors, including direct trust, indirect trust, recent trust, and trust based on data bytes. For each node i in relation to node j, the trust score t_{ij} can be calculated as per Eq. (2).

$$t_{ij} = t_{dire}(i,j) + t_{indire}(i,j) + t_{rece}(i,j) + t_{bytes}(i,j) \tag{2}$$

Where, $t_{dire}(i,j)$ is the direct trust score based on observed interactions, $t_{indire}(i,j)$ is the trust score derived from other nodes' recommendations, $t_{rece}(i,j)$ is the reflects recent interactions, and $t_{bytes}(i,j)$ is the trust score based on the amount of data successfully transmitted.

3.2.3. Link Stability

Link stability assesses how consistently a link between two nodes remains operational. Stability can be measured by evaluating the frequency of link failures or disruptions. A typical measure of link stability might involve calculating the link stability factor l_{ij} given using Eq. (3).

$$l_{ij} = \frac{1}{1+lf_{ij}} \tag{3}$$

Where lf_{ij} is the number of times the link between nodes i and j has failed?

3.2.4. Bandwidth Assessment

Bandwidth is crucial for ensuring that the selected routes can handle the data load without causing delays. The available bandwidth of a node i can be denoted as b_i, and the required bandwidth for the route can be compared to ensure it is sufficient. The bandwidth requirement for a route can be calculated as per Eq. (4).

$$b_{req} = \max(b_{i1}, b_{i2}, \dots, b_{in}) \tag{4}$$

Where, $b_{i1}, b_{i2}, \dots, b_{in}$ are the bandwidths of the nodes along the route. To establish optimal routes, the network nodes are evaluated based on their energy and trust levels, while also considering link stability and available bandwidth. By incorporating these factors into the route selection process, the network ensures efficient, reliable, and secure communication from the Base Station to multiple destinations.

3.3. Route Optimization using ALGWO

ALGWO is a hybrid algorithm combining ALO and GWO techniques. It leverages the hunting behavior of antlions and the leadership hierarchy of grey wolves to find optimal solutions. By integrating energy, trust, link stability, and bandwidth metrics, ALGWO efficiently identifies secure and energy-efficient routes in multicast routing scenarios. GWO algorithm is inspired by the social hierarchy and hunting behavior of grey wolves. It models three leader wolves α, β, and δ as the top solutions guiding the rest of the pack (ω wolves) towards optimal solutions. The algorithm simulates wolf hunting in three main steps: encircling, hunting, and attacking the prey to find the global optimum.

- The encircling behavior of grey wolves around their prey in the GWO algorithm is mathematically modelled using Eq. (5) and Eq. (6).

$$\text{Distance Calculation: } d = c \times x_p(t) - x(t) \tag{5}$$

$$\text{Position Update: } \quad x(t+1) = x_p(t) - a \times d \tag{6}$$

$$a = 2ar_1 - A(t) \tag{7}$$

Integrating the ratio I from ALO into the coefficient vector c in the GWO enhances solution quality and prevents premature convergence. The updated coefficient vector is given by proposed Eq. (8).

$$c = 2r_2 \times I \tag{8}$$

Where $I = 10^{w}\left(\frac{t}{T}\right)$ adjusts based on the iteration stage. This dynamic adjustment of c balances exploration and exploitation effectively. By varying w throughout the iterations, the approach avoids premature convergence, ensuring the algorithm explores a broader search space and finds more optimal solutions. r_1 and r_2 are random vectors within the range. As demonstrated by Eq. (9), the elements of vector A fall linearly from 2 to 0 during the iterations.

$$A(t) = 2 - \frac{2t}{T} \tag{9}$$

Here, t is the current iteration, and T is the maximum number of iterations.

- In GWO, hunting behavior is modelled by assuming that the α, β, and δ wolves have superior knowledge of the prey's location. The remaining ω wolves update their positions based on these top three wolves' positions, guiding them toward the prey. This behavior is described by Eq. (10) to Eq. (12).

$$d_\alpha = |c_1 \times x_\alpha - x(t)| \tag{10}$$

$$d_\beta = \left|c_2 \times x_\beta - x(t)\right| \tag{11}$$

$$d_\gamma = \left|c_3 \times x_\gamma - x(t)\right| \tag{12}$$

Where c_1, c_2, and c_3 are calculated using Eq. (8).

$$x_{i1}(t) = x_\alpha(t) - a_{i1} \times d_\alpha(t) \tag{13}$$

$$x_{i2}(t) = x_\beta(t) - a_{i2} \times d_\beta(t) \tag{14}$$

$$x_{i3}(t) = x_\gamma(t) - a_{i3} \times d_\gamma(t) \tag{15}$$

Where, x_α, x_β, and x_γ are the top three solutions, with a_1, a_2, a_3, d_α, d_β, d_γ calculated using Eq. (13) to Eq. (16).

$$x(t+1) = \frac{x_{i1}(t)+x_{i2}(t)+x_{i3}(t)}{3} \tag{16}$$

- The attacking phase in GWO begins when wolves converge on the prey as it stops moving, signifying the end of the hunt. This phase is controlled by the parameter a, which decreases linearly from 2 to 0 over the course of iterations, balancing exploration and exploitation. The first half of the iterations focus on exploration, searching for diverse solutions, while the second half transitions smoothly to exploitation, refining the search around optimal areas. Wolves adjust their positions randomly between their current location and the prey’s position.

The GWO algorithm repeats the steps of encircling, hunting, and attacking until a set number of iterations (Maxiter) is reached. The best solutions (α, β, and δ) update their positions iteratively. However, GWO often suffers from limited population diversity and an imbalance between exploration and exploitation.

3.4. Improved Salp Swarm Algorithm with ECC

The protocol integrates ISSA for optimal secure path selection based on energy and trust, while ECC ensures secure data transmission by validating node keys, allowing only authorized network participation. SSA is an optimization technique inspired by the behavior of salp, gelatinous marine organisms that move in chains through water. Salp collective movement, known as salp chains, aids their foraging and navigation. SSA divides the population into leader and follower salp. The leader guides the swarm, while followers adjust their positions based on the leader's position. The algorithm models this behavior mathematically to solve optimization problems by frequently updating the positions of salp to explore the search space and find optimal solutions. ISSA enhances the traditional SSA by addressing its tendency to get stuck in local optima. While SSA adjusts the leader salp position solely based on the best solution (food source), ISSA incorporates the leader's previous position into the update process. This dual-based position adjustment helps maintain exploration capabilities and prevents premature convergence. By considering both past and current positions, ISSA improves the search efficiency and flexibility, making it more suitable for complex optimization problems with multiple local optima.

In the Improved Salp Swarm Algorithm (ISSA), the leader salp position is updated using Eq. (15), which incorporates both the current position and the best food source. This update is influenced by a time-varying parameter v_1 and a random number r_2. If r_2 is greater than 0.5, the position is adjusted positively; otherwise, it is adjusted negatively. This approach enhances exploration across the search space. For followers, Eq. (16) introduces a random time-varying factor, replacing the constant 0.5 in traditional SSA, which boosts global search in early iterations and refines local search later. Additionally, the ISSA improves performance by replacing the salp with the best fitness with a randomly generated one each generation, ensuring continued diversity and exploration.

$$x_i^1 = \begin{cases} x_i^j + v_1 \times \left(fp_i - x_i^j\right) & r_2 \geq 0.5 \\ x_i^j + v_1 \times \left(fp_i - x_i^j\right) & r_2 < 0.5 \end{cases} \tag{15}$$

$$x_i^j = v_1 \times rand(x_i^j + x_i^{j-1}) \tag{16}$$

Where, x_i^j represents the position of the leader salp in the jth dimension, while fp_i indicates the food position.

Elliptic Curve encryption (ECC) is a contemporary public key encryption technology that, in contrast to more conventional approaches like RSA, offers robust security with reduced key sizes. The foundation of ECC is the mathematics of elliptic curves, which are described by the formula $y^2 = x^3 + ax + b$. The security of ECC arises from the difficulty of solving the elliptic curve discrete logarithm problem, making it highly resistant to attacks even with shorter keys. This efficiency translates into faster computations and reduced resource usage, which is particularly beneficial for devices with limited processing power, such as smartphones and IoT devices. ECC is commonly used in digital signatures (e.g., ECDSA), secure communications (e.g., SSL/TLS), and cryptocurrencies, where it ensures data integrity and privacy. Compared to RSA, ECC offers enhanced security, faster performance, and lower computational demands, making it an increasingly popular choice for securing modern digital communications.

3.5. Data Transmission

In the data transmission phase, the focus shifts to executing the communication process based on the optimized routes identified in the route establishment phase. This process involves using these routes to efficiently deliver data from BS to the destination nodes and updating node metrics to maintain accurate network status.

3.5.1. Route Utilization

Once the optimal routes are established, multicast data transmission begins. The optimized routes, which have been selected based on criteria such as energy levels, trust scores, link stability, and bandwidth, are used to ensure that data is transmitted efficiently and reliably from the BS to the destination nodes. The chosen routes help in minimizing delays, reducing packet loss, and ensuring that the data reaches all intended recipients with high fidelity. During transmission, the network dynamically manages the data flow, routing it through the selected nodes while adhering to the path that was optimized.

3.5.2. Node Update

After each data transmission, it is crucial to update the state of the participating nodes to reflect their current status. This involves:

Energy Update: Nodes involved in the transmission experience energy consumption, which must be tracked to prevent early depletion. The energy level of each node is adjusted based on the amount of energy consumed during the data transmission. Regular updates ensure that the network has an accurate picture of the remaining energy in each node, which is essential for future routing decisions and maintaining network longevity.

Trust Update: Trust levels of nodes are also updated post-transmission to reflect their performance. Trust scores are recalculated based on the successful completion of the transmission and the reliability of the node during this process. If a node performs well, its trust score may improve; conversely, if it encounters issues or behaves maliciously, its trust score may decrease. These updates help in maintaining the integrity and security of the network, as future routing decisions will be influenced by the most recent trust data. This continuous update process ensures that the network adapts to changing conditions, maintains optimal performance, and remains secure and reliable over time.

Algorithm 1 demonstrates the ALGWO-ETP approach, optimizing multicast routing by evaluating energy, trust, link stability, and bandwidth metrics.

```
Algorithm 1: ALGWO-ETP
1. Initialize network nodes (N) with energy, trust, link stability, and bandwidth attributes.
2. Set parameters for ALGWO: maximum iterations (MaxIter), population size (PopSize), etc.
3. Evaluate each node's energy (E), trust (T), link stability (L), and bandwidth (B)
4. Define objective function to balance E, T, L, and B for route optimization.
5. While (t < MaxIter):
   a. For each node
      i.  Calculate energy dissipation
      ii. Calculate trust score
      iii. Calculate link stability
      iv. Assess bandwidth
   b. Update wolf positions using GWO (Eq. 5–16).
   c. Update antlion positions for exploration (using ALO ratio integration).
   d. Evaluate fitness of each node based on objective function (E, T, L, B).
   e. Select the top α, β, δ wolves for next iteration.
6. Establish optimal route based on highest fit nodes.
7. Begin data transmission using selected route.
8. Update node metrics (energy, trust) after each transmission.
9. If convergence is reached or MaxIter completed, terminate
10. Output optimized multicast routes.
```

4. RESULT-AND-DISCUSSION

4.1. Experimental-Setup

MATLAB is used to examine the experiment, and a simulation with between 50 and 100 nodes is created for examination. The proposed model was compared with Artificial Bee Colony (ABC), Grey Wolf Optimization (GWO), Chaotic Grey Wolf Adaptive Algorithm (CGWAA), and Hybrid Optimization Trust Energy Secure Routing Optimization (HO-TESRO). The results demonstrated that proposed model outperformed these models across key performance metrics, showing reduced delay, higher detection rate, improved energy efficiency, lower data loss, extended network lifetime, enhanced routing accuracy, and increased throughput. The optimized routing and security mechanisms in proposed model significantly contributed to these improvements, confirming its effectiveness.

4.2. Performance Metrics Analysis

The success of the suggested strategy in many elements of network performance is demonstrated by the results across the various performance metrics for both the proposed model and current models, as displayed in the tables.

Table 1: Delay indicates the time taken for data to be transmitted through the network. The proposed model demonstrates significantly lower delay across all time intervals compared to existing models. At a time, interval of 5 sec, the proposed model has a delay of just 0.15, while other models like Grey Wolf Optimization (GWO) and Hybrid Optimization Trust Energy Secure Routing Optimization (HO-TESRO) show delays of 25.5 and 4, respectively. This reduction in delay suggests that the proposed model provides more efficient data transmission, crucial for applications requiring real-time processing.

Table 1: Delay

TIME (sec)	5	10	15	20	25
GWO	25.5	25.85018	25.88863	25.95733	27.5243
ABC	18	18.56178	18.8503	19.56086	20.11429

CGWAA	13.2	15.94686	18.59046	24.72729	25.08743
HO-TESRO	4	6.27485	7.812383	8.55349	12.46691
Proposed	0.15	1.574974	3.310138	4.062402	4.457558

Table 2: Detection Rate measures the accuracy of detecting relevant events or anomalies. The proposed model achieves the highest detection rates, starting at 98% at a time interval of 5 sec and slightly decreasing to 93.94% at 25 sec. In comparison, existing models such as GWO and Antlion Grey Wolf Energy-Trust Pathway (HO-TESRO) show lower detection rates, with the best being 95% and 88%, respectively. This highlights the proposed model's superior capability in maintaining high detection accuracy over time.

Table 2: Detection Rate

TIME (sec)	**5**	**10**	**15**	**20**	**25**
GWO	88	71	70.76655	70.74091	70.69511
ABC	90	75	74.53185	74.29142	73.69928
CGWAA	92	80	77.50285	75.09959	69.52064
HO-TESRO	95	91	88.72515	87.18762	86.44651
Proposed	98	97.85	96.42503	94.68986	93.9376

Table 3: Energy assesses the energy efficiency of the network. The proposed model exhibits the highest energy values across all time intervals, starting at 96 at a time interval of 5 sec and decreasing to 91.94 at 25 sec. This is higher than all other models, where energy values for models like GWO and Antlion Grey Wolf Optimization (CGWAA) range from 84 to 66 and 89 to 66, respectively. The higher energy values for the proposed model suggest better utilization and management of energy resources.

Table 3: Energy

TIME (sec)	**5**	**10**	**15**	**20**	**25**
GWO	84	67	66.76655	66.74091	66.69511
ABC	86	71	70.53185	70.29142	69.69928
CGWAA	89	77	74.50285	72.09959	66.52064
HO-TESRO	92	88	85.72515	84.18762	83.44651
Proposed	96	95.85	94.42503	92.68986	91.9376

Table 4: Loss represents the amount of data loss in the network. The proposed model shows the lowest loss across all time intervals, with values starting at 0.003889 and peaking at 0.159253. In contrast, models like GWO and ABC show higher loss values, with losses ranging from 0.075 to 0.313981 and 0.015 to 0.297366, respectively. Lower loss indicates that the proposed model is more reliable in preserving data integrity during transmission.

Table 4: Loss

TIME (sec)	**5**	**10**	**15**	**20**	**25**
GWO	0.075	0.234793	0.273932	0.296964	0.313981
ABC	0.015	0.196993	0.257013	0.283142	0.297366

CGWAA	0.022	0.140451	0.146284	0.197582	0.257643
HO-TESRO	0.018889	0.112522	0.132927	0.17373	0.215635
Proposed	0.003889	0.105316	0.115079	0.158145	0.159253

Table 5: Network Lifetime measures the duration the network remains operational before depleting its resources. The proposed model achieves the longest network lifetime, starting at 82 and increasing to 86.06. This is significantly higher compared to other models such as GWO and ABC, where lifetime values range from 12 to 29 and 20 to 35, respectively. A longer network lifetime is crucial for sustaining network operations over extended periods without frequent maintenance.

Table 5: Network Lifetime

TIME (sec)	**5**	**10**	**15**	**20**	**25**
GWO	12	29	29.23345	29.25909	29.30489
ABC	20	35	35.46815	35.70858	36.30072
CGWAA	38	50	52.49715	54.90041	60.47936
HO-TESRO	55	59	61.27485	62.81238	63.55349
Proposed	82	82.15	83.57497	85.31014	86.0624

Table 6: Throughput measures how much data is successfully sent over a network in a given length of time. The proposed model has the highest throughput values, ranging from 1144 at a time interval of 5 sec to 854 at 25. This outperforms other models like HO-TESRO, which shows throughput ranging from 977 to 687. Higher throughput indicates that the proposed model is more efficient in handling and processing large volumes of data.

Table 6: Throughput

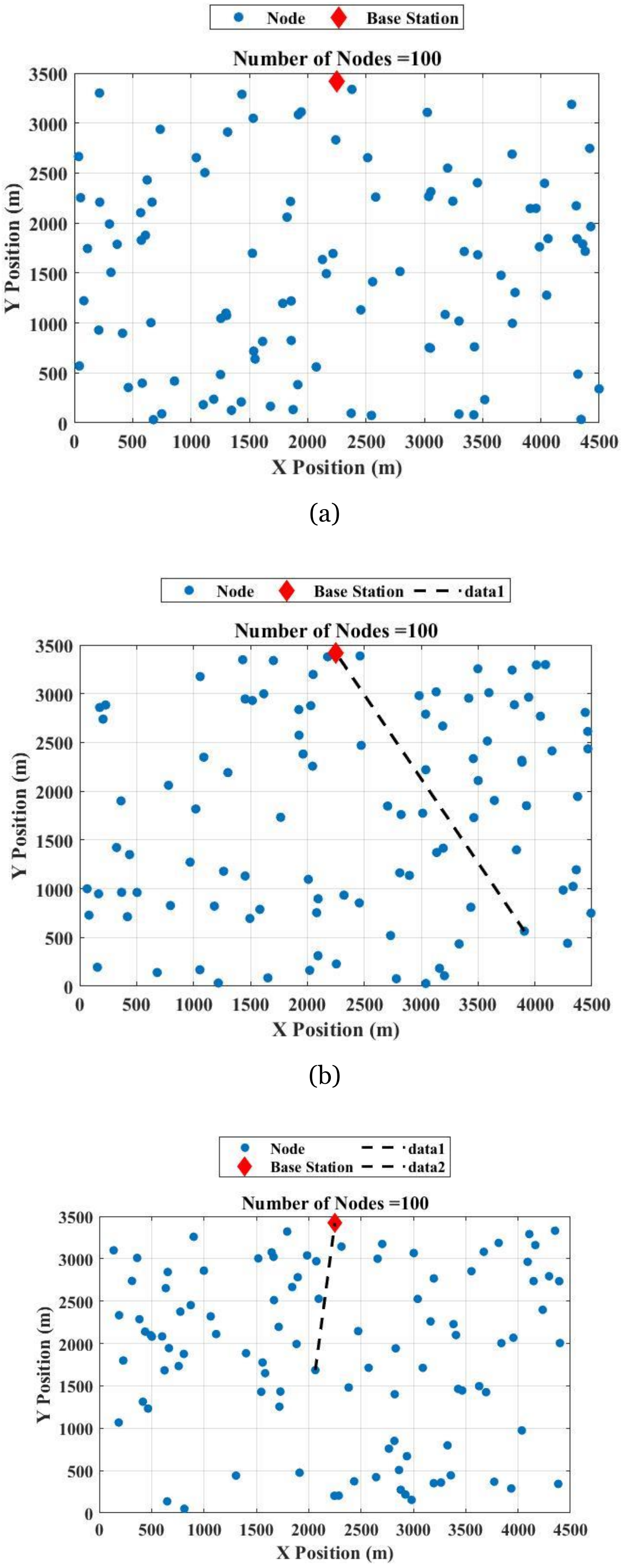
TIME (sec)	**5**	**10**	**15**	**20**	**25**
GWO	618	538	468	398	328
ABC	763	683	613	543	473
CGWAA	866	786	716	646	576
HO-TESRO	977	897	827	757	687
Proposed	1144	1064	994	924	854

4.3. Overall Graphical Representation

Fig. 2 illustrates a comparative analysis of network models across various performance metrics, including initialization, routing, delay, detection rate, energy efficiency, loss, network lifetime, and throughput. It highlights how the proposed model consistently outperforms existing models in all key areas.

Journal of Information Systems Engineering and Management
2025, 10(38s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

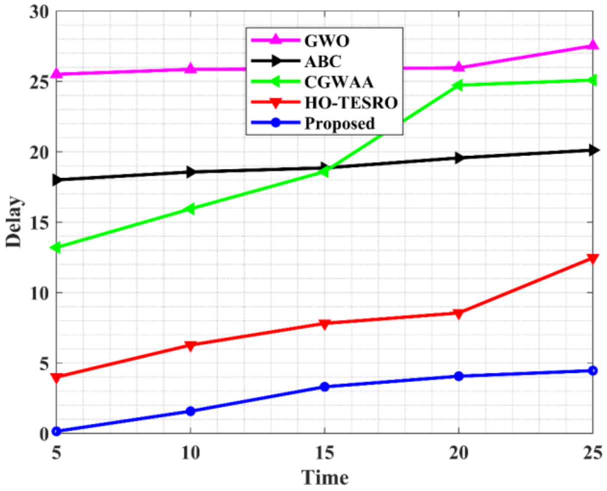


(a)

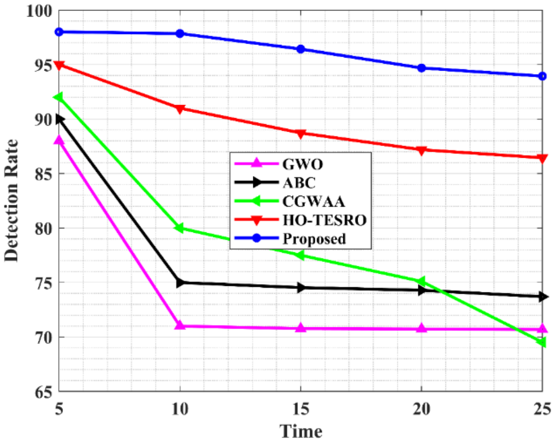
(b)

(c)

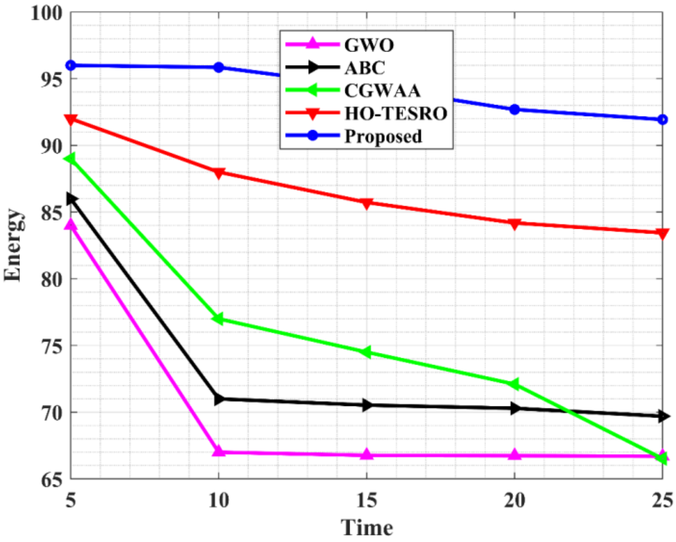
Journal of Information Systems Engineering and Management
2025, 10(38s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/



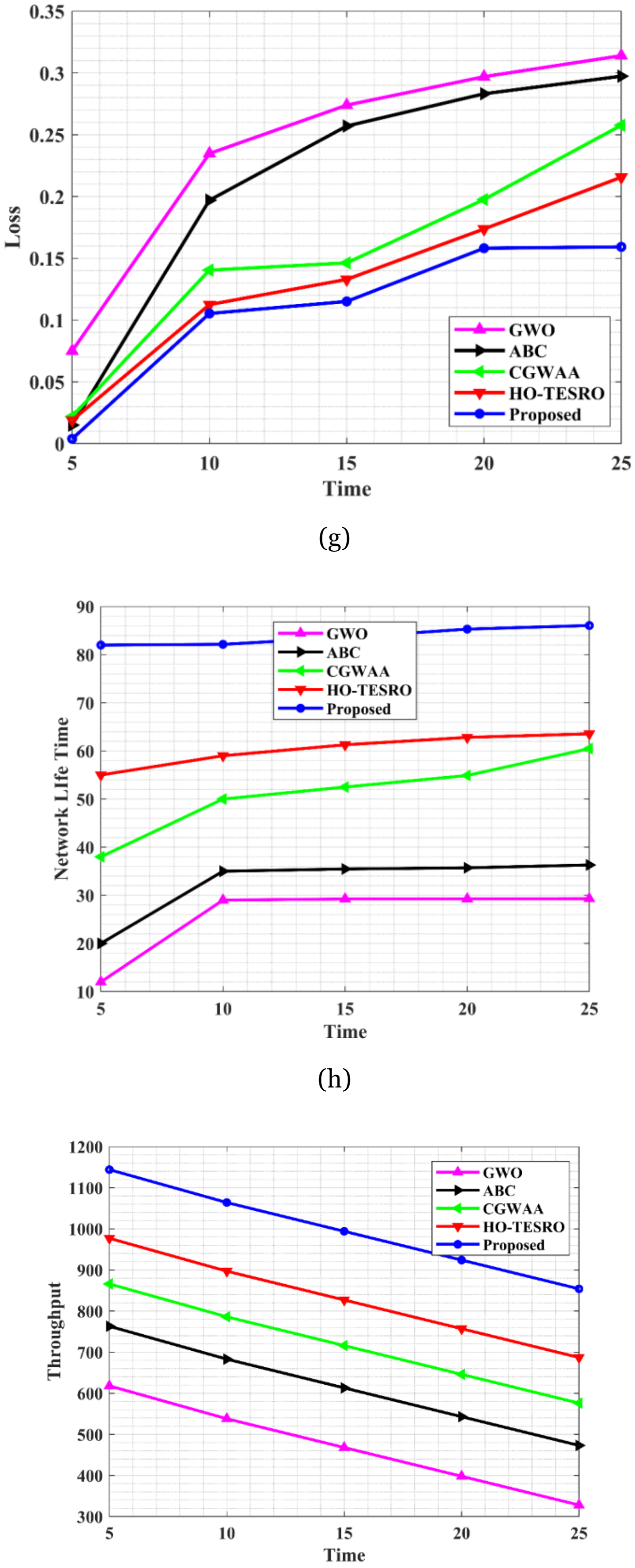
(d)



(e)



(f)



(g)

(h)

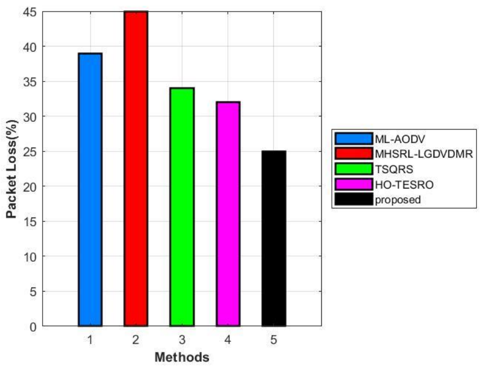
(i)

Figure 2: Performance Comparison of Network Models

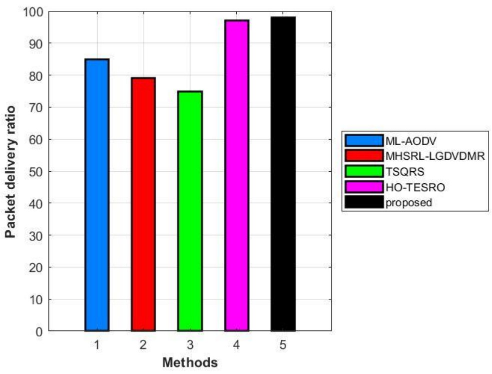
Table 7: Basepaper comparison with proposed model

Methods	Pkt Loss (kbps)	Pkt delivery ratio (%)	Throughput (kbps)
ML-AODV [26]	38	85	110
MHSRL-LGDVDMR [27]	45	79	96
TSQRS [28]	34	75	240
HO-TESRO	32	97	320
Proposed ALGWO-ETP	25	98	360

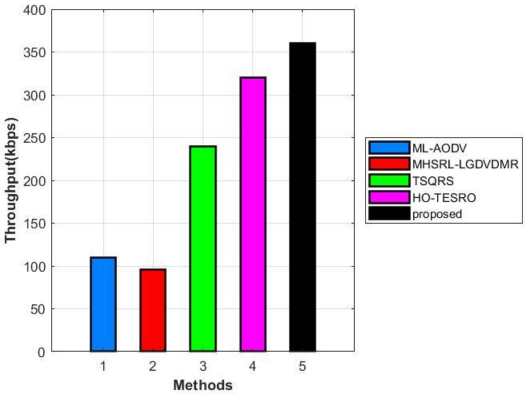
Routing techniques are compared in Table 7 according to throughput, packet delivery ratio, and packet loss. With the maximum throughput (360 kbps), the lowest packet loss (25 kbps), and the highest packet delivery ratio (98%), the proposed ALGWO-ETP model works well. On the other hand, ML-AODV exhibits mediocre performance with 110 kbps throughput, 85% delivery ratio, and 38 kbps packet loss. While TSQRS has a lower delivery ratio but a greater throughput, MHSRL-LGDVDMR has a higher packet loss (45 kbps) and performs worse overall. Although HO-TESRO works well, ALGWO-ETP outperforms it. All things considered, ALGWO-ETP provides exceptional efficiency in reducing packet loss and maximizing data transfer.



(a)



(b)



(c)

Figure 3: Base paper Comparison with Proposed Model

Fig. 3 illustrates a performance comparison between the base models and the proposed ALGWO-ETP model across key metrics.

5. CONCLUSION

A major difficulty in IoT and MANET, multicast routing required the BS to safely transfer data to numerous destinations via intermediary nodes. This study presented ALGWO-ETP, an energy-aware multicast routing technology, to solve these problems. This protocol combined ALO and GWO based on an objective function that included the energy, trust, connection stability, and bandwidth characteristics of the nodes. Initially, routes were created by assessing node energy and trust levels together with network stability and capacity. The ALGWO hybrid approach was then utilized to optimize the routes. Data was transmitted via the optimum path, and after each transmission, the energy and trust levels of each node were updated, guaranteeing the selection of secure and effective nodes. The protocol was enhanced with the addition of the ISSA and ECC to further improve security and routing efficiency. While the ECC mechanism secured data transmission by validating node keys and shared codes, keeping only legitimate nodes in the network, the ISSA evaluated and chose the most secure and efficient multiple paths, optimizing routing decisions based on node energy and trustworthiness. This procedure improved the efficiency and dependability of communication.

DECLARATION OF INTERESTS:

FUNDING

On Behalf of all authors the corresponding author states that they did not receive any funds for this project.

CONFLICTS OF INTEREST

The authors declare that we have no conflict of interest.

COMPETING INTERESTS

The authors declare that we have no competing interest.

DATA AVAILABILITY STATEMENT

All the data is collected from the simulation reports of the software and tools used by the authors. Authors are working on implementing the same using real world data with appropriate permissions.

ETHICS APPROVAL

No ethics approval is required.

CONSENT TO PARTICIPATE

Not Applicable

CONSENT FOR PUBLICATION

Not Applicable

HUMAN AND ANIMAL ETHICS:

Not Applicable.

CODE AVAILABILITY:

Not Applicable.

REFERENCES

[1] Udhayamoorthi, M., Pradeep, S., Marimuthu, K. and Karthikeyan, A., 2024. TEE-AODV Trust-based Route Selection and Improving Energy Efficiency in MANET. IETE Journal of Research, pp.1-14.

[2] Krishnaveni, S. and Angel, N., 2019. Energy Efficient MANET by Trusted Node Identification Using IHSO Optimization. Smart Network Inspired Paradigm and Approaches in IoT Applications, pp.239-253.

[3] Dalal, S., Seth, B., Jaglan, V., Malik, M., Surbhi, Dahiya, N., Rani, U., Le, D.N. and Hu, Y.C., 2022. An adaptive traffic routing approach toward load balancing and congestion control in Cloud–MANET ad hoc networks. Soft Computing, 26(11), pp.5377-5388.

[4] Ravi, S., Matheswaran, S., Perumal, U., Sivakumar, S. and Palvadi, S.K., 2023. Adaptive trust-based secure and optimal route selection algorithm for MANET using hybrid fuzzy optimization. Peer-to-Peer Networking and Applications, 16(1), pp.22-34.

[5] Jose, M.R. and Vigila, S.M.C., 2023. F-CAPSO: Fuzzy chaos adaptive particle swarm optimization for energy-efficient and secure data transmission in MANET. Expert Systems with Applications, 234, p.120944.

[6] Shende, D.K. and Sonavane, S.S., 2020. CrowWhale-ETR: CrowWhale optimization algorithm for energy and trust aware multicast routing in WSN for IoT applications. Wireless Networks, 26, pp.4011-4029.

[7] Reddy, M.V.K., Srinivas, P.V.S. and Mohan, M.C., 2023. Energy efficient routing with secure and adaptive trust threshold approach in mobile ad hoc networks. The Journal of Supercomputing, 79(12), pp.13519-13544.

[8] AM, A.B., 2021. High energy efficient lifetime management system and trust management framework for manet using self-configurable cluster mechanism. Peer-to-Peer Networking and Applications, 14, pp.1229-1241.

[9] Gurram, G.V., Shariff, N.C. and Biradar, R.L., 2022. A secure energy aware meta-heuristic routing protocol (SEAMHR) for sustainable IoT-wireless sensor network (WSN). Theoretical Computer Science, 930, pp.63-76.

[10] Abujassar, R.S., 2024. A novel algorithm for the development of a multipath protocol for routing and energy efficient in IoT with varying density. Telecommunication Systems, pp.1-15.

[11] Singh, P., Khari, M. and Vimal, S., 2022. EESSMT: an energy efficient hybrid scheme for securing mobile ad hoc networks using IoT. Wireless Personal Communications, 126(3), pp.2149-2173.

[12] Khan, A.F. and Rajalakshmi, C.N., 2022. A multi-attribute based trusted routing for embedded devices in MANET-IoT. Microprocessors and Microsystems, 89, p.104446.

[13] Rajeswari, A.R., Kulothungan, K., Ganapathy, S. and Kannan, A., 2019. A trusted fuzzy based stable and secure routing algorithm for effective communication in mobile adhoc networks. Peer-to-Peer Networking and Applications, 12, pp.1076-1096.

[14] Usha, M.S. and Ravishankar, K.C., 2021. Implementation of trust-based novel approach for security enhancements in MANETs. SN Computer Science, 2(4), p.257.

[15] Hemalatha, R., Umamaheswari, R. and Jothi, S., 2021. Optimal route maintenance based on adaptive equilibrium optimization and GTA based route discovery model in MANET. Peer-to-Peer Networking and Applications, 14(6), pp.3416-3430.

[16] Naveen, G. and Prathap, P.J., 2024. Hybrid cat and mouse-based dolphin swarm optimization strategy for intelligent routing in wireless sensor network applicable for iot applications. Peer-to-Peer Networking and Applications, pp.1-25.

[17] Saleem, F., Majeed, M.N., Iqbal, J., Waheed, A., Rauf, A., Zareei, M. and Mohamed, E.M., 2021. Ant lion optimizer-based clustering algorithm for wireless body area networks in livestock industry. IEEE Access, 9, pp.114495-114513.

[18] Kaur, G. and Kakkar, D., 2024. DRIVE: Dual rider-remora optimization for vehicular routing. Peer-to-Peer Networking and Applications, 17(2), pp.834-857.

[19] Abdulhae, O.T., Mandeep, J.S. and Islam, M., 2022. Cluster-based routing protocols for flying ad hoc networks (FANETs). IEEE access, 10, pp.32981-33004.

[20] Dattatraya, K.N. and Rao, K.R., 2022. Hybrid based cluster head selection for maximizing network lifetime and energy efficiency in WSN. Journal of King Saud University-Computer and Information Sciences, 34(3), pp.716-726.

[21] Kaviarasan, S. and Srinivasan, R., 2024. Developing a novel energy efficient routing protocol in WSN using adaptive remora optimization algorithm. Expert Systems with Applications, 244, p.122873.

[22] Kothandaraman, D., Balasundaram, A., Dhanalakshmi, R., Sivaraman, A.K., Ashokkumar, S., Vincent, R. and Rajesh, M., 2022. Energy and Bandwidth Based Link Stability Routing Algorithm for IoT. Computers, Materials & Continua, 70(2).

[23] Gopala Krishnan, C., Nishan, A.H., Gomathi, S. and Aravind Swaminathan, G., 2022. Energy and trust management framework for MANET using clustering algorithm. Wireless Personal Communications, 122(2), pp.1267-1281.

[24] Mishra, M., Gupta, G.S. and Gui, X., 2021. Network lifetime improvement through energy-efficient hybrid routing protocol for IoT applications. Sensors, 21(22), p.7439.

[25] Chandravanshi, K., Soni, G. and Mishra, D.K., 2022. Design and analysis of an energy-efficient load balancing and bandwidth aware adaptive multipath N-channel routing approach in MANET. IEEE Access, 10, pp.110003-110025.

[26] Shafi, S., Mounika, S. and Velliangiri, S.J.P.C.S., 2023. Machine learning and trust based AODV routing protocol to mitigate flooding and blackhole attacks in MANET. Procedia Computer Science, 218, pp.2309-2318.

[27] Jia, X., Huang, D. and Qin, N., 2024. AI-enhanced security demand and routing management for MANETs with optical technologies. Optical and Quantum Electronics, 56(2), p.229.

[28] Pathan, M.S., Zhu, N., He, J., Zardari, Z.A., Memon, M.Q. and Hussain, M.I., 2018. An efficient trust-based scheme for secure and quality of service routing in MANETs. Future Internet, 10(2), p.16.