International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2025/09 Volume 12, Issue 1, January – February (2025)

RESEARCH ARTICLE

Secure and Energy-Efficient Location-Aware Protocols for Flying Ad-Hoc Networks (FANETs)

Gaurav Jindal
Department of Computer Applications, Post Graduate Government College, Sector-46, Chandigarh, India.
✉ jindal_08@yahoo.co.in

Navdeep Kaur
Department of Computer Science, Sri Guru Granth Sahib World University, Fatehgarh Sahib, Punjab, India.
drnavdeep@sggswu.edu.in

Received: 07 December 2024 / Revised: 29 January 2025 / Accepted: 19 February 2025 / Published: 28 February 2025

Abstract – The growing reliance on wireless networks and the unique attributes of Flying Ad-hoc Networks (FANETs) have propelled their advancement in both academic and industrial domains. With the proliferation of Unmanned Aerial Vehicles (UAVs), FANETs have become indispensable for diverse applications, including traffic monitoring, videography, and a wide range of military and civilian operations. This study introduces an innovative hybrid metaheuristic swarm intelligence approach integrated with a supervised learning framework utilizing a backpropagation neural network. The proposed method focuses on clustering-based, location-aware, and energy-efficient routing in FANETs. Results demonstrate significant improvements in network performance, including enhanced energy conservation, prolonged network lifetime, and reduced end-to-end delay. Furthermore, the approach achieves high throughput, emphasizing its potential as a robust solution for optimizing network efficiency and sustainability. Additionally, a comparative analysis with existing optimization-based methods highlights issues and significant improvements in metrics like energy consumption, packet delivery ratio, and resistance to attacks. The results reveal that the proposed protocols achieve better energy conservation and prolonged network lifetime without compromising security or quality of service. This research establishes a new paradigm for leveraging supervised learning to address critical challenges in FANETs while promoting energy efficiency and reliability.

Index Terms – FANETs, UAV, Wireless Networks Backpropagation, Neural Network, Supervised Learning, Clustering, Routing.

1. INTRODUCTION

The use of Unmanned Aerial Vehicles (UAVs) is rapidly expanding across various sectors such as traffic surveillance, film-making, and both defence and civilian applications, owing to their significant role in mission-critical operations. This increase in application has fuelled advancements in research within both the academic and industrial spheres, particularly in the area of Flying Ad-hoc Networks (FANETs) [1]. These networks represent a new wave in wireless technology, offering a flexible solution for a range of commercial and defence-related tasks. Flying Ad-Hoc Networks (FANETs), consisting of interconnected UAVs, are essential for efficient data transmission and seamless connectivity with terrestrial control units. These UAVs, integral to Unmanned Aerial Systems (UAS), extend communication networks and are especially valuable for rapid network deployment. Single-UAV networks, often using star topology, face challenges such as long transmission ranges and increased data loads, requiring high-directional antennas with Omni-directional properties for improved performance. On the other hand, multi-UAV systems enhance coverage, data capacity, and fault tolerance but introduce complexities like coordination and interference management. Balancing these systems' advantages and addressing their challenges is critical for advancing FANET technology. The multi-UAV system, despite its complexities, offers notable advantages [2][3].

1. Adaptability: The system utilizing multiple unmanned aerial vehicles (UAVs) boasts an extensive reach, capable of adjusting seamlessly to diverse environmental scenarios.
2. Operational Resilience: The network among these UAVs is consistently maintained. This ensures that even if one UAV encounters a malfunction or is compromised during a mission, other UAVs can seamlessly take over, ensuring mission completion.
3. Enhanced Speed: The collective effort of several UAVs in data relay significantly boosts the velocity of information transfer.
4. Improved Precision: Despite the small radar cross-section of the multi-UAV system, it remarkably achieves high accuracy, especially vital for military operations.

RESEARCH ARTICLE

Additionally, this system is more eco-friendly compared to using a singular UAV [4][5].

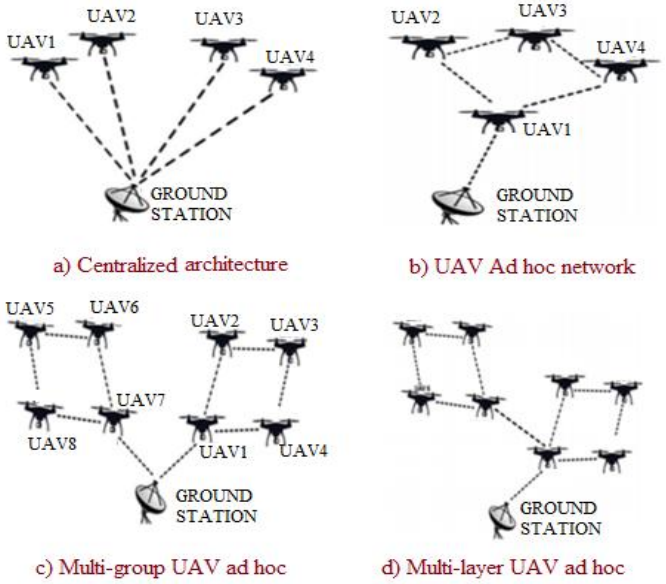

Figure 1 Multi-Level Networks-Based UAV Communications

In recent years, FANETs have demonstrated significant growth and versatility, becoming increasingly integral in modern network infrastructures. These networks allow Unmanned Aerial Vehicles (UAVs) to work either autonomously or through remote control, without the need for direct human oversight. This adaptability enables UAVs to efficiently integrate with terrestrial ad hoc networks. Ad hoc networks, known for their cost-effectiveness and spontaneity in network formation, operate without central data forwarding units.

In these networks, each individual node independently serves as a transmitter, receiver, and router. However, traditional ad hoc networks face limitations in dynamic environments due to their changing communication requirements.

Introducing UAVs as intermediate nodes in these networks presents a solution to overcome these challenges. UAVs facilitate a variety of complex tasks, such as cooperative searching, object monitoring, data acquisition, and analysis. While there are instances of successful integration of single UAV systems within existing ad hoc networks, these singular UAV networks often suffer from limited scalability and monitoring capabilities.

Consequently, the formation of a cohesive aerial network comprising multiple UAVs becomes essential. Such a network, operating in conjunction with ground-based networks, can significantly enhance monitoring and operational capabilities [6][7].

Figure 1 the deployment of multiple UAVs within a network significantly improves operational efficiency and data reliability by expanding coverage areas and providing redundancy. This redundancy ensures consistent data collection and stable communication, even in challenging or unpredictable environments. The distributed architecture of multi-UAV networks enhances their scalability and resilience, enabling them to adapt to diverse operational demands and scenarios effectively. Such adaptability is vital for applications in dynamic settings where reliability and flexibility are critical.

Beyond their roles in communication and data collection, UAVs in a FANET configuration demonstrate advanced capabilities, including real-time data processing, autonomous decision-making, and dynamic routing adjustments in response to environmental changes or mission-specific requirements. These features make UAV networks particularly suitable for tasks in remote or disaster-affected regions where conventional infrastructure is absent. By integrating machine learning and artificial intelligence, UAV systems gain the ability to optimize flight paths, analyse environmental data, and make intelligent decisions autonomously, thereby enhancing their operational efficiency and versatility in complex missions.

This is especially beneficial in scenarios requiring real-time data analysis and rapid response, such as in search and rescue operations or in monitoring fast-changing environmental conditions [8][9]. The research contributes to optimizing Flying Ad-Hoc Networks (FANETs) by developing energy-efficient, secure, and adaptive communication protocols. It integrates hybrid optimization techniques like PSO and MFO to enhance routing performance and reduce latency. These advancements improve network resilience, scalability, and Quality of Service (QoS) for diverse applications.

Figure 2 However, the deployment of multi-UAV systems also presents technical and regulatory challenges. These include ensuring secure and reliable communication links, effective coordination among UAVs, and compliance with evolving airspace regulations. Addressing these challenges is essential for the successful implementation and future expansion of UAV networks in various sectors.

Eventually, the evolution of FANETs and the increasing sophistication of UAV technology are paving the way for innovative applications and solutions across multiple domains. The potential of UAV networks in enhancing communication, improving data collection, and providing critical support in diverse operations is immense. As research and development in this field continue to advance, we can expect UAV systems to play an increasingly vital role in addressing complex challenges in both civilian and military contexts [10].

International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2025/09 Volume 12, Issue 1, January – February (2025)

RESEARCH ARTICLE

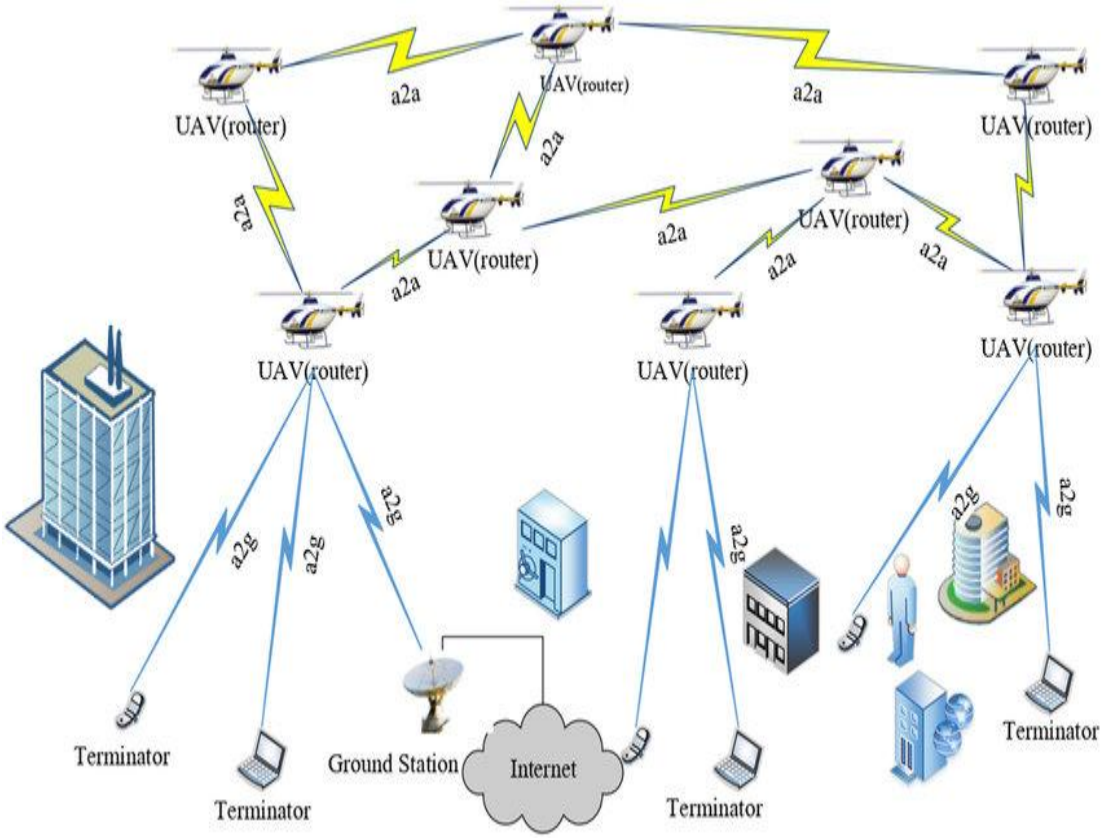

Figure 2 Modelling FANET Networks in Smart Cities

Figure 2 However, the deployment of multi-UAV systems also presents technical and regulatory challenges. These include ensuring secure and reliable communication links, effective coordination among UAVs, and compliance with evolving airspace regulations. Addressing these challenges is essential for the successful implementation and future expansion of UAV networks in various sectors. Eventually, the evolution of FANETs and the increasing sophistication of UAV technology are paving the way for innovative applications and solutions across multiple domains. The potential of UAV networks in enhancing communication, improving data collection, and providing critical support in diverse operations is immense. As research and development in this field continue to advance, we can expect UAV systems to play an increasingly vital role in addressing complex challenges in both civilian and military contexts [10].

1.1. Motivation

The growing demand for applications like real-time traffic monitoring, video streaming, and healthcare tracking has highlighted the critical need for energy-efficient solutions in Flying Ad-Hoc Networks (FANETs). These UAV-based networks are vital in fields such as traffic management and defence, where ensuring secure and energy-efficient operations is essential for maintaining reliability and effectiveness in dynamic and resource-constrained environments. However, FANETs face unique challenges due to their inherent characteristics, such as random deployment, dynamic topology, and high energy consumption, which significantly impact their routing efficiency.

Energy optimization has emerged as a key focus in FANET research, as effective routing strategies are crucial to ensuring operational reliability and sustainability. Addressing these challenges necessitates a comprehensive approach that incorporates relevance-based clustering and advanced hybrid optimization methods driven by artificial intelligence. These AI-driven solutions are tailored to enhance critical Quality of Service (QoS) parameters, such as throughput, end-to-end delay, packet delivery ratio, packet loss rate, collision avoidance, and energy usage, while enabling adaptive and location-aware routing mechanisms [11][12].

The integration of sophisticated AI techniques provides a transformative framework for tackling the inherent complexities of FANETs. By improving metrics like packet delivery and collision avoidance, as well as managing energy consumption efficiently, AI-based methodologies ensure robust and secure network operations. This becomes

RESEARCH ARTICLE

especially vital in high-demand scenarios, such as surveillance, emergency response, and military applications, where reliability and efficiency are non-negotiable.

This study underscores the potential of leveraging relevance clustering combined with hybrid optimization to address FANET challenges comprehensively. The proposed approach aims to create a resilient and adaptive routing mechanism that not only enhances network performance but also ensures energy conservation in highly dynamic environments. By focusing on the interplay between AI and energy-efficient routing, this research marks a significant stride toward revolutionizing FANET infrastructure, paving the way for more sustainable and high-performing UAV networks.

The rest of the manuscript is organized as follows. Section 2 reviews related work, offering insights into existing approaches. Section 3 articulates the problem statement, highlighting the gaps addressed in this study. Section 4 presents the proposed methodology, including flowcharts, algorithms. Section 5 results and discussions obtained from MATLAB-based simulations. Finally, Section 6 concludes the research by summarizing key findings and discussing their implications for future advancements in FANETs.

2. RELATED WORK

Table 1 shows the related work in the field of Flying Ad-Hoc Networks (FANETs), a study by Aftab et al. [11] presented a hybrid self-organized clustering strategy for drones within cognitive Internet of Things (IoTs) networks. Addressing challenges like energy consumption and security in drone-based IoTs, they introduced a Hybrid Self-organized Clustering Scheme (HSCS) combining GSO and Dragonfly Algorithm (DA). This scheme, focusing on cluster formation and head selection, leveraged the DA for effective cluster member tracking, ensuring efficient management. Their evaluation highlighted the HSCS's effectiveness in QoS parameters like cluster lifetime and energy consumption, although they noted the need for extending the cluster lifetime." Namdev et al. [13] focused on optimizing energy-efficient and secure communication in FANETs using hybrid models combining swarm intelligence, genetic algorithms, and cryptographic techniques. Their approach improves network resilience, extends drone lifespan, and integrates location-aware routing for reliable and secure data transmission. These efforts address energy consumption and security challenges effectively. Ali et al. [14] focused on developing a novel routing architecture to enhance drone-based internet applications in everyday life. These applications are diverse, including traffic surveillance, agricultural oversight, healthcare support, disaster management, and rescue operations. The study addressed challenges inherent in FANETs, such as dynamic network topology and the difficulty in optimal node selection and autonomous adaptation to prevent routing loops. The research emphasized the need for substantial improvements in FANETs performance for future application scenarios, leading to the creation of a performance-centric routing framework to facilitate better UAV-to-UAV communication. Liu et al. [15] also explored the realm of FANETs, particularly focusing on the architecture that supports performance-aware routing. This research highlighted the role of FANETs in enabling the Internet of Drones for various practical uses. Challenges like quick UAV movement and frequent changes in network topology, which complicate node selection and self-adjustment, were key issues addressed. The study proposed an enhanced performance routing system for effective communication in FANETs environments. Additionally, Mowla et al. [16] introduced an adaptive federated reinforcement learning (AFRL) approach tailored for intelligent defence against jamming in FANETs. Their methodology involved initial decisions based on centralized knowledge about communication and power constraints in FANETs, considering UAV mobility density. This approach led to the development of a model-based strategy for jamming defence, featuring an AFRL-based plan. The team also innovated a jamming detection system using Q-learning, which outperforms traditional methods with a significantly higher detection rate, thanks to its adaptive epsilon-greedy strategy. Furthermore, Li et al. [17] investigated mobility-assisted adaptive routing in FANETs comprising intermittently connected UAVs. Recognizing the limitations of existing routing algorithms in mobility-centric networks, they introduced the Mobility Assisted Adaptive Routing (MAAR), a geographic routing method that integrates routing with location services. This method aims to reduce latency and routing overhead, employing a store-carry-and-forward model to mitigate communication disruptions. Sang et al. [18] proposed an energy-efficient opportunistic routing strategy for FANETs, addressing the challenges of dynamic links and constant communication issues in these networks. Their EORB-TP protocol is a novel trajectory prediction-based opportunistic routing system that leverages the concept of resourceful communication to predict UAV positions and calculate trajectory metrics to avoid energy overuse. Lastly, Tropea [19]and team conducted research on a FANETs simulator to manage drones and enable dynamic connectivity. Their study aimed to address the challenges of traditional networking paradigms in emergency situations, developing a UAV/drone behaviour model that considers energy concerns and devises new methods for area coverage and human movement behaviours. A. Khan et al. [20] developed a novel clustering approach for enhancing communication within Flying Ad-Hoc Networks (FANETs). This approach, inspired by the natural behaviours of glow-worms, involves a Glow-worm Swarm Optimization (GSO) algorithm. It focuses on creating clusters and managing networks through an election process for cluster heads, based on factors such as proximity to the ground control station, luciferin levels, and the

RESEARCH ARTICLE

remaining energy of Unmanned Aerial Vehicles (UAVs). The algorithm also includes a method for choosing routes based on the UAVs' neighbour range, residual energy, and location, aiming to improve network communication efficiency. Although the authors compared their approach with existing bio-inspired clustering methods in aspects like energy usage, cluster formation time, and delivery success rates, they did not address network congestion control. Furthermore, M. A. Khan [21] introduced a hybrid communication strategy to optimize the deployment of FANETs in a cost-effective manner. With the growing use of UAVs in various sectors, FANETs have become increasingly significant. The study reviewed existing FANET communication frameworks and concluded that multi-layer FANETs are optimal for networking diverse groups of UAVs. Their hybrid communication model combines the high data transmission rate of 802.11 with the energy efficiency of 802.15.1, leading to enhanced network throughput and reduced delays for a specific number of UAVs. Lastly, Souza et al. [22] explored a fuzzy logic-based routing protocol for FANETs, aiming to ensure Quality of Service (QoS). They proposed an adaptive routing protocol using fuzzy logic for effective route discovery in FANETs. Simulations were used to validate this protocol, assessing it through QoS and Quality of Experience (QoE) metrics. The study suggests that the implementation of novel AI techniques could further improve the protocol by reducing path loss at varying altitudes.

Table 1 Challenges Based on Observations of Existing Routing Protocols and Optimizations

Challenges	Observations & Findings	Methodology	Limitations
Cluster Head Selection	Existing strategies for choosing cluster heads based on proximity neglect the potential of utilizing UAVs with the highest residual energy, which could mitigate data loss and delay issues [11].	Used bio-inspired techniques for head selection, considering UAV range, residual energy, and member tracking.	Limited strategies for extending cluster lifetime or managing network congestion.
Energy Efficiency	Prior methodologies exhibit elevated energy usage, attributed to inefficient clustering techniques, which hinge on routing protocols to nominate superior cluster heads [13].	Location-aware routing integrated with optimization algorithms and lightweight cryptographic techniques.	Increased computational complexity for large-scale deployments.
Delay Patterns	Understanding of delay patterns, influenced by transmission methods and cooperation strategies, remains inadequate, posing ongoing challenges in delay minimization and energy conservation [15].	Routing approaches considering quick UAV movement and self-adjustment in dynamic environments.	Limited scalability under increasing network size and complexity.
Fault Tolerance	Maintaining cluster functionality in case of cluster head failure or member UAV malfunction [15][19].	Designed UAV behavior models addressing energy concerns and human movement, with methods for coverage and emergency response.	Did not propose mechanisms for real-time fault recovery.
Mobility and Security	Approaches considering mobility for route discovery fall short in ensuring security and efficient communication for a broad array of UAVs, alongside issues with energy consumption [16].	Integrated AFRL-based strategies with Q-learning for adaptive jamming detection and centralized decision-making.	Computational overhead challenges for real-time jamming defence.

RESEARCH ARTICLE

Transmission Delays	The lack of sophisticated cluster head selection further exacerbates transmission delays, undermining network performance [17].	Store-carry-and-forward model combined with geographic routing and location services for delay reduction.	Inadequate performance in networks with high packet loss or intermittent connectivity.
Energy Balancing Among UAVs	Uneven energy consumption among cluster members and heads leads to premature node failures [18][20].	Opportunistic routing leveraging UAV position prediction to minimize unnecessary communication and energy overuse.	Challenges in adapting trajectory prediction to highly dynamic environments.
Scalability in Dense Networks	Managing a high number of UAVs efficiently without excessive overhead in large-scale networks [19][21].	Designed multi-layer FANETs to network diverse UAV groups with optimized protocols for improved communication.	Limited ability to adapt to dynamic density variations in large-scale networks.
Cluster Management	Initial methods for cluster formation in FANETs rely on random selection strategies, leading to inefficient route management due to the non-strategic allocation of cluster heads [20].	Clustering based on proximity, luciferin levels, and UAV energy	Lacked congestion control and scalability considerations in dense networks.
Optimization Goals	Research predominantly focuses on single-objective optimization for route discovery, neglecting multifaceted goals. When energy efficiency is prioritized, this often results in compromises on security and increases in transmission delays [21].	Adaptive routing strategies focusing on frequent topology changes and UAV mobility.	Lack of robust handling for extreme mobility or rapidly changing environments.
Traffic Congestion	Unforeseen traffic congestion prompts significant alterations in network topology, leading to unstable routes and heightened risks of transmission delays [22].	Applied fuzzy logic for route discovery and traffic management while addressing path loss at varying altitudes.	Potential improvements with AI techniques to enhance traffic prediction accuracy.

3. PROBLEM DEFINITION

The dynamic nature of Unmanned Aerial Vehicle (UAV) networks, also known as Flying Ad-Hoc Networks (FANETs), presents significant challenges in energy efficiency and security, both of which are critical for ensuring reliable communication. These challenges are particularly pronounced in high-stakes applications such as public safety surveillance, emergency response, military operations, and data collection tasks, where seamless and secure communication is paramount [9]. A key limitation of UAVs in FANETs is their constrained battery capacity, which necessitates the development of energy-efficient frameworks capable of managing routing, mobility, and timing without degrading network performance.

At the heart of this issue lies the need for a routing mechanism that optimizes energy usage while maintaining high-quality communication among UAVs. Achieving this balance is complicated by the dynamic and distributed nature of FANETs, where frequent topology changes and high mobility make traditional routing strategies inadequate.

RESEARCH ARTICLE

Additionally, safeguarding location privacy during data exchange becomes increasingly challenging due to the inherent mobility and open communication environment of UAVs, leaving the network vulnerable to security threats [23].

This research tackles the challenges of energy efficiency and location privacy in FANETs through a dual-module framework. The first module optimizes energy consumption by clustering the network area and utilizing a swarm-based metaheuristic algorithm to select effective Cluster Heads. This approach enhances throughput, reduces energy usage, and simplifies network operations. The second module addresses location privacy by integrating an advanced mechanism at the Medium Access Control (MAC) layer. Leveraging artificial intelligence and swarm-based metaheuristic techniques, it adapts dynamically to network changes, ensuring secure and efficient communication. The proposed solution combines energy-efficient routing with robust location-aware mechanisms to ensure secure and reliable communication in FANETs. By focusing on improving Quality of Service (QoS) metrics such as throughput, latency, and energy efficiency, the approach addresses the challenges posed by dynamic UAV environments. Additionally, it strengthens network security, making it well-suited for applications requiring high-performance communication in complex and rapidly changing scenarios. The anticipated outcomes aim to demonstrate the viability and effectiveness of this novel routing framework, paving the way for more resilient and efficient FANET infrastructures in diverse application domains [24]. A fuzzy-based trust model to enhance security in FANETs by assessing node trustworthiness. The model helps mitigate malicious attacks and ensures reliable data transmission in dynamic UAV networks [25].

4. PROPOSED WORK

This research presents an innovative approach combining hierarchical clustering and moth flame optimization to enhance routing efficiency and network performance in FANET networks. By employing hierarchical clustering, we adopt a stable election protocol as a routing mechanism, optimizing systematic routing while minimizing failure risks and maintaining load balance (Figure 3). Furthermore, the integration of moth flame optimization targets the reduction of network randomness and topology variations, significantly diminishing path delays and losses. This strategy is aimed at bolstering network stability. An illustrative flowchart of the suggested methodology is provided for clarity. This detailed exploration offers a more comprehensive understanding of the proposed solution's mechanics and its potential impact on network optimization (Figure 4).

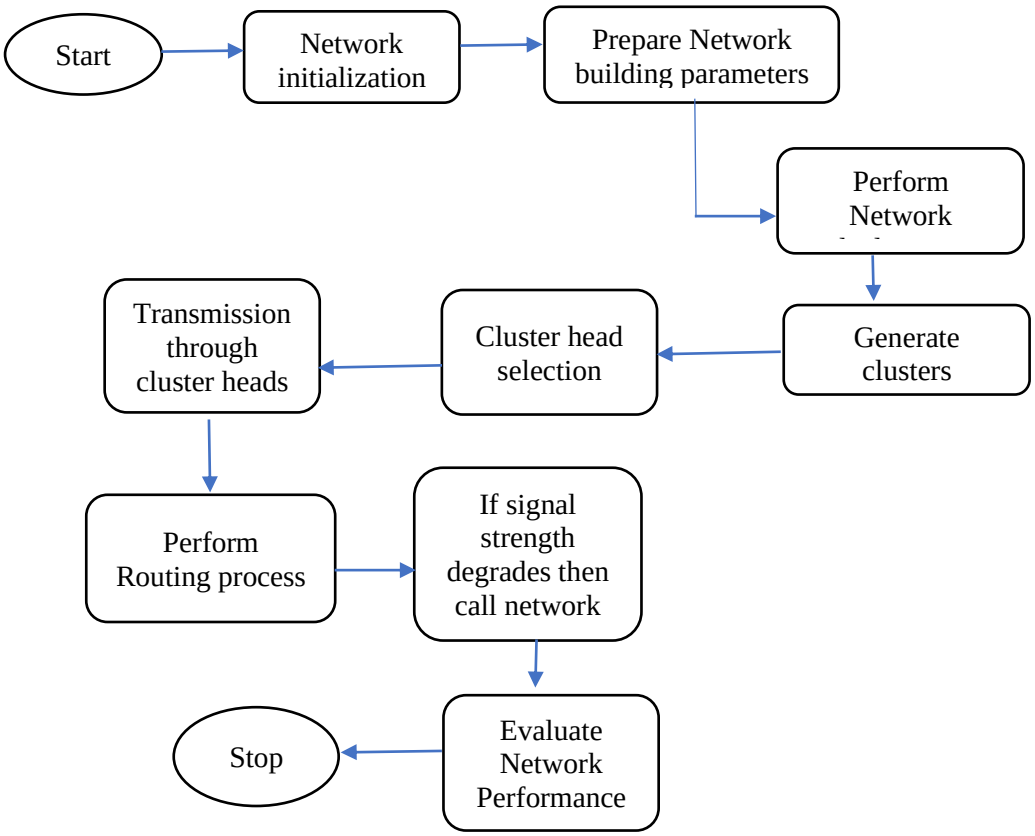

Figure 3 Proposed Energy Efficient System Model

RESEARCH ARTICLE

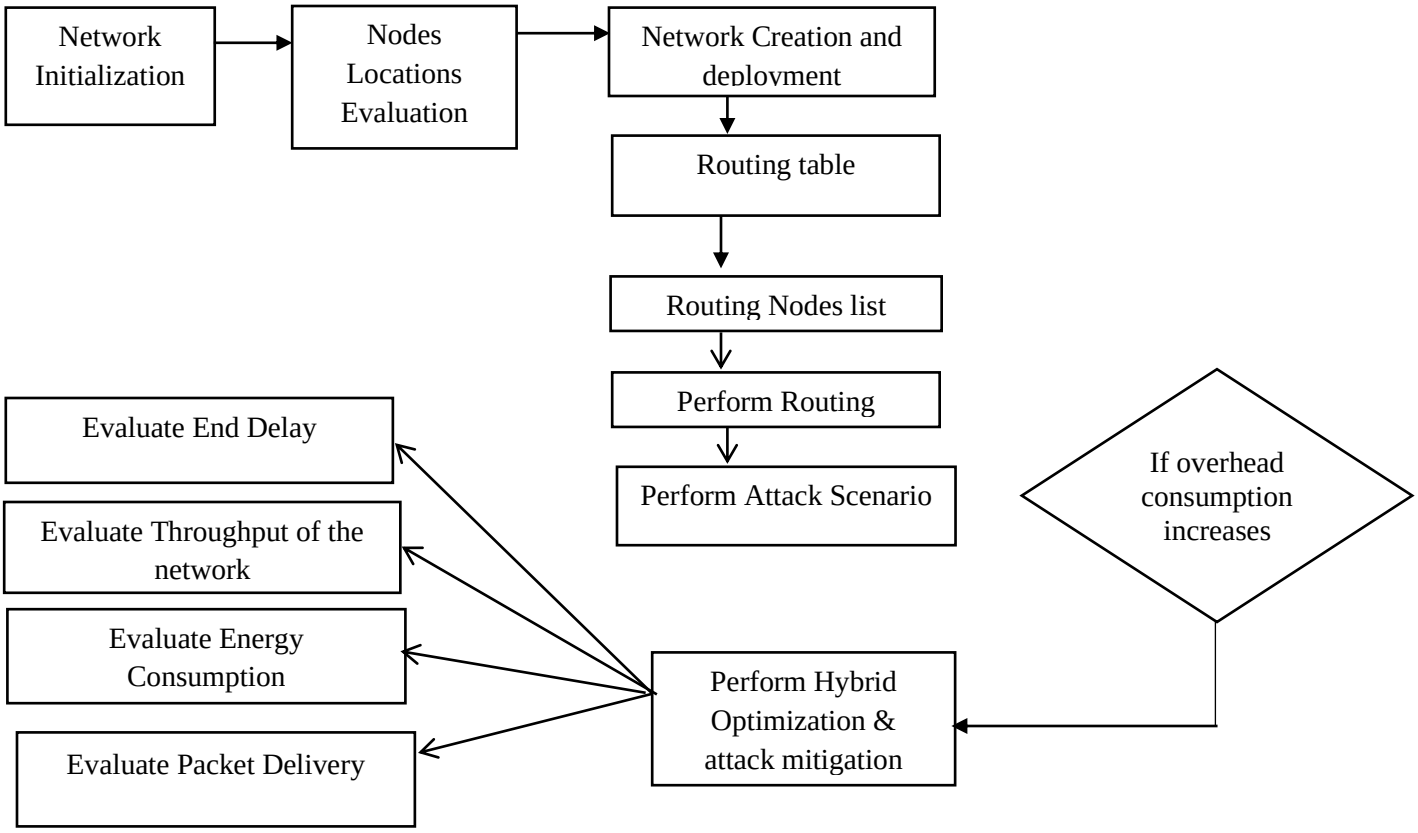

Figure 4 Proposed Energy Efficient Security Model

Step 1. Define the structure of the Network by initializing the specifications:

i. Determine the network length and width.

ii. Specify the network initial network parameters:

a. Aggregation energy

b. transmission ranges

c. initial delay factors

Step 2. Perform network deployment:

Deploy the network nodes based on uniform distribution.

Step 3. PSO (Particle Swarm Optimization) Phase:

i. Initialize PSO parameters:

a. Number of particles

b. Maximum iterations for PSO

c. Cognitive coefficient (c1)

d. Social coefficient (c2)

e. Velocity and position of each particle

ii. Define the fitness function

iii. For each iteration in PSO:

For each particle:

a. Update particle velocity and position based on current, personal best, and global best positions

b. Assign best particle's position based on fitness evaluation.

c. Evaluate particles convergence performance and update personal and global best if necessary

Step 4. Moth Flame Optimization (MFO) Phase:

i. Initialize MFO parameters:

a. Number of moths (flames)

b. Maximum iterations for MFO

c. Position of each moth

ii. Use the PSO performance as the initial positions for MFO

iii. For each iteration in MFO:

For each moth:

a. Update moth position towards the flame using the spiral update mechanism

b. Assign moth's position based on high bright intensities

RESEARCH ARTICLE

c. Evaluate performance and update flames based on the best solutions found

iv. Define the structure of the Neural Network (NN):

a. Determine the number of layers (input, hidden, and output layers)

b. Specify the number of neurons in each layer

c. Finalize NN weights to the best solution found by MFO

Step 5. Final Evaluation:

i. With the NN weights optimized through PSO followed by MFO, perform a final evaluation of the NN on the training dataset.

ii. Validate the optimized NN model based on predicted network error rates.

Step 6. Evaluate Performance:

i. Assess the network performance in terms of:

a. high network lifetime

b. throughput

c. end delay

d. high packet deliveries

Algorithm 1 Proposed Algorithm Secure Location Aware Energy Efficient Routing (SLAEER)

Explanation: The Algorithm 1: provides a clear, step-by-step procedure for optimizing a neural network using a hybrid PSO-MFO approach to enhance network performance.

1. Network Structure Definition: The network is initialized by defining its size and the parameters required for communication, like energy, transmission range, and delay factors.
2. Network Deployment: Once the structure is defined, nodes (UAVs) are deployed across the network area in a uniform distribution, which ensures optimal coverage.
3. PSO Phase:

✓ Particle Swarm Optimization (PSO) is used to find optimal positions for UAVs by iteratively adjusting the particles' positions. This phase optimizes network parameters such as energy usage and communication efficiency.

✓ Each particle in the swarm explores the search space and updates its position based on its personal best and the global best found so far. This ensures the optimization process converges toward the most efficient solution.

4. Moth Flame Optimization (MFO) Phase:

✓ MFO is used to further refine the solutions found by PSO. Moths in the optimization process move toward brighter flames (better solutions) using a spiral update mechanism. This phase fine-tunes the network's parameters for even better optimization.

5. Neural Network (NN) Setup:

✓ Once the best solutions are found through PSO and MFO, these solutions are used to optimize the weights of a neural network, which is designed to predict and evaluate network performance metrics.

6. Final Evaluation:

✓ After the NN is trained with optimized weights, its performance is evaluated to ensure the optimized parameters yield better network performance.

7. Network Performance Evaluation:

✓ Finally, the performance of the network is assessed in terms of key metrics such as lifetime, throughput, delay, and packet delivery. These metrics provide insights into the practical performance of the optimized FANET.

5. RESULTS AND DISCUSSIONS

The section delves into the discussion of the recommended deployment, executed within the MATLAB framework. Examination of the derived outcomes reveals that the utilization of a backpropagation neural network surpasses other models, particularly in achieving reduced energy usage and minimal latency. These improvements significantly extend the network's operational lifespan, marking a highly sought-after result. This enhancement in performance underscores the efficacy of backpropagation neural networks in optimizing critical parameters that contribute to the overall sustainability and efficiency of networks. By focusing on lowering energy demands and decreasing delay times, the proposed solution not only ensures a more reliable and longer-lasting network but also sets a new benchmark for future research in network design and implementation strategies within a MATLAB environment. This study's findings highlight the potential for significant advancements in network performance, opening avenues for further exploration in the field. Furthermore, the model's ability to balance computational efficiency with accuracy positions it as a practical solution for real-time network scenarios. Its scalability and robustness offer significant potential for deployment in diverse applications, such as disaster response and smart logistics. This advancement establishes a strong foundation for refining optimization strategies in future network implementations. The model achieves better results by employing adaptive optimization techniques, fine-tuning network operations to minimize energy consumption and latency, thereby improving overall efficiency and reliability.

RESEARCH ARTICLE

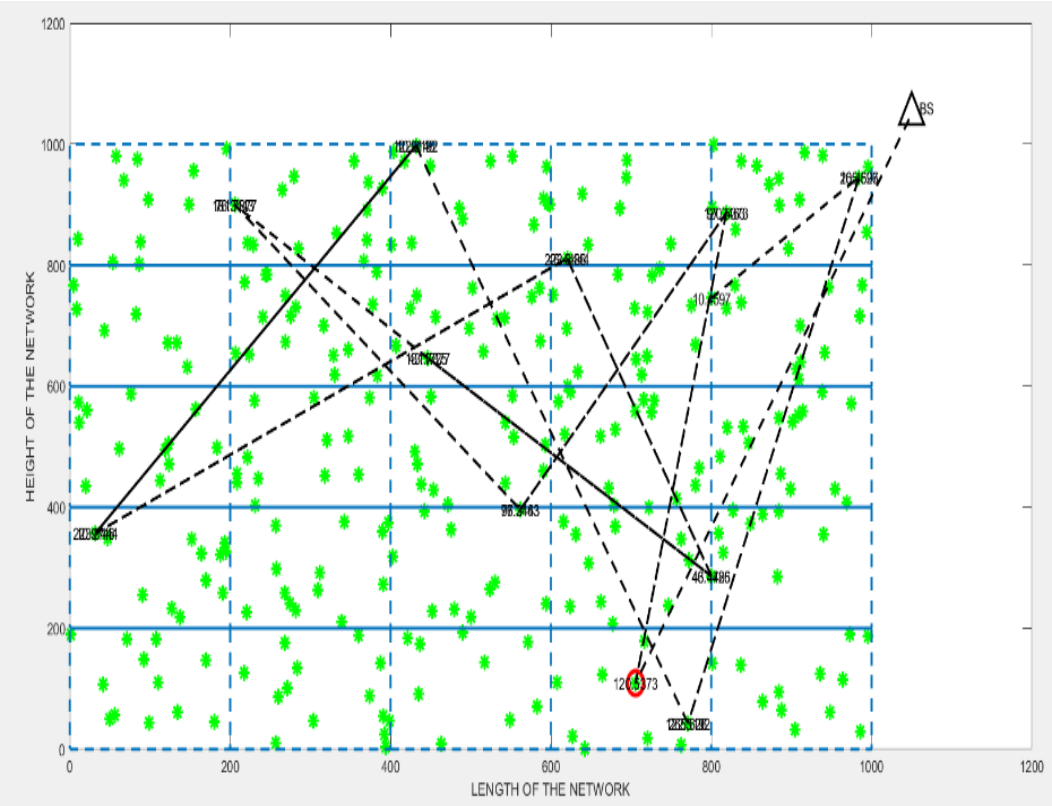

Figure 5 FANET Network Deployment

Figure 5 illustrates the organization of nodes using a hierarchical clustering approach, where the nodes within a cluster are represented by the colour green. In each cluster, a cluster head is designated through an election process. This model ensures that each node possesses an identical chance of being selected as the cluster head. The chosen cluster head serves a pivotal role as the intermediary, facilitating communication and data transfer between different clusters. This setup aims to optimize the network's efficiency and reliability by streamlining the process of information exchange across the hierarchical structure.

This structured arrangement enhances the network's scalability and performance by leveraging the cluster heads to manage and distribute the workload effectively. As a result, it mitigates potential bottlenecks and ensures a more balanced distribution of data processing tasks. The framework's design prioritizes equal opportunity for all nodes to participate in leading roles, thereby fostering a democratic and efficient network management system. Through this method, the hierarchical clustering model not only improves the robustness of the network but also contributes to a more efficient utilization of resources, facilitating smoother and more reliable inter-cluster communication. The outcomes are evaluated in two phases as given below.

The performance of the proposed model is evaluated in terms of low data gathering latency, low energy consumption, high throughput and low end to end delay.

The latency is evaluated as

The latency is evaluated using the given formula, where it considers the total network nodes, energy consumption, and data aggregation impact to measure delay in FANET communication (equation (1)).

$$L = \sum_{k=1}^{n} \binom{n}{k} (E(k) \times A(n)) \div N) \times \beta \qquad (1)$$

Where $E \rightarrow$
$Energy\ consumed\ by\ the\ Alive\ nodes\ to\ transfer\ the\ packets$

$A \rightarrow Number\ of\ alive\ nodes$

β
$\rightarrow Training\ error\ rate\ in\ transferring\ the\ packets\ from\ source\ to\ the\ destination$

$N \rightarrow Total\ route\ nodes\ to\ transfer\ the\ packets$

The end delay is evaluated as

RESEARCH ARTICLE

The end-to-end delay is evaluated using the given formula, considering network size, latency, overhead, and data aggregation to measure transmission efficiency in FANETs (equation (2)).

$$\text{ED} = \sum_{k=1}^{n} \binom{n}{k} (\text{L(k)} \times Ov(n)) \div A(n)) \times \beta \qquad (2)$$

Where $L \rightarrow$ *Total Latency achieved in gathering the information on alive nodes*

$A \rightarrow$ *Number of alive nodes*

$Ov \rightarrow$ *Overhead consumption achieved after optimizing the network*

$\beta \rightarrow$ *Training error rate in transferring the packets from source to the destination*

The energy consumption is evaluated as

Energy consumption is evaluated using the given formula, considering end-to-end delay, network load, and node distribution to measure power efficiency in FANETs (equation. (3)).

$$\text{EC} = \sum_{k=1}^{n} \binom{n}{k} (\text{ED(k)} \times L(n)) \div N(k))) \times \beta \qquad (3)$$

WhereED $\rightarrow$ *Total end to end delay of the network*

$L \rightarrow$ *Latency achieved in gathering packets to transmit*

$\beta \rightarrow$ *Training error rate in transferring the packets from source to the destination*

$N \rightarrow$ *Total number of route nodes evaluated*

The throughput is evaluated as

Throughput is evaluated using the given formula, considering overhead, latency, and energy consumption to measure the effective data transmission rate in FANETs (equation (4)).

$$\text{Tp(i)} = \sum_{k=1}^{n} \text{mean}\big(\text{Ov(k)} \times L(k)\big) \times Ec(k))) \div N \qquad (4)$$

WhereTp $\rightarrow$ *Total throughput of the network*

$L \rightarrow$ *Latency achieved in gathering packets to transmit*

$Ov \rightarrow$ *Overhead consumption achieved after optimizing the network*

$N \rightarrow$ *Total number of route nodes evaluated*

5.1. Proposed Implementation Outcome Based on Energy Efficiency

This section covers the results implemented without implementing the security threat in the network. It covers the optimization scenario if network fails to achieve the signal strengths and high path losses, delays and the matrices has been evaluated, usings equation mentioned at section 5.

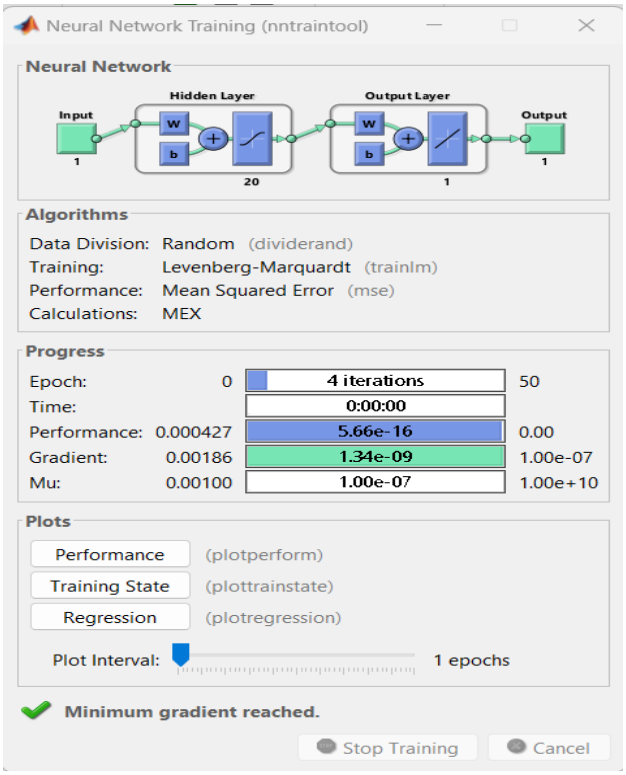

Figure 6 FANET Network Deployment

Figure 6 illustrates the network's training using the backpropagation technique. This Backpropagation Neural Network demonstrates a rapid processing speed, quick responsiveness, and the capacity for self-directed learning. It effectively manages the impact of network topology by achieving a reduced mean square error rate during training.

The training process is notable for requiring fewer epochs and minimal adjustments to connection weights, thereby decreasing the network's unpredictability. This streamlined approach enhances the efficiency of the BPNN, enabling it to adapt and optimize its structure more effectively. By limiting the necessity for extensive weight modifications, the network maintains stability and improves its ability to predict and analyse with precision. Consequently, this analysis not only expedites the learning process but also contributes to a more consistent and reliable performance of the neural network.

RESEARCH ARTICLE

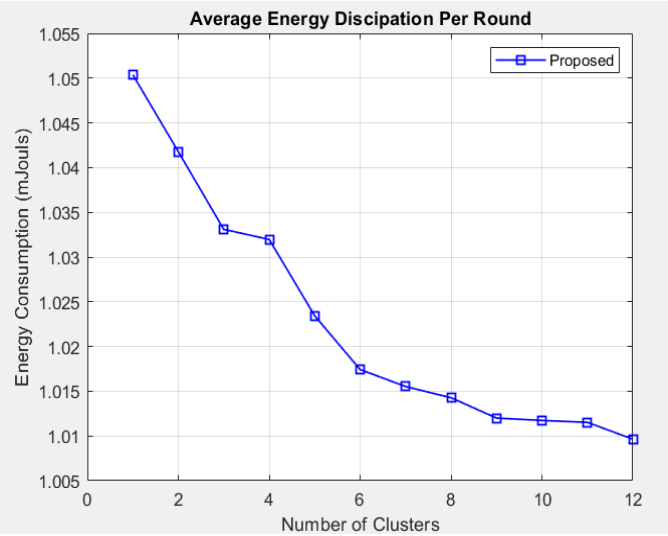

Figure 7 Average Energy Dissipation

Figure 7 illustrates the energy usage within the network, highlighting that the suggested method leads to reduced energy consumption, a crucial factor in enhancing energy efficiency. Minimizing energy consumption in FANETs is crucial for preserving higher levels of residual energy, which plays a vital role in ensuring successful packet transmissions in subsequent cluster rounds. The proposed strategy prioritizes energy efficiency, contributing to the network's overall performance while significantly extending its operational lifespan. By conserving energy, the approach ensures sufficient resources for future communication tasks, enhancing the network's reliability in managing data transmissions across its clusters.

The importance of optimizing energy usage lies in sustaining communication capabilities within FANETs. Through strategic reductions in energy expenditure, the network can effectively handle packet transmission processes over extended periods. This conservation of energy resources directly supports the prolonged functionality of FANETs, creating a reliable framework for continuous data exchange. By focusing on efficient energy management, this approach not only improves network performance but also strengthens the overall robustness of FANET operations.

Figure 8 presents an analysis of the cumulative delay experienced in the process of data collection for transmission across nodes. This aspect is fundamental within the network architecture, as minimizing latency is essential for reducing queue waiting times and, consequently, decreasing network congestion. This focus on reduced latency directly contributes to more efficient data flow, leading to a more streamlined network operation where information moves swiftly, enhancing overall performance and reliability. By prioritizing swift data transfer and low latency, the network ensures optimal utilization of resources, thereby minimizing potential bottlenecks and improving the user experience through faster communication and data processing capabilities. The latency computed using equation (1).

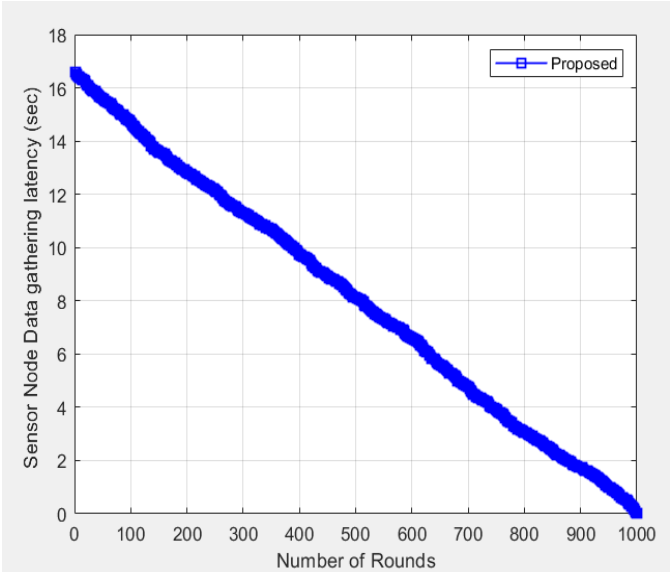

Figure 8 Data Gathering Latency

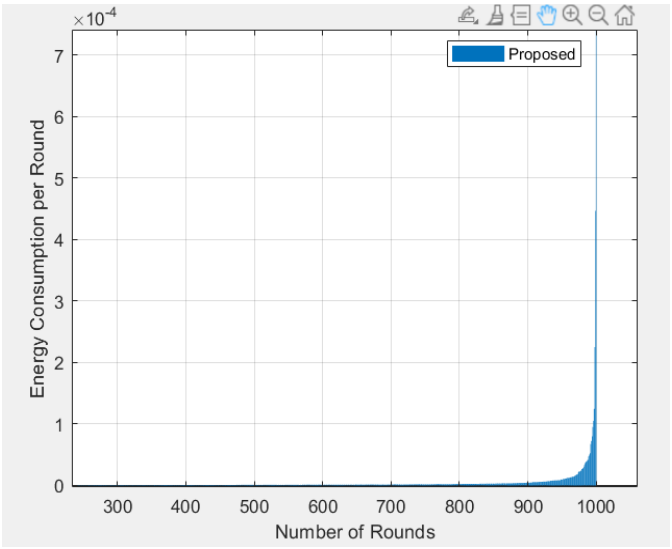

Figure 9 Energy Consumption Per Round

Figure 9 presented the energy usage per round. In the context of hierarchical clustering, packet exchanges are managed based on the cycle count. Additionally, as the cycle number grows, it becomes possible to gauge network performance through the monitoring of energy usage per cycle, alongside the tally of operational and non-operational nodes. This approach enables an effective assessment of the network's efficiency and sustainability over time, offering insights into the balance between energy expenditure and network

RESEARCH ARTICLE

longevity. Furthermore, this outcome supports the optimization of network by identifying critical thresholds for energy consumption that influence the network's operational lifespan.

It emphasizes the importance of strategic packet transmission planning and the role of cycle-based management in preserving network resources. Ultimately, such analysis contributes to the development of more energy-efficient networking solutions, aiming to prolong the functional period of nodes while maintaining high levels of data transmission efficiency. The energy consumption computed using equation (3).

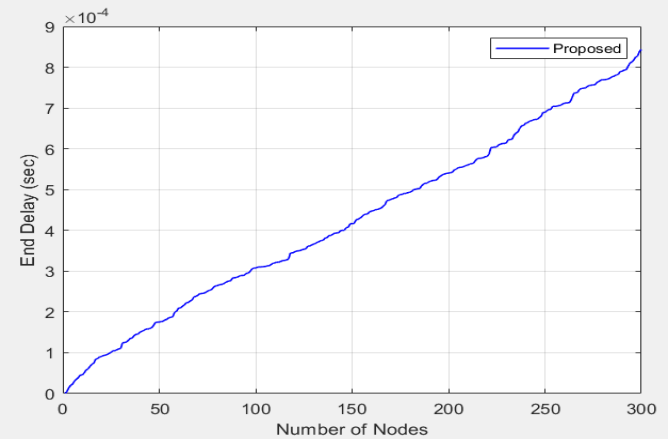

Figure 10 End Delay

Figure 10 illustration reveals a reduction in network latency due to our innovative method, which enhances the overall throughput. Latency impacts the rate at which data packets are relayed from clusters to the central station, minimizing potential bottlenecks. Enhanced latency among UAVs leads to prompt data transmission, reducing the likelihood of disruptions within the network.

This streamlined data flow ensures efficient communication and mitigates the risk of data transmission errors, thereby bolstering network reliability and performance. Our strategy focuses on optimizing the routing process, ensuring that data packets navigate through the network with minimal interference and delay. By addressing the critical aspect of latency, we significantly improve the network's capacity to handle high volumes of data swiftly and effectively, making it more robust against potential failures. The end-delay computed using equation (2).

5.2. Proposed Implementation Outcome Based on Secure Network

This section covers the results implemented including the security of the network that covers the hybrid optimization with training of the network layers using back propagation neural network.

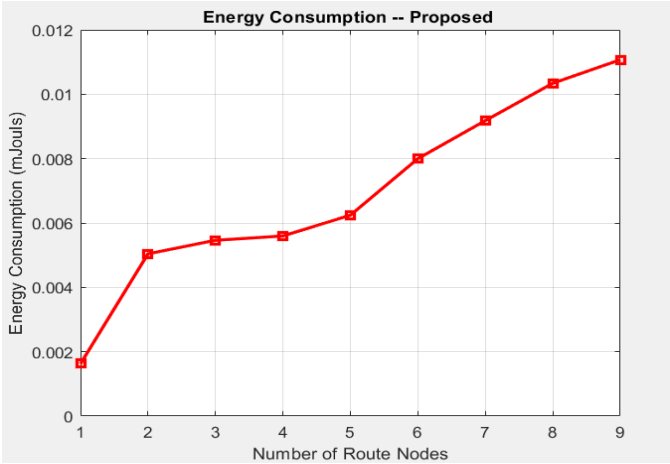

Figure 11 Energy Consumption (mJ)

Figure 11 presents data on the network's energy usage following the implementation of countermeasures against a security threat. Observations indicate a reduction in energy expenditure relative to the count of routing nodes, which is an optimal outcome. Elevated energy consumption is linked to a decline in network efficiency, highlighting the importance of maintaining low energy levels to ensure high throughput. This correlation underscores the significance of strategic interventions in minimizing energy consumption to enhance the network's performance and reliability.

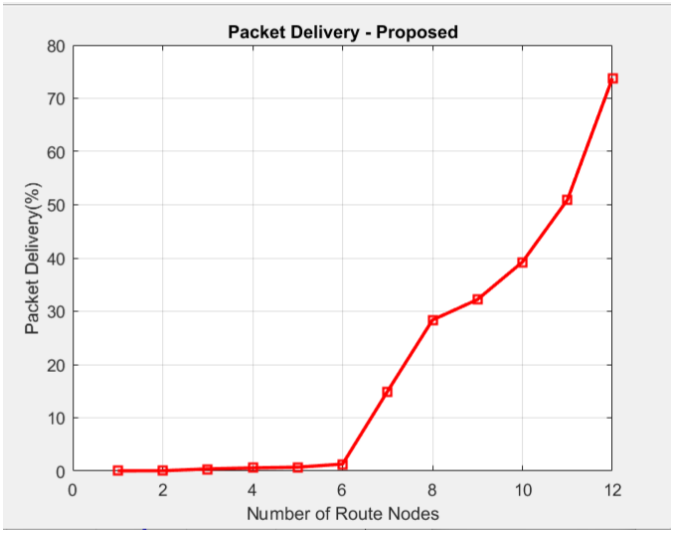

Figure 12 Packet Delivery (Proposed)

Figure 12 illustrates the packet delivery ratio of the proposed routing protocol in a wireless network improves significantly as the number of route nodes increases. Initially, with fewer nodes (0-5), the packet delivery remains low, suggesting limited routing options that restrict efficient data transmission. However, once the route node count exceeds six, the packet delivery rate rises sharply, reaching around 70% with twelve

RESEARCH ARTICLE

nodes. This trend indicates that the protocol benefits from a higher density of route nodes, enhancing network reliability and robustness by utilizing multiple paths, which reduces packet loss and improves successful data transmission. This analysis highlights the importance of routing node density in optimizing packet delivery performance within the network.

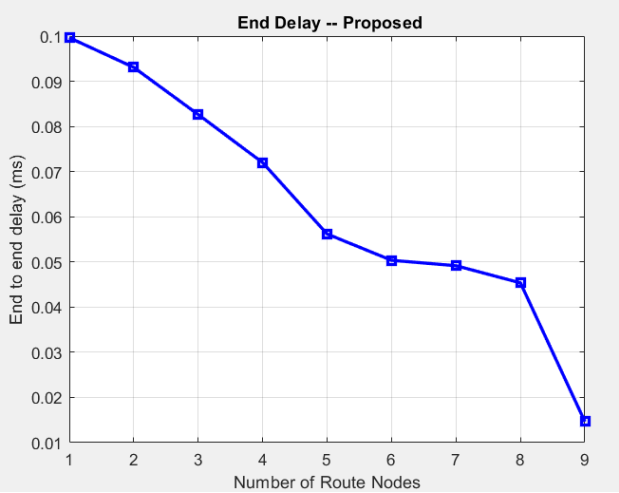

Figure 13 End Delay

Figure 13 presents the network's latency post-attack mitigation, highlighting a decrease in the time it takes for packets to travel from their origin to their destination. This outcome is favourable, indicating enhanced efficiency in data transmission. Conversely, a rise in latency suggests longer routes and extended delivery times, which is not optimal. Enhanced strategies for mitigating such attacks are crucial in maintaining the integrity and efficiency of network operations, ensuring that data flows remain unimpeded and reach their intended destinations promptly. This research focuses on the effectiveness of these strategies, demonstrating their impact on reducing network delays and improving overall performance.

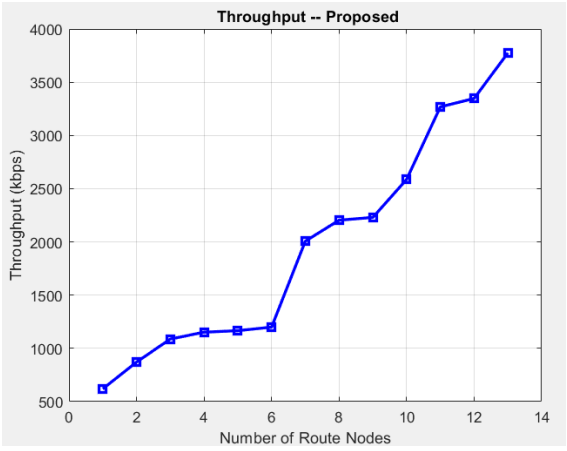

Figure 14 Network Throughput

Figure 14 presented the network's performance improvement following the implementation of countermeasures against the attack. Minimizing energy consumption in FANETs is crucial for preserving higher levels of residual energy, which plays a vital role in ensuring successful packet transmissions in subsequent cluster rounds. The proposed strategy prioritizes energy efficiency, contributing to the network's overall performance while significantly extending its operational lifespan. By conserving energy, the approach ensures sufficient resources for future communication tasks, enhancing the network's reliability in managing data transmissions across its clusters. The throughput computed using equation (4).

The importance of optimizing energy usage lies in sustaining communication capabilities within FANETs. Through strategic reductions in energy expenditure, the network can effectively handle packet transmission processes over extended periods. This conservation of energy resources directly supports the prolonged functionality of FANETs, creating a reliable framework for continuous data exchange. By focusing on efficient energy management, this approach not only improves network performance but also strengthens the overall robustness of FANET operations.

5.3. Secure Location Aware Energy Efficient Routing (SLAEER)Protocol: A Performance Analysis

The performance of the proposed SLAEER protocol is evaluated by comparing it with existing protocols such as G-OLSR, OLSR, and WOA-OLSR. MATLAB is employed for simulating and analyzing various performance metrics, allowing for a comprehensive comparison of the protocols in terms of efficiency, throughput, and energy consumption. Table 2 this evaluation aims to highlight the advantages of SLAEER in real-world network scenarios.

The SLAEER protocol is compared with reference to the metrics mentioned below:

Table 2 Pre-Defined Input Parameter

Parameter	Value
Number of nodes	0, 5, 10, 15, 20, 25, 30
Packet rate (packets/second)	10
Packet Size	512 bytes
Traffic type	CBR
Number of connections	5, 10, 15, 20, 25, 30
Mobility	Random waypoint Model
Minimum speed (m/s)	5
Maximum speed(m/s)	20

RESEARCH ARTICLE

Network area	1000 m *X* 1000 m
Simulation time (Sec)	500
Total Numbers of Nodes	300

5.3.1. Energy Consumption

Privacy-preserving techniques like cryptographic methods and additional routing steps increase energy consumption. However, lightweight strategies, such as location shifting, tend to have a smaller impact on energy use.

Table 3 Energy Consumption Comparison

M-OLSR	WOA-OLSR	SLAEER
6.5	3	0.008

In Table 3 comparison focuses on the energy consumption of three routing protocols: M-OLSR, WOA-OLSR, and SLAEER, showing clear differences in their performance. M-OLSR demonstrates the highest energy consumption at 6.5, making it less suitable for energy-sensitive applications. In comparison, WOA-OLSR shows improved energy efficiency with a consumption of 3 units, reflecting a better balance between performance and power usage. However, SLAEER emerges as the most energy-efficient protocol, consuming only 0.008 units of energy. This significant reduction in energy consumption positions SLAEER as the optimal solution for applications requiring low power usage, such as FANETs, where extended operational durations and enhanced network performance are critical. The comparison underscores SLAEER's superiority in energy efficiency for performance-driven, energy-conscious applications (Figure 15).

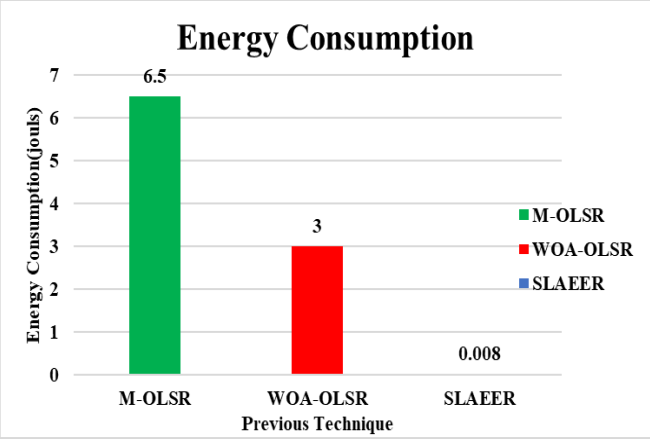

Figure 15 Energy Consumption Comparison

5.3.2. Packet Delivery Ratio (PDR)

Privacy-preserving techniques, by obscuring routing information, may reduce the packet delivery ratio slightly. However, intelligent routing protocols can help maintain an acceptable level of PDR.

Table 4 Packet Delivery Ration Comparison

OLSR	G-OLSR	SLAEER
0.934	.971	0.982

In Table 4 the data evaluates the performance of three routing protocols—OLSR, G-OLSR, and SLAEER based on specific criteria like efficiency or reliability. OLSR achieves a performance value of 0.934, indicating its moderate capability in managing network operations effectively. G-OLSR shows an improvement with a value of 0.971, highlighting advancements in efficiency or reliability compared to OLSR. However, SLAEER stands out with the highest performance value of 0.982, showcasing its exceptional ability to optimize network parameters. This means SLAEER not only surpasses OLSR and G-OLSR in terms of effectiveness but also proves to be the most reliable and efficient for applications requiring high-performance routing, such as in FANETs. This superior performance makes SLAEER a preferred choice for energy-critical and real-time scenarios, ensuring better data transmission, reliability, and overall network stability (Figure 16).

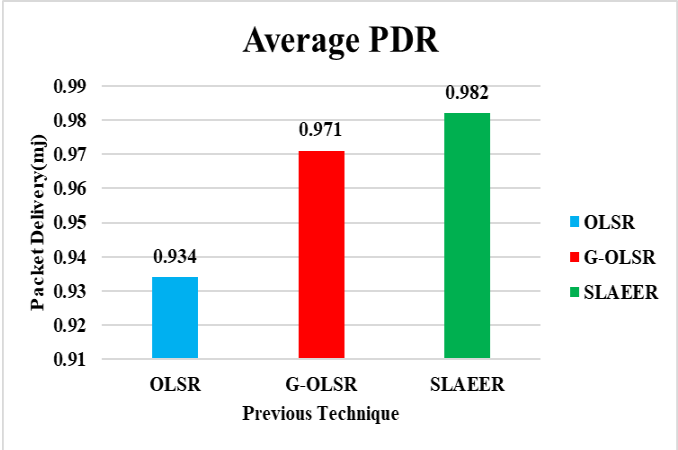

Figure 16 Packet Delivery Comparison

5.3.3. End-to-End Delay

Encryption and more complex routing decisions for privacy can lead to increased processing time, which may raise the end-to-end delay. Optimized solutions can minimize these delays while maintaining privacy.

Table 5 End-to-End Delay Comparison

OLSR	G-OLSR	SLAEER
0.4	0.3	0.009
0.4	0.38	0.009

RESEARCH ARTICLE

The Table 5 Shows the end-to-end delay comparison between OLSR, G-OLSR, and SLAEER highlights significant differences in performance. In the first round, SLAEER demonstrates the lowest delay at 0.009 seconds, making it the most efficient protocol in terms of latency. G-OLSR follows with a slightly higher delay of 0.3 seconds, while OLSR has the highest delay at 0.4 seconds. In the second round, SLAEER maintains its exceptional performance with a consistent delay of 0.009 seconds, while G-OLSR shows a minor increase to 0.38 seconds. OLSR again experiences the highest delay, remaining at 0.4 seconds. The results show that SLAEER is the optimal choice for applications requiring minimal latency, while G-OLSR provides a balance between performance and delay. OLSR, although still functional, exhibits higher delays, making it less suitable for low-latency environments. This comparison underlines the importance of selecting a protocol based on the specific delay requirements of the application (Figure 17).

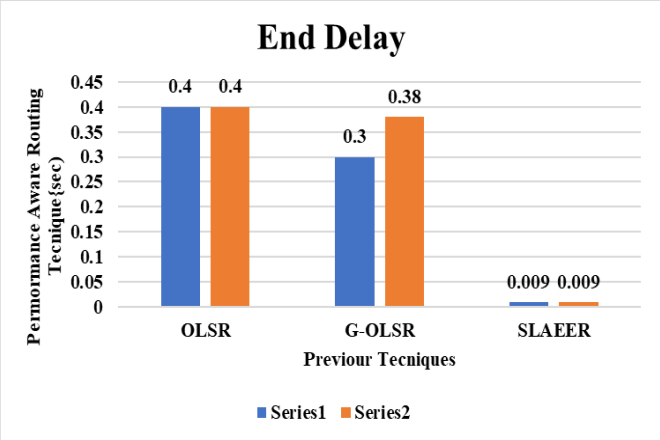

Figure 17 End Delay Comparison

5.3.4. Throughput

Throughput could be negatively affected by the added overhead from encryption and routing. Nonetheless, well-designed privacy protocols can reduce this impact, ensuring that throughput remains efficient.

Table 6 Throughput Comparison

OLSR	G-OLSR	SLAEER
79.68	83.5	182.01

The Table 6 provides a comparison of the throughput performance of three routing protocols: OLSR, G-OLSR, and SLAEER. OLSR achieves a throughput of 79.68, reflecting an average performance in data transmission. G-OLSR slightly outperforms it, with a throughput of 83.5, indicating better network efficiency and data delivery. However, SLAEER significantly surpasses both protocols with an impressive throughput of 182.01, showcasing its superior data management and transmission capabilities. This remarkable performance highlights SLAEER's effectiveness in handling larger data volumes, making it particularly well-suited for demanding applications like FANETs. In such environments, maintaining high throughput is critical to ensuring seamless communication and optimal operational efficiency (Figure 18).

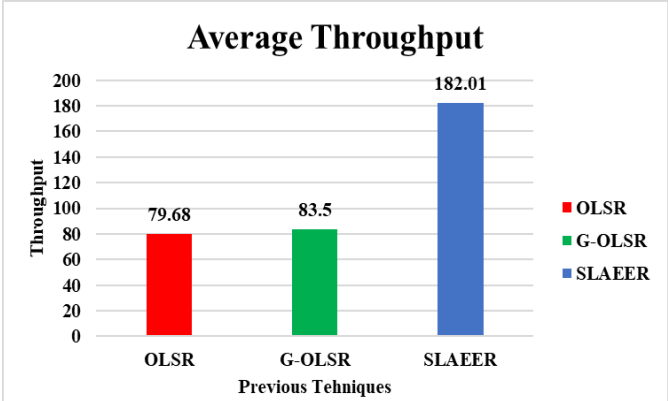

Figure 18 Throughput Comparison

Table 7 Proposed Comparison

Parameters	Base G-OLSR	Proposed (SLAEER)
Energy Consumption (mJ)	3.2	0.008
End to End Delay (sec)	0.28	0.009

Table 7: The proposed SLAEER protocol significantly outperforms G-OLSR in terms of energy efficiency and latency. SLAEER consumes only 0.008 mJ compared to G-OLSR's 3.2 mJ, demonstrating superior energy optimization. Additionally, SLAEER reduces end-to-end delay to 0.009 seconds, far lower than G-OLSR's 0.28 seconds, ensuring faster and more efficient data transmission in FANETs.

6. CONSLUSION

This research presents a transformative approach to addressing the multifaceted challenges inherent in Flying Ad-Hoc Networks (FANETs). By integrating clustering methodologies with advanced hybrid optimization and artificial intelligence techniques, the study achieves significant improvements in routing efficiency, energy consumption, and network security. The proposed framework not only minimizes network congestion and overhead but also establishes robust defence mechanisms to safeguard against sophisticated cyber threats, ensuring a secure and reliable communication environment.

RESEARCH ARTICLE

The research highlights substantial advancements in Quality of Service (QoS) metrics, including enhanced throughput, reduced latency, improved packet delivery ratio, and optimized energy usage. These enhancements are crucial for supporting the dynamic and resource-constrained nature of FANETs, making them more adaptable to real-world applications such as surveillance, disaster management, and military operations. Furthermore, the emphasis on a holistic approach—encompassing routing optimization, security fortification, and performance enhancement—sets a new benchmark for future developments in this field. The novel application of artificial intelligence and hybrid optimization methods in FANETs demonstrates a forward-looking strategy for creating scalable, adaptive, and efficient network infrastructures. This research not only addresses current limitations in FANET operations but also provides a foundation for continuous innovation in aerial communication networks. By systematically tackling critical challenges such as energy efficiency, network robustness, and secure data transmission, the study contributes to shaping the next generation of FANET technologies. In conclusion, this comprehensive framework serves as a blueprint for optimizing the operational dynamics of FANETs, ensuring their resilience and effectiveness across diverse scenarios. The future scope of this research lies in advancing the Quality of Service (QoS) in FANET operations by developing more adaptive, energy-efficient, and secure protocols. These enhancements will enable resilient aerial communication networks, supporting diverse applications such as disaster management, smart logistics, and environmental monitoring. Integration with emerging technologies like AI and 5G will further optimize performance, ensuring scalability and reliability in dynamic scenarios.

REFERENCES

[1] H. Ali, S. ul Islam, H. Song, and K. Munir, “A performance-aware routing mechanism for flying ad hoc networks,” Trans. Emerg. Telecommun. Technol., vol. 32, no. 1, pp. 1–17, 2021, doi: 10.1002/ett.4192.

[2] J. Liu et al., “QMR:Q-learning based Multi-objective optimization Routing protocol for Flying Ad Hoc Networks,” Comput. Commun., vol. 150, pp. 304–316, 2020, doi: 10.1016/j.comcom.2019.11.011.

[3] N. I. Mowla, N. H. Tran, I. Doh, and K. Chae, “AFRL: Adaptive federated reinforcement learning for intelligent jamming defence in FANET,” J. Commun. Networks, vol. 22, no. 3, pp. 244–258, 2020, doi: 10.1109/JCN.2020.000015.

[4] X. Li, F. Deng, and J. Yan, “Mobility-assisted adaptive routing for intermittently connected FANETs,” IOP Conf. Ser. Mater. Sci. Eng., vol. 715, pp1-6, no. 1, 2020, doi: 10.1088/1757-899X/715/1/012028.

[5] Q. Sang, H. Wu, L. Xing, H. Ma, and P. Xie, “An Energy-Efficient Opportunistic Routing Protocol Based on Trajectory Prediction for FANETs,” IEEE Access, vol. 8, pp. 192009–192020, 2020, doi: 10.1109/ACCESS.2020.3032956.

[6] C. Pu, “Jamming-Resilient Multipath Routing Protocol for Flying Ad Hoc Networks,” IEEE Access, vol. 6, no. c, pp. 68472–68486, 2018, doi: 10.1109/ACCESS.2018.2879758.

[7] T. Ahn, J. Seok, I. Lee, and J. Han, “Reliable Flying IoT Networks for UAV Disaster Rescue Operations,” Mob. Inf. Syst., vol. 2018, no. ii,pp 1-12 2018, doi: 10.1155/2018/2572460.

[8] R. Duan, J. Wang, C. Jiang, Y. Ren, and L. Hanzo, “The Transmit-Energy vs Computation-Delay Trade-Off in Gateway-Selection for Heterogenous Cloud Aided Multi-UAV Systems,” IEEE Trans. Commun., vol. 67, no. 4, pp. 3026–3039, 2019, doi: 10.1109/TCOMM.2018.2889672.

[9] J. Gu, T. Su, Q. Wang, X. Du, and M. Guizani, “Multiple Moving Targets Surveillance Based on a Cooperative Network for Multi-UAV,” IEEE Commun. Mag., vol. 56, no. 4, pp. 82–89, 2018, doi: 10.1109/MCOM.2018.1700422.

[10] Z. Zheng, A. K. Sangaiah, and T. Wang, “Adaptive Communication Protocols in Flying Ad Hoc Network,” IEEE Commun. Mag., vol. 56, no. 1, pp. 136–142, 2018, doi: 10.1109/MCOM.2017.1700323.

[11] F. Aftab, A. Khan, and Z. Zhang, “Hybrid Self-Organized Clustering Scheme for Drone Based Cognitive Internet of Things,” IEEE Access, vol. 7, pp. 56217–56227, 2019, doi:10.1109/ACCESS.2019.2913912.

[12] D. Liu et al., “A Coalition-Based Communication Framework for Task-Driven Flying Ad-Hoc Networks,” pp. 1–7, 2018, [Online]. Available: http://arxiv.org/abs/1812.00896.

[13] Namdev, Mayank, Sachin Goyal, and Ratish Agarwal. "An optimized communication scheme for energy efficient and secure flying ad-hoc network (FANET)." Wireless Personal Communications 120, pp 1291-1312 no. 2 (2021): 1291-1312.

[14] M. Tropea, P. Fazio, F. De Rango, and N. Cordeschi, “A new FANET simulator for managing drone networks and providing dynamic connectivity,” Electron., vol. 9, pp 1-18, no. 4, 2020, doi: 10.3390/electronics9040543.

[15] K. A. Darabkh, M. G. Alfawares, and S. Althunibat, “MDRMA: Multi-data rate mobility-aware AODV-based protocol for flying ad-hoc networks,” Veh. Commun., vol. 18, p. 100163, 2019, doi: 10.1016/j.vehcom.2019.100163.

[16] Y. He, X. Tang, R. Zhang, X. Du, D. Zhou, and M. Guizani, “A Course-Aware Opportunistic Routing Protocol for FANETs,” IEEE Access, vol. 7, pp. 144303–144312, 2019, doi: 10.1109/ACCESS.2019.2944867.

[17] J. Hong and D. Zhang, “TARCS: A topology change aware-based routing protocol choosing scheme of FANETs,” Electron., vol. 8, pp 1-13, no. 3, 2019, doi: 10.3390/electronics8030274.

[18] A. Khan, F. Aftab, and Z. Zhang, “BICSF: Bio-Inspired Clustering Scheme for FANETs,” IEEE Access, vol. 7, pp. 31446–31456, 2019, doi: 10.1109/ACCESS.2019.2902940.

[19] I. Mahmud and Y. Z. Cho, “Adaptive Hello Interval in FANET Routing Protocols for Green UAVs,” IEEE Access, vol. 7, pp. 63004–63015, 2019, doi: 10.1109/ACCESS.2019.2917075.

[20] A. Khan, F. Aftab, and Z. Zhang, “Self-organization based clustering scheme for FANETs using Glowworm Swarm Optimization,” Phys. Commun., vol. 36, p. 100769, 2019, doi: 10.1016/j.phycom.2019.100769.

[21] M. A. Khan, I. M. Qureshi, and F. Khanzada, “A hybrid communication scheme for efficient and low-cost deployment of future flying AD-HOC network (Fanet),” Drones, vol. 3, no. 1, pp. 1–20, 2019, doi: 10.3390/drones3010016.

[22] J. Souza, J. Jailton, T. Carvalho, J. Araújo, R. Francês, and Z. Kaleem, “A Proposal for Routing Protocol for FANET: A Fuzzy System Approach with QoE/QoS Guarantee,” Wirel. Commun. Mob. Comput., vol. 2019, pp. 1-14 doi: 10.1155/2019/8709249.

[23] R. Valentino, W. S. Jung, and Y. B. Ko, “A design and simulation of the opportunistic computation offloading with learning-based prediction for unmanned aerial vehicle (UAV) clustering networks,” Sensors (Switzerland), vol. 18, no. 11, 2018, doi: 10.3390/s18113751.

[24] T. Lagkas, V. Argyriou, S. Bibi, and P. Sarigiannidis, “UAV IoT framework views and challenges: Towards protecting drones as ‘things,’” Sensors (Switzerland), vol. 18, no. 11, pp. 1–21, 2018, doi: 10.3390/s18114015.

[25] K. Singh and A. K. Verma, “A fuzzy-based trust model for flying ad hoc networks (FANETs),” Int. J. Commun. Syst., vol. 31, no. 6, pp. 1–19, 2018, doi: 10.1002/dac.3517.

RESEARCH ARTICLE

Authors

Gaurav Jindal was born in India in 1978. He completed his Master's in Computer Applications from IMT Faridabad, affiliated with MD University, Rohtak. Currently, he is working as an Assistant Professor at Postgraduate Government College, Sector 46, Chandigarh, and is pursuing his Ph.D. in the Department of Computer Science at SGGSWU, Fatehgarh Sahib, India. His research interests include adaptive network management and algorithm analysis.

Dr. Navdeep Kaur, a distinguished academician and renowned subject expert in Computer Science at SGGSWU, Fatehgarh Sahib. Dr. Kaur earned her PhD in Computer Science and Engineering from IIT Roorkee in 2008 and boasts an impressive teaching career spanning over 25 years. As Professor and Head of the Department of Computer Science, Dr. Kaur leads the forefront in integrating cutting-edge technological trends, specializing in Software Engineering, Cloud Computing, and Network Security. Her research excellence is prominently displayed in her work on authentication protocols and secure data transfer within Flying Ad-hoc Networks (FANETs), reflected in numerous publications and citations on Google Scholar. Dr. Kaur has made significant contributions to the academic community with a substantial number of publications in SCI-indexed and Scopus-indexed journals, underscoring her impactful research achievements.

How to cite this article:

Gaurav Jindal, Navdeep Kaur, "Secure and Energy-Efficient Location-Aware Protocols for Flying Ad-Hoc Networks (FANETs)", International Journal of Computer Networks and Applications (IJCNA), 12(1), PP: 121-138, 2025, DOI: 10.22247/ijcna/2025/09.