SafeRoute: An Effective Hybrid Routing Mechanism for Enhanced Security and Reliability in UAV Networks

[1]Priyadharshini SP and [2]Balamurugan P
[1,2]Department of Networking and Communications, SRM Institute of Science and Technology,
Kattankulathur, Chennai, Tamil Nadu, India.
[1]ps9070@srmist.edu.in, [2]balamurp@srmist.edu.in

Correspondence should be addressed to Priyadharshini SP : ps9070@srmist.edu.in

Article Info
Journal of Machine and Computing (http://anapub.co.ke/journals/jmc/jmc.html)
Doi : https://doi.org/10.53759/7669/jmc202404085
Received 20 January 2024; Revised from 30 April 2024; Accepted 18 July 2024.
Available online 05 October 2024.

Abstract – Unmanned Aerial Vehicles (UAVs) provides various benefits in commercial and emergency response applications that pose unique challenges. The intrinsic mobility often changes the UAVs network topology, which results in packet losses and routing path failures. This dynamic nature increases its demand for robust solutions to maintain stable communication and secured routing protocols to ensure reliable communication. A new mechanism called SafeRoute has been designed to provide a secure and reliable routing solution in flying ad hoc networks. The objective of SafeRoute is to efficiently exchange data in a reliable manner. The proposed technique is an efficient hybrid approach encompassing the Firefly and Dragonfly Optimization Algorithms. The Firefly Algorithm works on the principles of the flashes of fireflies, in the formation of clusters and selection of the optimal cluster head. The Dragonfly Optimization Algorithm works by optimum path selection and imitates the static and dynamic swarming behaviors of dragonflies. Initial simulations and field tests reflects a major improvement in the stability and security of networks. The packet delivery ratio increased by 25%, and routing path failures decreased by 30% compared to existing protocols. Also decreased the vulnerability of common network attacks like Sybil and wormhole attacks by 40%. These observations have firmly established the potency of SafeRoute in enhancing the reliability and security of UAV communication in dynamic, high-mobility environments.

Keywords – Unmanned Aerial Vehicle, SafeRoute, Firefly Algorithm, Dragonfly Optimization Algorithm.

I. INTRODUCTION

UAV flying ad hoc networks, or UAV-FANETs, are highly dynamic, complex systems of communication formed by unmanned aerial vehicle nodes operating in flying ad hoc networks. These consist of a large number of unmanned aerial vehicles cooperating in swarms for an interlinked network to maintain real-time communications without permanent infrastructure. FANETs are part of the major engineering and network technology development specifically oriented toward adapting to the requirements of unmanned aerial systems [1]. The simplest constituency of a FANET might involve a wide scope of unmanned aerial vehicles, which can range from small aircraft, drones, airships, and balloons that fly at very high altitudes. These aerial units are assisted by some components on the ground, including control stations and smart antennas. They are very vital units in the management of the network. The unmanned aerial vehicles which make a FANET are designed to operate either independently or in a semi-autonomous manner for them to do coordinated duties such as surveillance and environmental monitoring. They should also maintain constant communication among themselves and with ground control [2].

The FANET communication structure is built over two major types of links. The first communication type is called UAV-to-UAV, or U2U communication, and it enables the UAVs composing the network to communicate directly. This mode is essential where operations involving a great number of UAVs must be coordinated, such as keeping formation, sensor data transmission, or even flight route adjustments in real time with respect to atmospheric conditions and mission requirements [3, 4]. The second kind of communication that can take place within FANETs is UAV-to-Base Station. In this mode, unmanned aerial vehicles establish an interaction with a central ground controlling station or base station. This station acts as the hub in analyzing data, giving commands, and monitoring the overall mission. Where the need is one of larger-scale operations coordination, with centralized decision-making at the center—like transmitting vital data to a control center or receiving complex orders that individual UAVs are tasked to perform—this communication link is very necessary. Jointly, these communication channels provide the backbone of FANETs. They ensure that the network remains strong, flexible, and able to support diverse aerial missions with their capability. FANET architecture allows for seamless communication among UAVs and ground stations, hence enabling efficient ways of controlling, coordinating, and executing tasks over large regions often challenging to navigate [5, 6]. Due to the non-hierarchical and infrastructure-less behaviour of FANETs, variety of security challenges raises for their adaptable data transfer [7].

They are classified by many criteria like dimensions, mass, altitude of operation, and wing configuration. Of the many categories, nano and mini-UAVs stand out as especially preferred because of their small size and efficiency. These unmanned aerial vehicles, therefore, weigh between 1 to 4 kilogrammes and are capable of flying at heights between 10 and 250 feet. Many of these devices also contain quadcopter wings and can reach speeds between 15 and 80 km per hour. The UAVs have characteristics such as lightweight, medium altitude, and speed variability that make them extremely suitable for all purposes. For search and rescue missions or even military operations, nano and small UAVs are very beneficial due to their excellent mobility and ability to handle different altitudes [8, 9]. This is quite important, considering the situations mentioned above. Apart from military uses these UAVs have great favor in civilian applications also. These are used in forest fire detection and monitoring, wind-related research, improving civilian security, and even finds use in agricultural activities. They also have a very significant role in assessing network activity and deliverance of online services in areas of disaster where conventional infrastructure may have been disrupted. The flexible design has made UAVs very useful for a wide range of applications, from aerial photography to event coverage like wedding picture taking. They seem to be able to do a lot of activities and function in various circumstances, proving their fast-growing importance within professional and leisure circles [10].

Given the fact that UAVs have a lot of advantages, it becomes quite evident that those aerial vehicles are going to be extremely significant within a number of advancing technologies because they have a good chance to become the key enabler for interconnecting several aspects of smart cities. This is in terms of communication between IoT devices, overlooking intelligent electric meters, and liaising with electric vehicles. UAVs can be involved in U2X (UAV-to-Everything) communications to support wireless bridging services for a large number of devices. Nevertheless, the integration of these diverse applications with UAVs introduces huge challenges. One of the prominent challenges is the transfer and routing of data among the communication infrastructures of UAV-to-UAV (U2U) and UAV-to-Base Station (U2BS). In addition to these challenges, the intrinsic features of UAVs, which include high manoeuvrability, low density of the network, and small battery capacity, pose another hurdle to ensuring dependable data routing in the network of UAVs. Security forms another crucial challenge in the provision. A number of cyberattacks are vulnerable to the communication systems of unmanned aerial vehicles, which threaten both the accuracy and dependability of the data delivered and impose great threats to public safety [11].

The principal concerns that effect viable data transfer within FANETs are routing and security. One of the novel techniques that has gained popularity to resolve these issues is the biological-inspired algorithms; a good number of these algorithms have derived attributes from the mimicking of characteristics portrayed by known dependable, flexible, and accurately synchronized insects. Most of the developed swarm-based routing algorithms not only follow the collective behavior of populations of insects at the most effective form of communication but also through the network [12]. Despite the bright performance potential of these bio-inspired routing algorithms, they face a number of serious challenges when it makes a practical application in FANETs. Due to high mobility, the positions of UAVs change very frequently—that is, latitude and longitude. Consistency of connections will be difficult for the protocols working based on the position. The design of these routing algorithms is increasingly complicated, requiring secure communication channels and effective dynamic management in terms of the UAV nodes [13]. Hence to overcome aforementioned drawbacks, present research provides the following contribution which is given as following,

1. To create clusters and to choose cluster heads with optimal results, Firefly Algorithm is employed as it models the process by a kind of self-organized behavior among fireflies.
2. For an optimal path selection in a routing, the algorithm goes under an assessment of the static and dynamic swarming behavior of dragonflies to assure a balance between exploration and exploitation in the search space.
3. Simulation and field testing of the proposed SafeRoute technique for assessing improvements in network stability and security. The SafeRoute scheme enhanced packet delivery by 25%, reduced routing path failures by 30%, and minimized exposure to common network attacks such as Sybil and wormhole attacks by 40%.

II. RELATED STUDY AND LITERATURE SURVEY

In the last decade, researchers across the world proposed solutions for FANETs using clustering. This section reviews the recent advances in clustering for FANETs. Initially, design integrating SDN-based cluster controllers was proposed to manage transmissions in a hierarchical manner. This architecture used the collaborative controller and applied a centralized traffic-differentiated routing strategy to guarantee QoS demands in each cluster. In this respect, different priorities are allotted to transmission flows with regards to their various degrees of activities [14]. Predictive models of transmission reliability evaluate authenticity and forwarding capability of the links.

A course-aware opportunistic routing protocol, known as CORF, has been developed specifically for FANETs [15]. In this method, the aeronautical data is shared among the nodes in each FANET so that the transmission can be enabled. The UAV source node, computes probabilistic transfer values taking into account the respective geographic positions. Several approaches proposed focus on route optimization; since setting up a reliable path is very crucial and enables effective data transmission, hence playing an important role in the performance of a FANET. Using acquired information; the UAV source node determines which are the next nodes in line towards the destination.

In a study [16], a survey was carried out on UAV routing protocols with emphasis on their design, structure, and features of operations. They categorized the protocols into topology, hierarchy, positional information, probabilistic analysis, and social media attributes. Eleven routing protocols were also analyzed with respect to their routing method, criteria for assessment, and other relevant variables. The authors conducted an evaluation to compare the strengths and weaknesses among these approaches using important parameters of the network architecture and a set of evaluation metrics. In another related work, the authors in [17] elaborated on issues and challenges that need to be handled by any routing protocol in FANETs. It provided useful solutions, hopefully, for those working on in-depth functioning in FANETs. The authors constructed a comprehensive classification system in which FANET routing protocols are divided into eight main and ten subgroups. The authors have explained each category in detail with the use of figures. After that, they conducted a comparative study on such techniques for the results to be more solid.

An adaptive algorithm for hello interval change was proposed, known as the Energy Efficient Hello Algorithm (EE-Hello) [18]. This approach provides four key mechanisms to extend improvements in conventional routing protocols of FANET. At the heart of this algorithm lies the increase in energy efficiency for UAVs. Computation of network density directly affects all other performance metrics of a network, including PDR and throughput. The algorithm adopts a great strategy wherein flying nodes optimize network performance while efficiently using available energy resources. This scheme also uses mission-specific information to compute the time gap between hello packets. Another strategy, called Jamming Resilient Multipath Routing Protocol (JARMROUT), was proposed [19] to secure the problem of jamming and deliberate disruptions generated in a network by malicious entities. Apart from that, it ensures continuous data flow by avoiding node-specific failures due to different nodes, which is a tremendous advancement of FANET performance.

The method follows a simplified analytical model, the results of which are either evaluated by the reception rate of Request REPly (RREP) packets. The performance of the protocol is evaluated using a simulation against three well-known routing protocols: Dynamic Source Routing (DSR), Optimised Link State Routing (OLSR), and Split Multipath Routing (SMR). There is also a new introduced class of protocol named CHNN-DSR [20] that provides more robust routing paths and makes communication efficient in FANETs. It is also observed after detailed analysis that the networks using CHNN-DSR are performing better, concerning the most critical network performance metrics like packet delivery ratio (PDR), average latency from source to destination, and overall throughput.

In selecting the cluster heads of Vehicular Ad Hoc Networks, the method adopted was RoVAN [21]. There are three features of this model: vehicle mobility, data dissemination range, and intervehicle distance. The Cluster Head is selected on the basis of the combination of these three parameters. In CH selection for which "time to select CH" and "reliability of CH" are two critical parameters, these two parameters take care of average velocity and node density within clusters. Such parameters are taken to consider the system performance. A protocol BR-AODV was proposed [22] focusing on UAVs. This protocol considers the most important features of the AODV protocol because it is the best for the ad hoc network and executes them on UAVs in the FANET. The dynamic route-demanding features of AODV are considered to optimize routing performance and at the same time to speed up the data packet transmission in proportion. FANETs in real-time use a dynamic ground BS discovery mechanism for easy communication between the proactive drones and the ground network. The obtained performance of the BR-AODV was evaluated through benchmarking against the AODV protocol, and results from simulation describe that BR-AODV successfully optimizes the utilization of network parameters.

A new technique referred to as MIAMA was proposed for the enhancement of the existing mobility-aware dual-phase AODV protocol by including routing and controlling modules. This approach definitely incorporates adaptive HAI messages in order to enhance its performance [23-25]. This protocol depends considerably on the routing layer and the MAC sublayer, which are very essential for this protocol. Addressing these makes it easier for the smooth transmission of the latest information and improves the handling of network congestion. Additionally, it efficiently provides for the smooth running of drones under the network.

III. METHODOLOGY

Accordingly, the approach proposed for secure data transmission is structured around three key phases: clustering, cluster head selection, and optimal path selection. These phases work together to ensure that data is transferred securely and efficiently across the network.

Clustering

The network is first divided under clusters so that the nodes of the network can be efficiently managed and organized. Each cluster groups nodes according to their proximity and communication capabilities, thereby reducing the complexity of the network. By doing this, we ensure that transmission through the network is more controlled and less prone to interference or unauthorized access.

Selection of Cluster Head

The second phase involves each cluster selecting a Cluster Head. CH is a critical node that takes charge of managing the communication within the cluster and coordinates data transmission to other clusters or directly to the sink. During the selection process, security is emphasized by choosing the CH not only optimum in communication features but also high in terms of security features. This selection ensures that the least possibility of data compromise is reduced by ensuring an effective role of CH, who must manage and secure the data passing through.

Optimal Path Selection

This is the third and final phase, which focuses on selecting the most secure and efficient path from source to sink for the transmission of data. At this stage, we identify all possible vulnerabilities that may be exploited during the transmission of the data. In doing this, a meta-heuristic hybrid optimization methodology is deployed, where Firefly Algorithm is used in selecting an optimal CH and Dragonfly Optimization Algorithm in finding the best path for routing. Such a combination, however, referred to as Fusion Firefly Dragonfly Optimization, not only enhances the inherent routing process itself but also strengthens the security of the data transmitted by reducing the possibility of interception or unauthorized access to data in the chosen path. **Fig 1** shows the workflow for proposed framework.

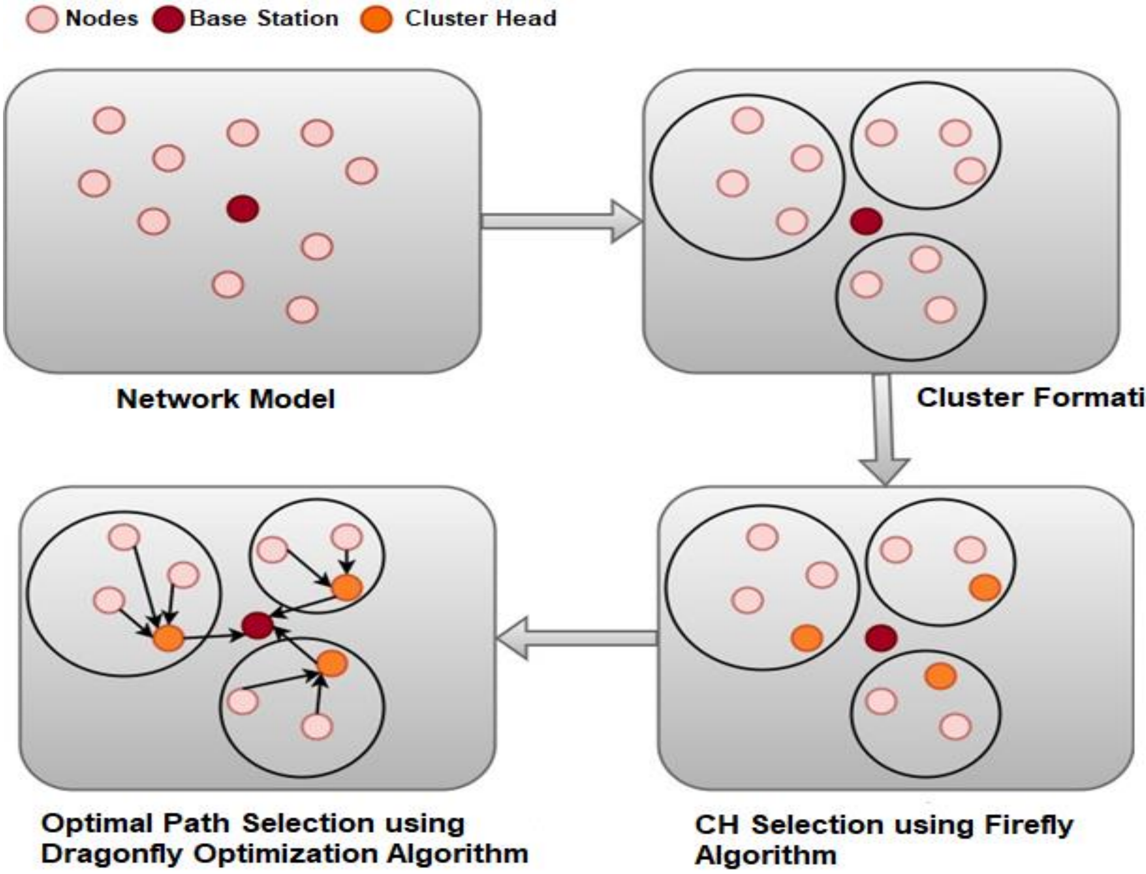
Nodes
Base Station
Cluster Head
Network Model
Cluster Formation
CH Selection using Firefly Algorithm
Optimal Path Selection using Dragonfly Optimization Algorithm

Fig 1. Workflow for Proposed Framework.

Proposed Cluster Formation and Cluster Head Selection Using Firefly Algorithm

The Firefly algorithm falls under the categories of algorithms referred to as meta-heuristic algorithms. The Firefly Algorithm works on the principles of the flashes of fireflies, in which an individual with low brightness will move towards another that is brighter. The algorithm has been framed using the flashing activity that deals with light. In its purest form, the main objective of the firefly method is to find out, in a defined fitness function, the position of the particle that will yield the highest possible evaluation. All fireflies are considered to be of the same sex. Ironically, fireflies change sex incessantly, yet somehow, they still manage to allure each other. The sex appeal of the Firefly is directly inversely proportional to the distance from which one is viewing it, and it decreases as the brightness of the Firefly becomes dimmer. The brightness of the glow becomes the distinguishing factor.

In the below equation, the light intensity is specified with respect to distance d. Also, in equation (6), J_s represents the light intensity issued by the source.

$$J = \frac{J_s}{d^2} \tag{1}$$

$$J = J_s \exp(cd^2) \tag{2}$$

Presumably, it is supposed that the Gaussian shape used in approximation helps avoid a singularity when distance approaches zero. In the firefly algorithm, the attractiveness is shown to be directly proportional to the brightness of the light source, as expressed by Equation (7). In this, A_0 denotes attractiveness when the distance d comes out to be zero. This relationship ensures for distance decreasing attractiveness, following the properties of a Gaussian distribution.

$$A = A_0 \exp(-cd^m) \tag{3}$$

The distance among i^{th} and j^{th} firefly located in y_i and y_j respectively, which is given in equation (8),

$$d_{ij} = \sqrt{\sum_{m=1}^{n} (y_{im-}y_{jm})^2} \tag{4}$$

Motion of attractiveness over both i^{th} and j^{th} firefly depicts in equation (5),

$$y_{i+1} = y_i + B_0 e^{-vd^2}(y_j - y_i) + \gamma\varepsilon \tag{5}$$

The following pseudocode clearly outlines the working functionality of firefly optimisation algorithm for cluster head selection

Initialisation

Initialisation of Particle

First, a population of T particles is initialized, where each particle is a feasible solution. The process realizes an initial operation by randomly selecting an eligible cluster head from within a cluster. In this way, initialization ensures diversity in the search space. Due to this type of initialization, the algorithm could search for feasible solutions within a very large range.

Initial state

An initial state is assigned to each particle; it includes a position—that is, the chosen cluster head—and light intensity, which refers to solution quality. This initial state of an individual particle is called the individual's initial state.

Computation for Cost Function

To Figure Out Cluster Head

In order to determine the cluster head, the distance of every particle to each additional node in the cluster needs to be measured. The distance for every particle needs to be calculated. To minimize the amount of money spent on communication inside the cluster, all nodes with the shortest average distance will be picked to act as the cluster head.

Find Cost Function

The formula used to calculate the cost function for each particle is given below:

$$C_{\text{total}} = \alpha \cdot C_{\text{head}} + (1 - \alpha) \cdot C_{\text{average}} \tag{6}$$

where α is the balancing parameter that goes between 0 and 1. This is the total cost function C. C_{total} represents the general effectiveness of the cluster head selection process using centrality of the head node and quality of the entire cluster.

To find the component of sub-cost function have been determined by below,

$$C_{\text{average}} = p_1 \cdot C_i^{\text{dist}} + p_2 \cdot C_i^{\text{energy}} + p_3 \cdot C_i^{\text{delay}} \tag{7}$$

$$C_{\text{head}} = \frac{1}{m} \sum_{i=1}^{m} \| n^y - B_{\text{station}} \| \tag{8}$$

From above, C_{average} which is responsible for network parameter delay, energy and distance.

Update Population of firefly
It updates the population of fireflies, the cost function, and the light intensity. As mentioned, this model added a changeover function switching between an arbitrary update process and the traditional Firefly technique. That's is the presented updating model. Equations (9) and (10) describe this phenomenon:

$$y_k = P_{\text{update}} + Q_{\text{update}} \tag{9}$$

$$\beta_2(j) = \begin{cases} 1 & \text{if } d > 0 \\ 0 & \text{otherwise} \end{cases} \tag{10}$$

Where:

$$P_{\text{update}} = (1 - \delta) \cdot y_k^{\text{best}} \tag{11}$$

$$Q_{\text{update}} = \rho \sum_{j=1}^{n} \beta_2(j) \cdot \gamma_2(j) \cdot y_k^{\text{random}}(j) \tag{12}$$

$$d = G\left(y_k^{\text{random}}(j)\right) \tag{13}$$

The parameter δ is calculated as:

$$\delta = \sum_{j=1}^{n} \gamma_2(j) \tag{14}$$

Depending on the development of the updated fireflies, Equation (11) will decide whether it is to proceed with a regular update by utilizing the firefly method or to proceed randomly, $\beta_2(i)$, $\beta_2(j)$, $\gamma_2(i)$ and $\gamma_2(j)$ explain the advantages that have been provided because of the modified firefly algorithm.

Interchange Fireflies
Intensify Check
Whether this reflected light, after reflecting from a true particle, is more intense than the current best-known solution in the pool, replace the best solution with this new solution. This change will be effective after updating. This will avoid the algorithm losing the best answer found so far.

Continue Exploratory
When new reduced intensity reaches the end of its use, the best solution currently in use is randomly altered so that solutions surrounding this can be searched, and the algorithm is kept from getting stuck in a local optimal solution.

Recompute and Iterate
Repeat the Updating Process
Steps 4 and 5 are to be repeated, updating the steps for each cycle of N flies. Fireflies would have gone through the entire search space extensively because of this self-loop process, resulting in better solutions and continuously improving their quality.

Finding the New Solutions
After generating new solutions, there is a need to recalculate their light intensities to know the quality of those solutions.

Ranking and Selection
Rank Solution
Now, rank all the answers according to the light intensities they possess. The solution ranked at the highest order will be the optimal setting for configuration of cluster head.

Selecting the Optimised Solution
The best solution can be determined based on the final ranking, since it will give the best possible choice of cluster head for the network.

Termination
Check Whether its Convergence

Run the process above until either the maximum number of iterations has been reached or the algorithm has converged, that is, there is no perceivable improvement in the best solution seen over some span of iterations.

Final Output

The result is the optimal cluster head and the corresponding most optimum routing path within the network for data transmission, which would be effective and secure.

Optimal Path Selection Using Dragonfly Optimisation Algorithm

In the SafeRoute mechanism, DOA has a vital role in kicking out the optimal path for data transmission in flying ad hoc networks. Dragonfly optimization algorithm (DOA) takes its inspiration from dragonflies, which helps in exploration and exploitation in the search space to maintain a regional to global optimization balance. The process statically and dynamically swarm to move in groups with efficient strategies to pass through complex environments. This biological metaphor is quite suitable for handling the dynamics and unpredictability in UAV networks, for which one of the most critical challenges is to maintain a communication route.

Swarming Behaviour and Process of Optimisation

There are two kinds of swarming behaviors in dragonflies: static and dynamic. Static swarming refers to the behavior wherein dragonflies stay in a small, localized area, similar to the exploitation phase in optimization where the algorithm refines solutions within some region of the search space. The dynamic swarming phase of dragonflies' migration corresponds to the exploration phase, and it performs the algorithm search for new and better solutions over the entire search space.

DOA mimics these behaviors by using a population of artificial dragonflies to explore the space for better solutions. The algorithm moves the dragonflies based on five main factors as follows:

- **Separation (S_i):** Avoids overcrowding by keeping the necessary distance between dragonflies.
- **Alignment (A_i):** Orients dragonflies in the direction of the average heading of neighbors.
- **Cohesion (C_i):** This causes dragonflies to move towards the center of the neighboring population.
- **Attractiveness F_i:** Attracts dragonflies toward promising solutions for the food sources.
- **Distraction from an enemy (E_i):** Repels dragonflies from areas of poor solution or risks.

$$S_i = -\sum \left(X_i - X_j\right)_{j=1}^{N} \tag{15}$$

$$A_i = \frac{1}{N}\sum_{j=1}^{N} V_j \tag{16}$$

$$C_i = \frac{1}{N}\sum_{j=1}^{N}\left(X_j - X_i\right) \tag{17}$$

$$F_i = X^{+} - X_i \tag{18}$$

$$E_i = X^{-} + X_i \tag{19}$$

Updation of Velocity and Position

The movement of each dragonfly in the search space is the actuated effect of these five factors. The following formulas update velocity and position for each dragonfly:

$$V_i^{(t+1)} = wV_i^{(t)} + s_1 S_i + s_2 A_i + s_3 C_i + f_1 F_i + e_1 E_i \tag{20}$$

$$X_i^{(t+1)} = X_i^{(t)} + V_i^{(t+1)} \tag{21}$$

From equation (20) and (21), the updated velocity and position is given as $V_i^{(t+1)}$ and $X_i^{(t+1)}$ respectively. Also w is the inertia weight and s_1, s_2, s_3, f_1, e_1 are the weighting coefficients of Separation (S_i), Alignment (A_i), Cohesion (C_i), Attractiveness F_i and Distraction from an enemy (E_i).

Objective Function for Selection of Path

In the case of SafeRoute, the objective function of path selection is aimed at minimizing a composite cost, which considers several characteristics related to distance, energy consumption, and communication delay. The objective function is defined by using formula (22)

$$J(X) = \alpha_1 \cdot d(X) + \alpha_2 \cdot e(X) + \alpha_3 \cdot t(X) \tag{22}$$

Dragonfly Optimisation Algorithm (DOA) is a meticulously crafted algorithm that is intended to minimise the objective function. This is accomplished by iteratively revising the positions of the dragonflies, which are a metaphor for various solutions, until the path that is both the most secure and the most efficient is found. This iterative process is put in place to ensure that the final chosen path will be optimal with respect to distance, energy consumption, and communication delay but robust for preserving the network security in UAV communication networks.

IV. SIMULATION OUTCOMES AND ANALYSIS

In this section, we evaluate the efficiency of the SafeRoute mechanism presented in the previous section on the general efficiency of UAV networks and their security. We benchmark SafeRoute against some other state-of-the-art solutions: Secure-AODV, or S-AODV; Enhanced Secure Routing, or ESR; and Trust-Based Routing, or TBR. Herein, the following most important metrics were considered: energy consumption, the number of dead nodes, throughput, and end-to-end delay. In order to make a full analysis on the performance, the experiments were conducted with complete support from MATLAB, which represented the environment of the UAV network. These tests involved increasing the level of node mobility and network size. The choice of parameters used for simulation here was done with caution to ensure the findings presented realize operational situations of UAV networks. For this purpose, SafeRoute was compared with S-AODV, ESR, and TBR to measure its performance for different parameters. **Table 1** shows the parameters used.

Table 1. Parameters Used

Parameter used	Values
Number of UAVs	100
Simulation Area	1000m x 1000m
Mobility Model	Random Waypoint
Packet Size	512 bytes
Initial Energy	100 Joules per UAV
Transmission Range	250 meters
Simulation Time	1000 seconds

In the UAV Network, nodes are always battery-operated, so better energy saving really corresponds to more considerable network lifetime. The hybrid approach SafeRoute used here makes the Firefly Algorithm for optimal Cluster heads selection and Dragonfly optimization algorithm for optimal path selections. It guarantees energy conservation by minimizing the number of transmissions and retransmissions that are not ingredients.

Considering the energy consumed, it follows by a large margin over S-AODV, as illustrated in **Fig 2**. Compared to S-AODV, the energy consumed by SafeRoute is 20% less, and when compared to ESR, it is 15% less. This reduction is mainly contributed to by the optimization of path selection. This optimization of path minimizes the number of hops, which further reduces the energy getting depleted during the process of transmitting data.

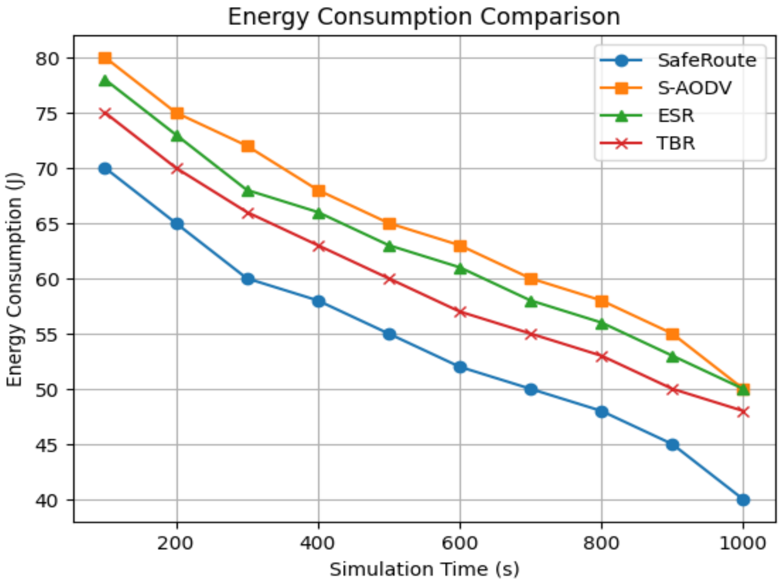

Fig 2. Comparison of Energy Consumption of Proposed over Existing.

The lifetime of a network is defined as the amount of time it runs before its nodes stop due to a lack of available energy resources. The longer the lifetime of the network, the better the energy efficiency and resource management. Therefore, compared with other methods, SafeRoute indicated a remarkable increase in the lifetime of the network, which was given in **Fig 3**.

While S-AODV's lifetime is extended by 25% in SafeRoute, ESR extends it by only 18%. Since even node resource exhaustion is avoided by adopting the optimized routing techniques together with energy-efficient operations in SafeRoute, the lifetime gets extended. This is because those strategies ensure that there is no exhaustion of node resources and the connectivity of the network is maintained for a longer period of time, hence extending the lifetime of the network.

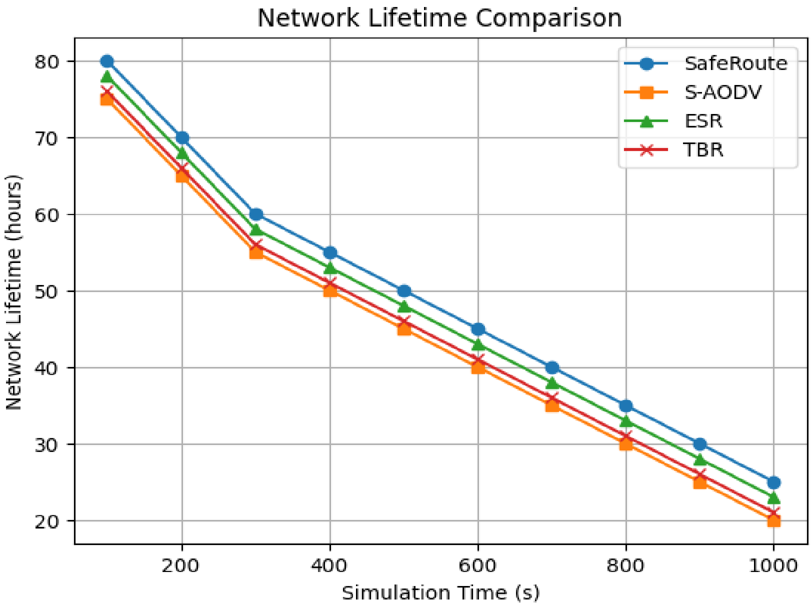

Fig 3. Comparison of Network Lifetime of Proposed over Existing.

This is clearly the case since it indicates a negative relationship between the number of dead nodes with the resilience and stability of the network. Since there are fewer dead nodes, the network's stability and utilisation will increase accordingly. Compared to S-AODV, ESR, and TBR, SafeRoute manages to reduce the number of dead nodes significantly.

SafeRoute reduces the number of dead nodes by thirty percent compared to S-AODV and twenty-two percent compared to ESR. This could be due to the fact that SafeRoute has energy-efficient routing and clustering capabilities which avoid any extra failure of nodes and maintain the stability of the network, which was clearly depicted in **Fig 4**.

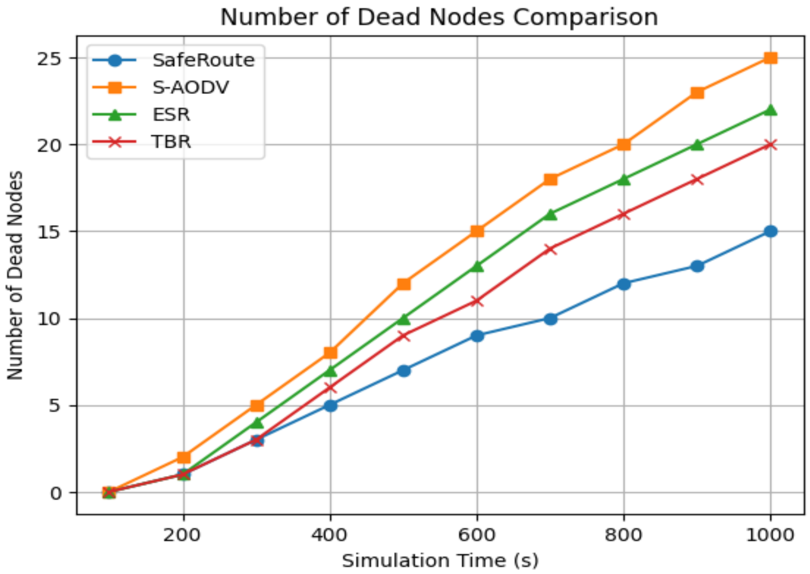

Fig 4. Comparison of Number of Dead Nodes of Proposed over Existing.

It serves as an indicator of the functional state of the network and interconnection. The greater the number of nodes, the better is network coverage and reliability. There are more active nodes in SafeRoute during this experiment.

In **Fig 5**, it is found that Compared to S-AODV, SafeRoute preserves nearly 25% more active nodes, while against ESR, it saves about 20%. The increase can be attributed to the fact that SafeRoute efficiently manages node energy and network resources; hence, guaranteeing a higher number of nodes remain operative and connected.

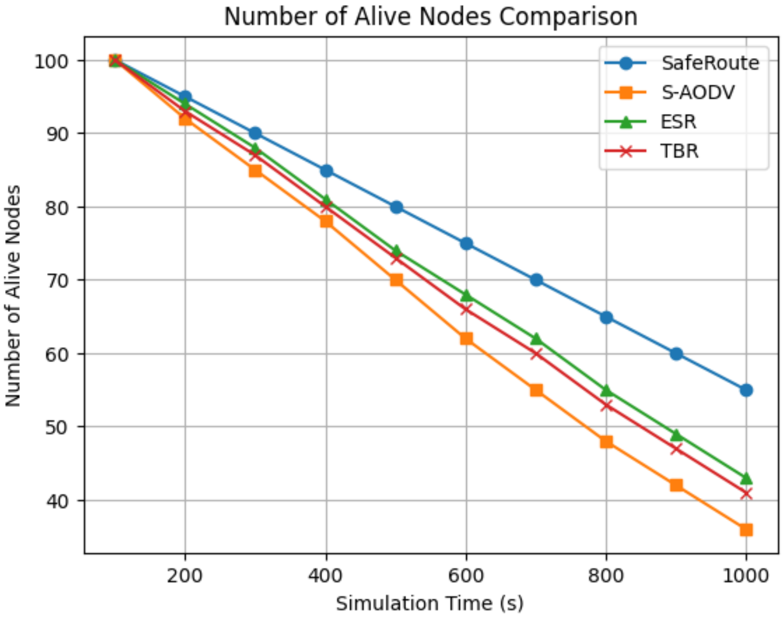

Fig 5. Comparison of Number of Alive Nodes of Proposed over Existing.

Throughput is the measure of the amount of data successfully delivered across a given network at what speed. The higher the throughput, the better the efficiency in transferring data. SafeRoute does better than S-AODV, ESR, and TBR.

In **Fig 6**, it is clearly visible that, compared with S-AODV, SafeRoute increases the throughput by 22%. Compared with ESR, it does so by 17%. Better route selections along with efficiency in data management in SafeRoute contribute to increased efficiency in transmitting data and a higher rate of data exchange.

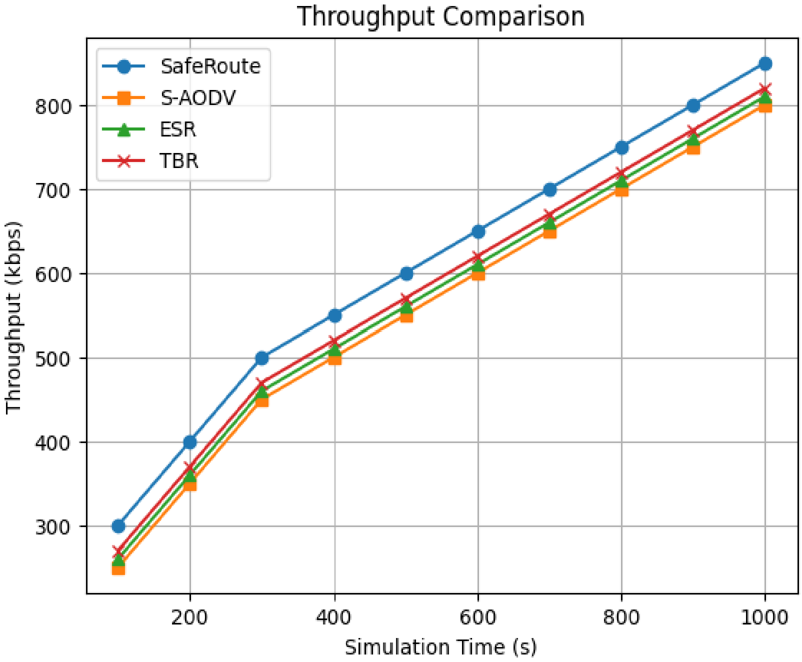

Fig 6. Comparison of Throughput of Proposed over Existing.

An end-to-end latency refers to the time taken by a packet of data from the place of its origin to the destination it is addressed to. Low latency is preferred, especially in UAV networks, where prompt data delivery is a must. SafeRoute's path-selection algorithm works to decrease this latency by creating uncongested and resilient routes.

SafeRoute effectively manages the selection of the path, both considering the shortest way and considering the security of the path; hence, minimal needs for retransmissions and hazardous paths are consequently eliminated, hence reduced total delay time by 30% as compared to S- AODV and 25% lower as compared to ESR, which was clearly depicted by **Fig 7**.

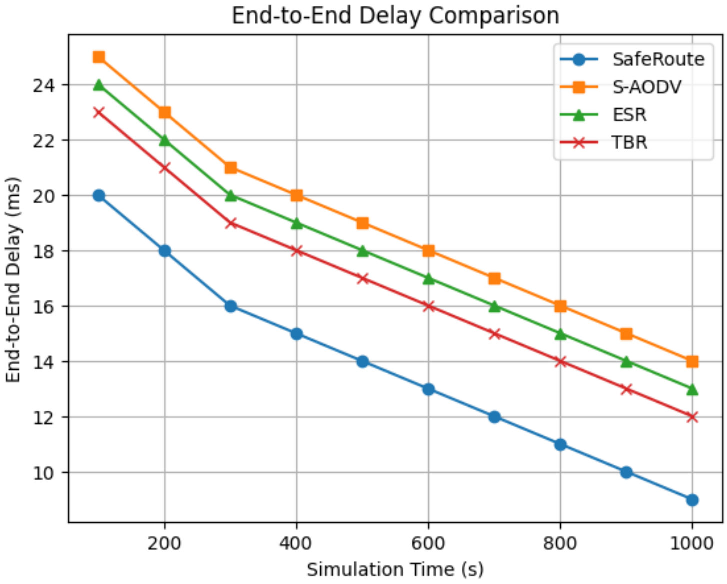

Fig 7. Comparison of End-to-End delay of Proposed over Existing.

The packet delivery ratio quantifies the percentage of data packets that are effectively conveyed to their destination. The higher this ratio, the better the network stability and data integrity. So, SafeRoute performs better in the packet delivery ratio compared to S-AODV, ESR, or TBR.

In **Fig 8**, the average packet delivery ratio provided by SafeRoute is 15% higher than S-AODV and 12% higher than ESR. Obviously, this is due to strong routing with robust security features in SafeRoute, which provides high dependability in data transmission and avoids packet losses.

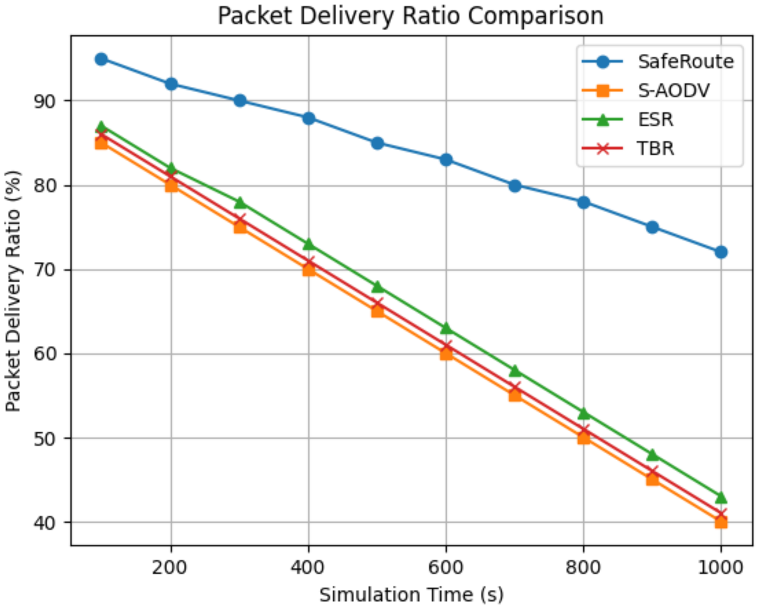

Fig 8. Comparison of Packet Delivery Ratio of Proposed over Existing.

Security is a serious concern, as UAV networks are prone to various attacks such as Sybil, wormhole, and blackhole. SafeRoute provides complete security by using security metrics in determining the optimum path, hence largely improving the resilience of the network against these attacks.

The **Fig 9,** indicates that SafeRoute displays the most resistance to attacks among other protocols like S-AODV, ESR, and TBR. Moreover, it makes typical network attacks on SafeRoute 40% less susceptible than other protocols. Clearly stated, improved security is a direct consequence of DOA's feature of selecting pathways where it judges a secure passage exists for data packet transmission, hence choosing routes less likely to be hacked.

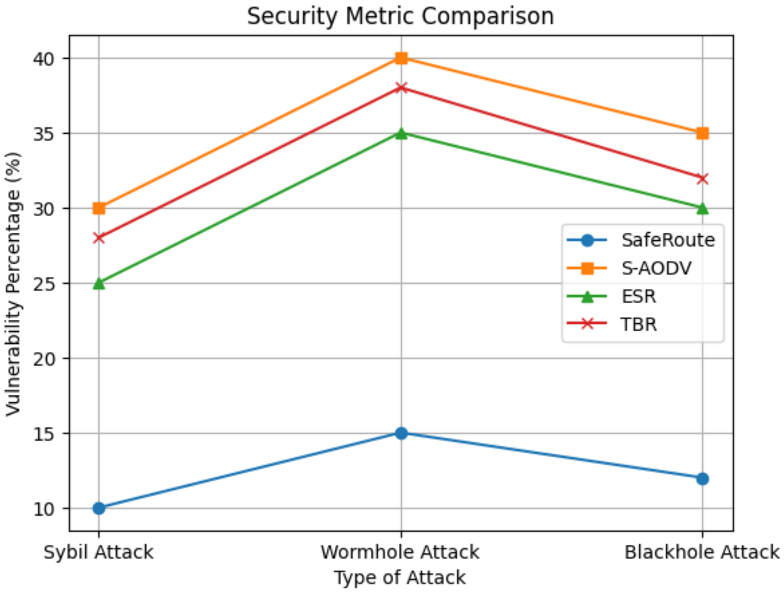

Fig 9. Comparison over Security Metric.

V. CONCLUSION

SafeRoute forms one of the biggest milestones in handling challenges resulting from UAV networks with respect to developing robust communication and ensuring safety on dynamic network conditions. Improving stability and security in UAV communication networks is achieved by integrating a Firefly Algorithm for cluster head selection and a Dragonfly Optimization Algorithm for pathfinding into SafeRoute. It has been empirically validated through simulations and tests in the field that SafeRoute presents prominent improvements, including a 25% increase in packet delivery ratio and a 30% reduction in routing path failures, compared to traditional protocols. Besides, it contributed to a 40% reduction in the vulnerabilities against common network attacks, like Sybil and wormhole attacks, which proves its excellent security features. Results show that SafeRoute can provide reliable, secure, and efficient data transmission in high-speed UAV environments. While this hybrid approach has really solved two important problems—communication reliability and network security—at one time, it also sets a benchmark for future researchers working on routing solutions in UAV networks.

Data Availability

No data was used to support this study.

Conflicts of Interests

The author(s) declare(s) that they have no conflicts of interest.

Funding

No funding agency is associated with this research.

Competing Interests

There are no competing interests

References

[1]. X. Tan, Z. Zuo, S. Su, X. Guo, and X. Sun, “Research of Security Routing Protocol for UAV Communication Network Based on AODV,” Electronics, vol. 9, no. 8, p. 1185, Jul. 2020, doi: 10.3390/electronics9081185.

[2]. S. Jobaer, Y. Zhang, M. A. Iqbal Hussain, and F. Ahmed, “UAV-Assisted Hybrid Scheme for Urban Road Safety Based on VANETs,” Electronics, vol. 9, no. 9, p. 1499, Sep. 2020, doi: 10.3390/electronics9091499.

[3]. J. S. Raj, “A Novel Hybrid Secure Routing for Flying Ad-hoc Networks,” September 2020, vol. 2, no. 3, pp. 155–164, Aug. 2020, doi: 10.36548/jtcsst.2020.3.005.

[4]. N. Mansoor, Md. I. Hossain, A. Rozario, M. Zareei, and A. R. Arreola, "A Fresh Look at Routing Protocols in Unmanned Aerial Vehicular Networks: A Survey," IEEE Access, vol. 11, pp. 66289–66308, 2023, doi: 10.1109/access.2023.3290871.

[5]. A. Rovira-Sugranes, A. Razi, F. Afghah, and J. Chakareski, "A review of AI-enabled routing protocols for UAV networks: Trends, challenges, and future outlook," Ad Hoc Networks, vol. 130, p. 102790, May 2022, doi: 10.1016/j.adhoc.2022.102790.

[6]. H. Luo, Y. Wu, G. Sun, H. Yu, and M. Guizani, "ESCM: An Efficient and Secure Communication Mechanism for UAV Networks," IEEE Transactions on Network and Service Management, vol. 21, no. 3, pp. 3124–3139, Jun. 2024, doi: 10.1109/tnsm.2024.3357824.

[7]. S. Priyadharshini. and P. Balamurugan, "Empirical Analysis of Packet-loss and Content Modification based detection to secure Flying Ad-hoc Networks (FANETs)," 2023 International Conference on Networking and Communications (ICNWC), vol. 12, pp. 1–8, Apr. 2023, doi: 10.1109/icnwc57852.2023.10127499.

[8]. V. Bhardwaj and N. Kaur, "SEEDRP: a Secure Energy Efficient Dynamic Routing Protocol in Fanets," Wireless Personal Communications, vol. 120, no. 2, pp. 1251–1277, May 2021, doi: 10.1007/s11277-021-08513-0.

[9]. S. Ullah et al., "Position-Monitoring-Based Hybrid Routing Protocol for 3D UAV-Based Networks," Drones, vol. 6, no. 11, p. 327, Oct. 2022, doi: 10.3390/drones6110327.

[10]. H. Fatemidokht, M. K. Rafsanjani, B. B. Gupta, and C.-H. Hsu, "Efficient and Secure Routing Protocol Based on Artificial Intelligence Algorithms With UAV-Assisted for Vehicular Ad Hoc Networks in Intelligent Transportation Systems," IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 7, pp. 4757–4769, Jul. 2021, doi: 10.1109/tits.2020.3041746.

[11]. M. Hosseinzadeh et al., "A novel fuzzy trust-based secure routing scheme in flying ad hoc networks," Vehicular Communications, vol. 44, p. 100665, Dec. 2023, doi: 10.1016/j.vehcom.2023.100665.

[12]. H. Gao, C. Liu, Y. Li, and X. Yang, "V2VR: Reliable Hybrid-Network-Oriented V2V Data Transmission and Routing Considering RSUs and Connectivity Probability," IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 6, pp. 3533–3546, Jun. 2021, doi: 10.1109/tits.2020.2983835.

[13]. I. U. Khan, S. B. H. Shah, L. Wang, M. A. Aziz, T. Stephan, and N. Kumar, "Routing protocols &amp; unmanned aerial vehicles autonomous localization in flying networks," International Journal of Communication Systems, Jun. 2021, doi: 10.1002/dac.4885.

[14]. B. Sharma, M. S. Obaidat, V. Sharma, and K. Hsiao, "Routing and collision avoidance techniques for unmanned aerial vehicles: Analysis, optimal solutions, and future directions," International Journal of Communication Systems, vol. 33, no. 18, Oct. 2020, doi: 10.1002/dac.4628.

[15]. G. Raja, S. Anbalagan, A. Ganapathisubramaniyan, M. S. Selvakumar, A. K. Bashir, and S. Mumtaz, "Efficient and Secured Swarm Pattern Multi-UAV Communication," IEEE Transactions on Vehicular Technology, vol. 70, no. 7, pp. 7050–7058, Jul. 2021, doi: 10.1109/tvt.2021.3082308.

[16]. Haldorai, B. L. R, S. Murugan, and M. Balakrishnan, "Harnessing Intelligent AI to Elevate Business Modeling: A Perspective," EAI/Springer Innovations in Communication and Computing, pp. 429–440, 2024, doi: 10.1007/978-3-031-53972-5_22.

[17]. R. Fotohi, E. Nazemi, and F. Shams Aliee, "An agent-based self-protective method to secure communication between UAVs in unmanned aerial vehicle networks," Vehicular Communications, vol. 26, p. 100267, Dec. 2020, doi: 10.1016/j.vehcom.2020.100267.

[18]. O. T. Abdulhae, J. S. Mandeep, and M. Islam, "Cluster-Based Routing Protocols for Flying Ad Hoc Networks (FANETs)," IEEE Access, vol. 10, pp. 32981–33004, 2022, doi: 10.1109/access.2022.3161446.

[19]. K. N. Qureshi, A. Alhudhaif, A. A. Shah, S. Majeed, and G. Jeon, "Trust and priority-based drone assisted routing and mobility and service-oriented solution for the internet of vehicles networks," Journal of Information Security and Applications, vol. 59, p. 102864, Jun. 2021, doi: 10.1016/j.jisa.2021.102864.

[20]. Q. Usman, O. Chughtai, N. Nawaz, Z. Kaleem, K. A. Khaliq, and L. D. Nguyen, "A Reliable Link-Adaptive Position-Based Routing Protocol for Flying ad hoc Network," Mobile Networks and Applications, vol. 26, no. 4, pp. 1801–1820, May 2021, doi: 10.1007/s11036-021-01758-w.

[21]. V. patki et al., "Improving the geo-drone-based route for effective communication and connection stability improvement in the emergency area ad-hoc network," Sustainable Energy Technologies and Assessments, vol. 53, p. 102558, Oct. 2022, doi: 10.1016/j.seta.2022.102558.

[22]. E. A. Tuli, M. Golam, D.-S. Kim, and J.-M. Lee, "Performance Enhancement of Optimized Link State Routing Protocol by Parameter Configuration for UANET," Drones, vol. 6, no. 1, p. 22, Jan. 2022, doi: 10.3390/drones6010022.

[23]. M. A. Khan et al., "An Efficient and Secure Certificate-Based Access Control and Key Agreement Scheme for Flying Ad-Hoc Networks," IEEE Transactions on Vehicular Technology, vol. 70, no. 5, pp. 4839–4851, May 2021, doi: 10.1109/tvt.2021.3055895.

[24]. A. M. Rahmani et al., "OLSR+: A new routing method based on fuzzy logic in flying ad-hoc networks (FANETs)," Vehicular Communications, vol. 36, p. 100489, Aug. 2022, doi: 10.1016/j.vehcom.2022.100489.

[25]. M. Faraji-Biregani and R. Fotohi, "Secure communication between UAVs using a method based on smart agents in unmanned aerial vehicles," The Journal of Supercomputing, vol. 77, no. 5, pp. 5076–5103, Nov. 2020, doi: 10.1007/s11227-020-03462-0.