Journal of Fuzzy Extension and Applications

www.journal-fea.com

J. Fuzzy. Ext. Appl. Vol. 5, No. 1 (2024) 48–59.

Paper Type: Research Paper

Trusted Fuzzy Routing Scheme in Flying Ad-hoc Network

Sahabul Alam[1], Joydeep Kundu[1], Shivnath Ghosh[2], Arindam Dey[3,*]

[1] Department of Computer Science and Engineering, Brainware University, Barasat, Kolkata-700125, West Bengal, India; sahabul2009@gmail.com; joydeep.1988kundu@gmail.com.

[2] Brainware University, Barasat, Kolkata-700125, West Bengal, India; shivghosh.cs@gmail.com.

[3] School of Computer Science and Engineering, VIT-AP University, Amaravati, Andhra Pradesh, India; arindam84nit@gmail.com.

Citation:

Received: 16 September 2023 *Revised: 18 November 2023* *Accepted: 12 Januray 2024*	Alam, S., Kundu, J., Ghosh, Sh., & Dey, A. (2024). Trusted fuzzy routing scheme in flying ad-hoc network. *Journal of fuzzy extension and applications*, *5*(1), 48-59.

Abstract

Unmanned Aerial Vehicles (UAVs) bring both potential and difficulties for emergency applications, including packet loss and changes in network topology. UAVs are also quickly taking up a sizable portion of the airspace, allowing Flying Ad-hoc NETworks (FANETs) to conduct effective ad hoc missions. Therefore, building routing protocols for FANETs is difficult due to flight restrictions and changing topology. To solve these problems, a bio-inspired route selection technique is proposed for FANET. A combined trustworthy and bioinspired-based transmission strategy is developed as a result of the growing need for dynamic and adaptable communications in FANETs. The fitness theory is used to assess direct trust and evaluate credibility and activity to estimate indirect trust. In particular, assessing UAV behavior is still a crucial problem in this field. It recommends fuzzy logic, one of the most widely utilized techniques for trusted route computing, for this purpose. Fuzzy logic can manage complicated settings by classifying nodes based on various criteria. This method combines geocaching and unicasting, anticipating the location of intermediate UAVs using 3-D estimates. This method guarantees resilience, dependability, and an extended path lifetime, improving FANET performance noticeably. Two primary features of FANETs that shorten the route lifetime must be accommodated in routing. First, the collaborative nature necessitates communication and coordination between the flying nodes, which uses a lot of energy. Second, the flying nodes' highly dynamic mobility pattern in 3D space may cause link disconnection because of their potential dispersion. Using ant colony optimization, it employs trusted leader drone selection within the cluster and safe routing among leaders. a fuzzy-based UAV behavior analytics is presented for trust management in FANETs. Compared to existing protocols, the simulated results demonstrate improvements in delay routing overhead in FANET.

Keywords: Security, Clustering, Trust management, Routing, Bio-inspired, Fuzzy.

1 | Introduction

In the upcoming years, the Flying Ad-hoc NETwork (FANET) [1]–[5], which consists of Unmanned Aerial Vehicles (UAVs) that fly without a pilot, is anticipated to have a major impact on human existence. FANETs provide actuation services while limiting human engagement and possibly life-threatening risks. They enable

Corresponding Author: sahabul2009@gmail.com

https://doi.org/10.22105/jfea.2024.436052.1370

complicated applications beyond the capabilities of standard MANETs or individual UAVs. FANETs are becoming more and more popular because of their durability, flexibility, affordability, and simplicity of construction. Precise geographic localization, search and rescue operations, intelligent transportation systems, target identification, disaster tracking, volcano monitoring, medical supply delivery, border patrol operations, and forest fire prevention are just a few of the potential applications for multi-UAV collaboration. Both academics and industry are developing FANETs for a range of uses, including mapping and surveying. This means that boosting transmission power to enable long-distance communication in FANETs will not be able to alleviate frequent disconnections. Therefore, it isn't easy to build long-term, dependable, and durable connections and routes in FANETs, even though doing so increases route lifespan and improves the quality of service. Still, there are a lot of technical obstacles to be solved, like quickly shifting network topologies, node velocity, energy limitations, UAV collaboration and communication, dependable connections, transmission ranges, density, and security issues.

However, due to its distinctive properties, such as long-distance communication, power consumption, and sensitive military and monitoring applications, FANETs have difficulties in networking and communication. Because of these issues, developing a routing protocol for FANETs is difficult. The communication architecture for UAV-to-UAV and UAV-to-Base Station control comprises UAVs, ground controllers, and smart antennas. UAVs are divided into groups according to size, weight, wing shape, and attitude [6]–[9].

1.1 | Motivation

The paper's motivation is to do a thorough assessment to pique research interest in routing algorithms in FANETs due to the lack of research on the subject and the neglect of key elements like three-dimensional movement and mobility. Several routing strategies are categorized, examined, and analyzed based on a taxonomy. To meet the demands of the moment, new solutions are still required for the problems relating to FANETs. QoS measurements, routing, and security [10]–[14]. To satisfy the demands of the situation, the major goal of this work is to increase confidence among communicating UAVs and choose the most dependable UAV that can store data and have enough energy to complete the task.

1.2 | Key Contribution to the Research Article

Due to these facts, the proposed scheme can create a reliable and trustworthy route based on three-dimensional estimates and provide a quick update mechanism for the flight route in FANETs. To protect data transmission, the contributions of this article have been summarised below:

- *To involve a cluster formation that maximizes UAV's energy efficiency.*
- *To locate and choose the most effective leader UAVs for routing purposes. Each leader employs bioinspired-based Ant Colony Optimization (ACO) techniques.*
- *To protect data confidentiality and integrity, it proposes an inter-cluster routing protocol through the most trusted and energy-consumed leaders that is secure and dependable to generate stable routes.*
- *To examine path planning based on the UAV's broadcast range, pheromone level-based path, path trust value, and key generation technique to produce a robust route.*
- *To protect the UAVs during FANET data transfer by keeping them safe along their paths.*
- *To dynamically reselect the drone leader when numerous drones in a clustered FANET communicate.*
- *To create a simple trust-based surveillance system in FANET to support data privacy.*

The remaining six sections of the article are as follows related works to FANETs-based routing are included in Section 2. The suggested bio-inspired route selection technique is presented in Section 3. The results of the simulation and implementation are described in Section 4. The Section 5 contains the conclusion and the scope of future research.

2 | Related Work

Many scholars from around the world have contributed significantly in the last ten years by using various clustering strategies to offer solutions [15]–[20]. Cluster leaders were employed in the FANET design to control transmission hierarchically. To maintain the QoS criteria throughout each cluster, it also made use of a centralized traffic differential routing algorithm and a collaborative controller. Depending on the transmission activities of each flow, different weights are applied to the flows. Thus, a transmission reliability prediction model is employed to assess the link's legitimacy and forwarding capacities. The UAV source node calculates probabilistic transfer values based on their geographic positions. The bulk of suggested solutions focus mostly on effective routing because path formation boosts transmission speed and is necessary for the FANET to function.

An efficient FANET routing protocol, SecRIP [13], was proposed to help prolong the network's routing lifetime. The algorithms (chaotic algae and dragonfly) were proposed initially. The former helps with cluster formation using the available drones, and the dragonfly helps choose an efficient leader from the rest of the cluster member drones. The above techniques are suitable for the secure and efficient routing of data packets with the support of each cluster's designated leader drone across the network. This identifies control for each cluster, facilitating data forwarding to the desired location. Furthermore, this model ensures that the gearbox consumes the minimum energy. This scheme is also able to reduce the use of drone energy. Therefore, it satisfied the overall quality of the network. The simulation results demonstrated that the suggested protocol could achieve greater network objectives than the current approaches compared to a variety of existing protocols. By doing this, you could help safeguard the data from network assaults.

A unique trust-based context-aware technique [10] discriminated between deliberate and inadvertent misbehavior in FANETs. Moreover, it employed the different computed criteria to choose the best packet forwarders. In this sense, it offered dependable inter-UAV communications. Tested in multiple real-world scenarios, including rescue operations where uncertified personal UAVs can help by instantly notifying about natural disasters like earthquakes, volcanoes, blocked roads, or even rural auto accidents, this trust-based, context-dependent inter-UAV routing communication system. The simulation results show that this technique surpasses the previous solution, i.e., UNION, in terms of guaranteeing low packet loss ratios, low end-to-end latency, and high detection ratios with fewer false positives.

The FANET features discussed so far highlight how challenging it is to design a routing system that meets every need, including power supply, security, and fast topology changes. As a result, the FANET routing protocol categories vary according to the network's condition. Nature-based algorithms are search strategies that mimic nature's numerous random judgments. Bio-Inspired Algorithms (BIA) effectively simplify difficult-to-understand sophisticated optimization approaches. BIA implements many algorithms in FANET, increasing their efficiency over other existing algorithms.

The UNION model does not account for energy usage. It is unable to develop an optimal strategy for dynamically selecting a leader drone at various geographic obstacles, one that will lead the other drones regardless of transmission range, both high and low. SecRIP cannot determine the drones' dependability or route when exchanging data. Pioneering the broadcast storm problem at the onset of interest propagation is inappropriate. The idea of using technology to detect and protect private areas from unapproved drones has not yet been presented.

Energy use is not taken into consideration by the UNION model. It cannot create an ideal plan for dynamically choosing a leader drone at different geographic barriers, one that will guide the other drones regardless of the high or low transmission range. SecRIP cannot ascertain the route or the drones' reliability when data is being shared. Addressing the broadcast storm issue at the outset of interest propagation is inappropriate. Using technology to identify and keep unapproved drones out of private locations hasn't been proposed.

3|The Proposed Methodology

The three phases of the proposed technique are cluster formation, leader drone selection, and secure route discovery. The work is further categorized into various layers, i.e., classification of various UAV types (good, bad, and neutral) based on their trust score (direct, recommendation, and fitness score), formation of energy efficient clusters formation, and bioinspired optimized, secure route selection based on ACO technique. The Trust Management System, which evaluates each drone's trustworthiness using various trust criteria, is one of the interconnected components and layers that make up the architecture.

The cluster formation module establishes secure clusters, with cluster heads selected according to proximity and dependability. Cluster heads coordinate communication among their clusters and keep the cluster secure. Secure communication protocols are implemented to protect the integrity, confidentiality, and authenticity of data transferred between drones. Privacy preservation techniques can be utilized, such as data anonymization or encryption of sensitive information to stop unauthorized access to private data. The core of the system is the trust management system, which evaluates the trustworthiness of each drone in the network. The trust management system assigns each drone a trust value based on many trust indicators, such as past performance, reputation, and referrals from other drones. The fitness score of the nodes is then determined by considering a variety of network parameters, such as energy consumption, computational capacity, and the separation between drones (based on their latitude, longitude, and altitude).

The classification method distinguishing between malicious and honest UAVs in the network is reward- or punishment-based. The drones are arranged into clusters according to their proximity to one another and remaining energy. The drone's remaining energy and distance are used as selection parameters during the leader election phase. Below is a description of the cluster construction and leader election method. The primary goal of the suggested algorithm is to choose a data transmission technique that uses less energy using network leader drones to improve network security.

Several objectives can be supported Using ACO-based routing algorithms, such as energy conservation, bandwidth optimization, and reliability maximization. The pheromone-driven decision-making method enables UAVs to balance these objectives and select routes that comply with network goals and constraints. ACO's adaptability and flexibility make it a suitable routing method for FANETs. So, the optimal route discovery has been describe using the below algorithm. Assessing the dependability of the drones within FANET can be done using trust models. Historical behavior analysis, reputation systems, and collaborative monitoring can all be used to determine neighboring nodes' reliability. Mechanisms based on trust are used to detect and mitigate hazardous activities in real time. This may entail applying behavior analysis, signature-based detection, and anomaly detection to swiftly find and fix security vulnerabilities. Trust-based algorithms can adjust security measures based on network conditions and perceived threats.

The proposed method provides a trust-based secure routing method based on fuzzy logic. It first computes the trusted member drones and then observes their behavior. The leader drone has been chosen when the drones are fitted to compete within the network scenario. The leaders take responsibility for a secure communication system based on the optimization technique of fuzzy logic. The proposed method has been simulated with OMNET++ based on around 600 drones and compared with UNION and SecRIP protocol based on delay, packet delivery ratio, and latency.

Algorithm 1. Trust-based bio-inspired route discovery through selected leader drones.

```
   Input: Trust Matrix (T_(M_ij )), Distance Matrix (D_(M_ij )), Pheromone Matrix (P_ij),
   Number of Clusters, No. of Ants, No. of Iteration, Source Cluster, Destination Cluster
   Output: Optimal Route
1. No. of Clusters = n, No. of Ants = 10, No. of Iteration = 100
2. Initialize the Source and Destination Cluster
3. Initialize Node Distance (D_(ij(n*n))), Trust (T_(ij(n*n)))
4. Initialize Pheromone Matrix (P_(ij(n*n))) = 1.0
5. Define ConstructRoute() method:
   while ( CurrentCluster != Destination ) do
       NextCluster = FindNextCluster()// Find the next cluster
       CurrentCluster = NextCluster// Set the cluster as visited
   return Route
6. Define RouteLength( Route ) method:
   Length = 0.0     // Initialize the length as 0.0
   for i =0 to Route_size do
       Length += DistanceMatrix[i][i+1]
   return Length
7. Define updatePheromone( Route, RouteLength) method:
   for i = 0 to NumClusters, do
             // Evaporate Pheromones on all edges
   // Deposit pheromones on edges in the ant routes
       for i = 0 to Ants do
       for j = 0 to route_size do
       // Deposit pheromones on shorter routes
   end
8. Define FindNextCluster() method:
   for i = 0 to NumClusters do
       if ( Cluster Not Visited ) then
            Store in UnvisitedCluster list
   end
   Initialize TotalProbability = 0.0 and Probabilities[] array
   for i = 0 to UnvisitedClusters_size do
       // Pheromone Influence factor ( α ) = 1.0
        PheromoneFactor = $P_{[CurrentCluster][NextCluster]}{}^{\alpha}$
        TrustFactor = $T_{[CurrentCluster][NextCluster]}{}^{\beta}$
        Trust Influence factor ( β )= 2.0
        Probabilities[i] = PheromoneFactor * TrustFactor
        TotalProbability += Probabilities[i]
        end
        Initialize ProbabilityRate = 0.0
        for i = 0 to Probabilites_size do
        ProbabilityRate += probabilities[i]
        if ( RandomValue <= ProbabilityRate ) then
        return UnvisitedCluster
        end
        return UnvisitedCluster (Random)
     end
9. Now Calculate the Best Path suing FindBestPath() Method
   FindBestPath ( Iteration ) do
   BestPath = null
   BestPathLength = Max_Value
   for i = 0 : Iteration do
       for j = 0 : Ants do
       Route = ConstructRoute()
       RouteLength = RouteLength(Route)
       if ( RouteLength < BestPathLength ) then
            BestPathLength = RouteLength
       end
       updatePheromone( Route, Routelength);
     end
10. return BestPath
```

It is critical to design trust-based routing protocols considering the dynamic nature of drones in FANET. Route selection can be optimized by mobility-aware protocols, which adjust to changes in the network topology by considering the present positions and trajectories of nodes. Based on nodes' past data, predictive models can assist in projecting their future locations. This makes it possible to allocate resources and plan routes more intelligently, considering anticipated movement patterns. FANET nodes may encounter a range of communication situations as a result of variations in direction. Trust-based techniques for dynamic management can be used to optimize frequency allocation and adjust to evolving communication environments. Because FANET nodes frequently have limited resources, energy-efficient methods are essential. The network's total lifetime can be increased by optimizing data transmission and communication patterns based on the current energy levels and flying conditions.

Trust-based authentication techniques ensure that only selected drones and base stations can access the network. Data communication between drones and ground control stations is protected by it. Mechanisms for integrity verification and encryption assist in monitoring network traffic, spotting potentially harmful activity, and preventing illegal access, eavesdropping, and communication manipulation. Trust-based algorithms in the context of FANETs seek to decentrally build and preserve trust connections among nodes "drones". Because FANETs are distributed and dynamic networks, decentralized methods are essential. These few decentralized techniques are frequently applied to trust-based FANET algorithms. Trust models disperse the trust assessment process among several network nodes as opposed to depending on a single authority. Every node evaluates neighbor behavior and assigns trust scores based on interactions seen. Next, nodes exchange trust information to create a decentralized trust model as a whole. Nodes use locally observed behavior to choose which behaviors to trust. Every node keeps track of a local trust metric for its surrounding nodes, considering things like collaboration, consistency in communication, and protocol observance. Decisions are then made decentralized using local trust measures. Peer-to-Peer interactions can directly develop trust among peers. Nodes share trust information and use direct observations to assess one other's reliability.

4 | Implementation and Performance Result Discussion of the Proposed Scheme

The modeling environment creates a network of positive and negative nodes called FANET [21]–[30]. Nodes in the experiment are categorized as good drones, neutral nodes, and bad nodes. A drone should ideally have an abundance of resources, adhere to network protocols, and not engage in malicious activity. The neutral nodes often function at maximum efficiency, have fewer resource constraints, and rarely take harmful or self-serving actions. The malignant nodes within the FANET are designed to function independently and malevolently. After 40 seconds, the drones' trust score interval is recorded. The proposed scheme employs the fuzzy classification system to distinguish between the drones in the network.

The fuzzy model's several parts work together to determine the network's trust score. Both social and service quality criteria are used in the model. Reliability and performance are represented, respectively, by social parameters and service quality. The genius of this approach is that it has a backup cluster head in case the first one selected becomes sick or moves. Since a backup cluster head can easily take over for the primary one in the event of a relocation, the FANET can continue to operate with smooth communication.

The fuzzy membership function aims to incorporate past knowledge about the crisp value into the input space. Triangular types of membership fuzzy functions have been used within FANET to establish performance and social characteristics. Ten replications of each experiment were carried out to take experiment variability into account. The average outcomes of the experiment are shown in *Table 1*.

Table 1. Experiment value of parameters.

Name of the Parameters	Values
Simulation area size	(1700×1300×800) m3
No. of UAVs	600
Packet size	4700 bits
Placement of nodes	Random
Mobility model	Random Waypoint
Traffic	CBR
Range of Velocity of drone	25–70 mph
Simulation time duration	350s
Initial trust value	0.45

4.1 | Result and Discussions

Due to its dynamic nature, it is the perfect use case for FANETworks [31]–[39]. FANET have the main advantage of not requiring a centralized administrative framework. It has been compared against SecRIP [13] and UNION [10] to demonstrate the advantages of applying the method. The performance of the proposed scheme has been analyzed based on the existing routing protocols in FANET. The proposed scheme is contrasted with different types of FANET routing protocols. The comparison facilitates the performance analysis of the proposed scheme. An emulated model of the real-world network scenario is provided. This simulation provides insight into how protocols might respond to changes in the network environment. It helps to understand the significance of the proposed method in the FANETabove other protocols.

4.2 | The Significance of UAV Density on the FANET

Any network with more drones usually faces decreased speeds as the number of drones increases. No matter how good a protocol is, it usually loses effectiveness as more networks are added over time. The suggested strategy aims to progressively increase the number of UAVs better to understand the variations in the FANET routing protocol. Since new paths are only established when necessary, improving this network's routing matrix takes a while. Even though this flying ad hoc protocol's dynamic variations are excellent, we should keep in mind that this increases the processing load. Although it can optimize the network configuration, the routing procedure will still consume significant bandwidth. The suggested approach clusters the network before managing the nodes based on trust scores. When a new UAV is introduced, the trust-based categorization accuracy system counts it as an addition to the neighboring cluster. This will prevent the new UAV from becoming isolated.

Moreover, the clustering procedure resolves security concerns and enables efficient network administration. Next, in addition to aiding in selecting the leaders, the leader drone selection protocol controls inter-cluster routing. This pre-planner routing helps ensure that the packet reaches its destination safely. To choose which UAV to send the data to next, the leader will immediately speak with the other leaders rather than inspect each node. In FANET, the entire routing process is controlled by the leaders of the several clusters dispersed along the way. Therefore, the suggested method can achieve higher throughput compared to SecRIP [13] and UNION [10].

The figure demonstrates that the suggested methodology is not significantly affected by an increase in nodes. The delay that happens when packets are sent to their destination is computed to determine the network performance. The delay may be from dropped packets or getting caught in congestion. Because it is hard to predict the network at any given time, delays will always occur, regardless of how efficient the network is. The delay is a little longer than that of the previously mentioned methods. The recommended method also provides lower overhead because of a higher node density, as shown in *Fig 1*.

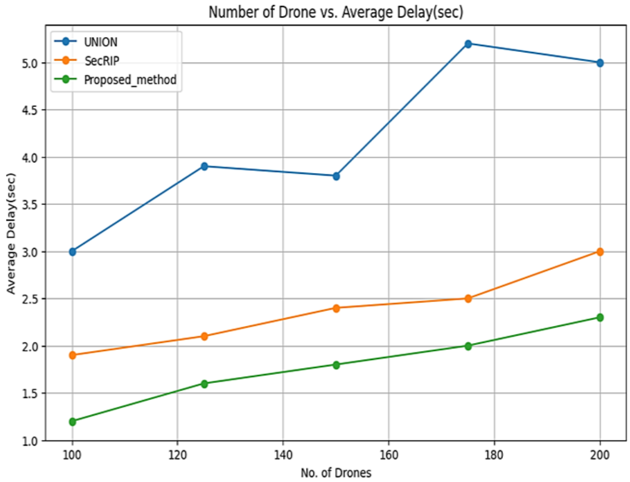

Fig. 1. Comparison of the proposed scheme with other models to the number of drones and average delay.

4.2.1 | Packet delivery ratio

The proposed scheme performs better than SecRIP and UNION in terms of packet delivery ratio, as it mostly routes packets by cluster heads despite network delays, as shown in *Fig. 2*. SecRIP prioritizes security, potentially resulting in a lower packet delivery ratio. UNION only covers routing, not security measures.

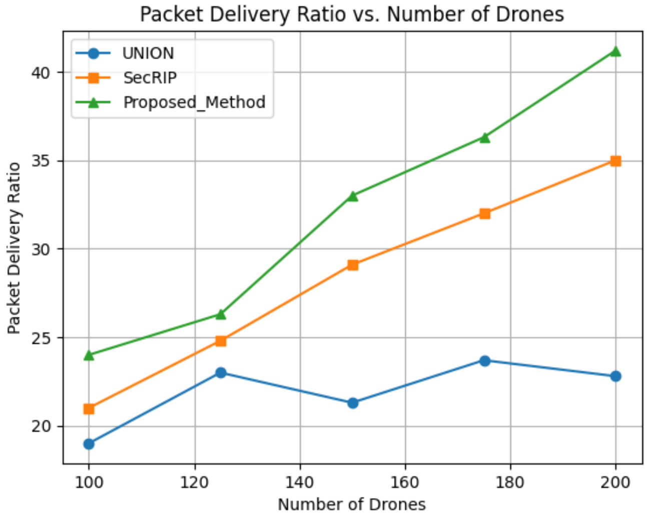

Fig. 2. Comparison of the proposed scheme with other models to the number of drones and packet delivery ratio.

4.2.2 | Latency

The proposed approach to network latency reduction is clustering, partitioning the network into multiple clusters under a cluster head. This trust-based clustering technique ensures the total transmission of each cluster is controlled, thereby reducing latency and maintaining service quality in trusted communication networks. The proposed scheme performs better than UNION and SecRIP regarding network latency, as described in *Fig. 3*.

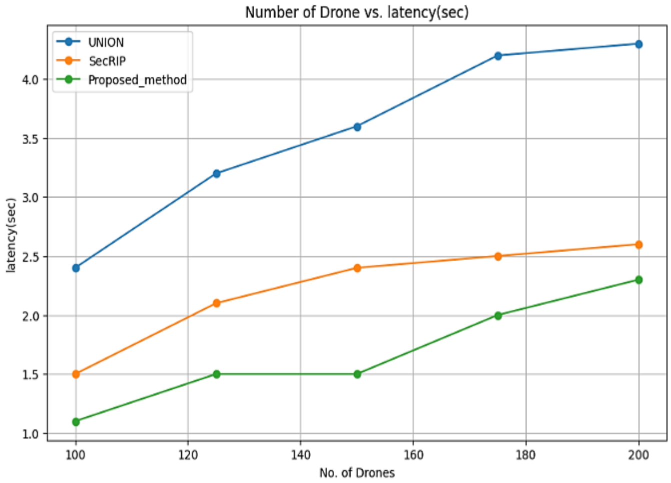

Fig. 3. Comparison of the proposed scheme with other models to the number of drones and latency.

4.3 | The Significance of UAVs Data Flow Effect in FANET

The amount of data flow within FANET is important because large data flows might cause more traffic jams and collisions. With increasing data traffic comes the possibility that packets may go along a path that has long till the end. Data loss and needless network delays would surely result from this. The proposed protocol guarantees network efficiency by simplifying the routing process through clustering. The leader drone is in charge of safely guiding packets through its clusters, then to other clusters, and finally to the desired location. Since the leader drones would have already determined which nodes will form the route towards the objective, an increase in data flow won't cause any additional delays. Takes a far shorter amount of time than alternative protocol iterations. For the simulation, the data rate is altered. The result of the graph illustrates the amount of delay time that procedures under examination encountered about the various data rates individually. The delay between SecRIP [13] and UNION [10] is more than the proposed scheme. The increase in different amounts of data traffic caused routing overheads. As shown in figure, the overhead due to the increasing data flow in the proposed method is less than that of existing ones. As Figure shows, the packet delivery ratio rates of SecRIP [13] and UNION [10] are lower than the proposed protocol shown in *Fig. 2*.

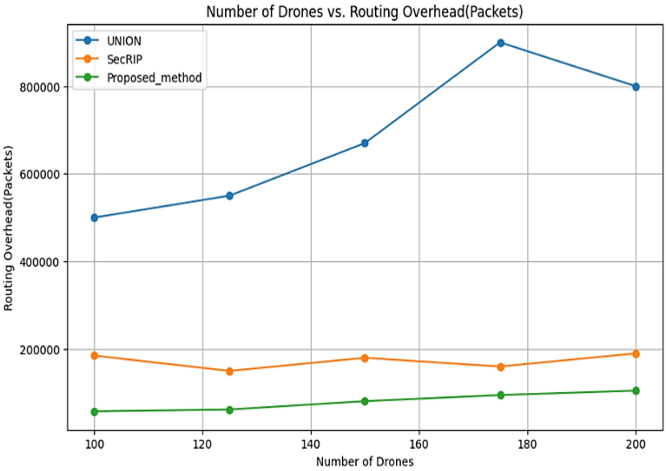

Fig. 4. Comparison of the proposed scheme with other models concerning the number of drones and routing overhead.

5 | Conclusion

FANET is made up of unmanned aerial vehicles that communicate with one another. The scheme is based on bioinspired technology. The two algorithms that make up this protocol are a bio-inspired ACO algorithm and a trust-aware algorithm. These algorithms group available UAVs into clusters and choose the best control form. It consists of two main phases: an ACO Algorithm based on bioinspired principles and a leader selection algorithm that considers trust. The first one helps to create clusters with the available drones in FANET, and the second one helps to select a suitable leader drone from them. Additionally, this proposed method guarantees that the transfer occurs with the least energy usage possible.

The proposed method aims to optimize the route within FANET. Simulation outputs show the higher network objectives the proposed protocol may reach over the current approaches compared to other protocols like UNION and SecRIP. Algorithms aid in effectively routing packets throughout the network using the selected leader drone for each cluster. This facilitates data forwarding to the intended destination by identifying control for every cluster. Additionally, the proposed method ensures that the transmission occurs with the least energy usage feasible. Stated differently, the algorithm seeks to minimize the energy consumption of the UAV. Consequently, the proposed method can meet the QoS and QoE parameters.

Author Contribution

All the authors contributed equally to the paper.

Data Availability

The data used in this study are available upon request from the corresponding author.

Funding

The study received no funding.

Conflicts of Interest

All the authors have no conflict of interest.

References

[1] Hosseinzadeh, M., Mohammed, A. H., Alenizi, F. A., Malik, M. H., Yousefpoor, E., Yousefpoor, M. S., … Tightiz, L. (2023). A novel fuzzy trust-based secure routing scheme in flying ad hoc networks. *Vehicular communications*, *44*, 100665. DOI:10.1016/j.vehcom.2023.100665

[2] Wang, Z., Tian, L., Lin, L., Xie, J., Wu, W., & Tong, Y. (2023). Data collection system of iot based on the coordination of drones and unmanned surface vehicle. *Journal of advanced transportation*, *2023*, 1–21. DOI:10.1155/2023/3426932

[3] Abdulhae, O. T., Mandeep, J. S., & Islam, M. (2022). Cluster-based routing protocols for flying ad hoc networks (FANETs). *IEEE access*, *10*, 32981–33004. DOI:10.1109/ACCESS.2022.3161446

[4] Liu, Y., Xie, J., Xing, C., & Xie, S. (2023). Topology construction and topology adjustment in flying Ad hoc networks for relay transmission. *Computer networks*, *228*, 109753. DOI:10.1016/j.comnet.2023.109753

[5] Ye, Z., Wang, K., Chen, Y., Jiang, X., & Song, G. (2022). Multi-uav navigation for partially observable communication coverage by graph reinforcement learning. *IEEE transactions on mobile computing*, *22*(7), 1–15. DOI:10.1109/TMC.2022.3146881

[6] Tsao, K. Y., Girdler, T., & Vassilakis, V. G. (2022). A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks. *Ad hoc networks*, *133*, 102894. DOI:10.1016/j.adhoc.2022.102894

[7] Messaoudi, K., Oubbati, O. S., Rachedi, A., Lakas, A., Bendouma, T., & Chaib, N. (2023). A survey of UAV-based data collection: Challenges, solutions and future perspectives. *Journal of network and computer applications*, *216*, 103670. DOI:10.1016/j.jnca.2023.103670

[8] Tlili, F., Fourati, L. C., Ayed, S., & Ouni, B. (2022). Investigation on vulnerabilities, threats and attacks prohibiting UAVs charging and depleting UAVs batteries: Assessments & countermeasures. *Ad hoc networks*, *129*, 102805. DOI:10.1016/j.adhoc.2022.102805

[9] Singh, K., & Verma, A. K. (2020). TBCS: A trust based clustering scheme for secure communication in flying ad-hoc networks. *Wireless personal communications*, *114*(4), 3173–3196. DOI:10.1007/s11277-020-07523-8

[10] Barka, E., Kerrache, C. A., Lagraa, N., Lakas, A., Calafate, C. T., & Cano, J. C. (2018). UNION: A trust model distinguishing intentional and unintentional misbehavior in inter-UAV communication. *Journal of advanced transportation*, *2018*. DOI:10.1155/2018/7475357

[11] Ganesan, R., Raajini, X. M., Nayyar, A., Sanjeevikumar, P., Hossain, E., & Ertas, A. H. (2020). Bold: Bio-inspired optimized leader election for multiple drones. *Sensors (switzerland)*, *20*(11), 3134. DOI:10.3390/s20113134

[12] Du, X., Li, Y., Zhou, S., & Zhou, Y. (2022). ATS-LIA: A lightweight mutual authentication based on adaptive trust strategy in flying ad-hoc networks. *Peer-to-peer networking and applications*, *15*(4), 1979–1993. DOI:10.1007/s12083-022-01330-7

[13] Bhardwaj, V., Kaur, N., Vashisht, S., & Jain, S. (2021). SecRIP: Secure and reliable intercluster routing protocol for efficient data transmission in flying ad hoc networks. *Transactions on emerging telecommunications technologies*, *32*(6), e4068. DOI:10.1002/ett.4068

[14] Gankhuyag, G., Shrestha, A. P., & Yoo, S. J. (2017). Robust and reliable predictive routing strategy for flying ad-hoc networks. *IEEE access*, *5*, 643–654. DOI:10.1109/ACCESS.2017.2647817

[15] Yu, S., Lee, J., Sutrala, A. K., Das, A. K., & Park, Y. (2023). LAKA-UAV: Lightweight authentication and key agreement scheme for cloud-assisted unmanned aerial vehicle using blockchain in flying ad-hoc networks. *Computer networks*, *224*, 109612. DOI:10.1016/j.comnet.2023.109612

[16] Bhardwaj, V., & Kaur, N. (2021). SEEDRP: a Secure energy efficient dynamic routing protocol in fanets. *Wireless personal communications*, *120*(2), 1251–1277. DOI:10.1007/s11277-021-08513-0

[17] Zhai, W., Liu, L., Ding, Y., Sun, S., & Gu, Y. (2023). ETD: An efficient time delay attack detection framework for UAV networks. *IEEE transactions on information forensics and security*, *18*, 2913–2928. DOI:10.1109/TIFS.2023.3272862

[18] Namdev, M., Goyal, S., & Agarwal, R. (2021). An optimized communication scheme for energy efficient and secure flying ad-hoc network (FANET). *Wireless personal communications*, *120*(2), 1291–1312. DOI:10.1007/s11277-021-08515-y

[19] Khan, M. A., Qureshi, I. M., & Khanzada, F. (2019). A hybrid communication scheme for efficient and low-cost deployment of future flying AD-HOC network (fanet). *Drones*, *3*(1), 1–20. DOI:10.3390/drones3010016

[20] Lu, Y., Wen, W., Igorevich, K. K., Ren, P., Zhang, H., Duan, Y., … Zhang, P. (2023). UAV ad hoc network routing algorithms in space–air–ground integrated networks: Challenges and directions. *Drones*, *7*(7), 448. DOI:10.3390/drones7070448

[21] Sharma, B., Obaidat, M. S., Sharma, V., & Hsiao, K. F. (2020). Routing and collision avoidance techniques for unmanned aerial vehicles: Analysis, optimal solutions, and future directions. *International journal of communication systems*, *33*(18), e4628. DOI:10.1002/dac.4628

[22] Khan, M. F., Yau, K. L. A., Noor, R. M., & Imran, M. A. (2020). Routing schemes in FANETs: A survey. *Sensors (switzerland)*, *20*(1), 38. DOI:10.3390/s20010038

[23] Xu, M., Xie, J., Xia, Y., Liu, W., Luo, R., Hu, S., & Huang, D. (2020). Improving traditional routing protocols for flying ad hoc networks: a survey. *2020 ieee 6th international conference on computer and communications, iccc 2020* (pp. 162–166). IEEE. DOI: 10.1109/ICCC51575.2020.9345206

[24] Mukherjee, A., Dey, N., Kausar, N., Ashour, A. S., Taiar, R., & Hassanien, A. E. (2016). A disaster management specific mobility model for flying ad-hoc network. In *International journal of rough sets and data analysis* (Vol. 3, pp. 72–103). IGI global. DOI: 10.4018/ijrsda.2016070106

[25] Kaur, M., Verma, S., & Kavita. (2020). Flying ad-hoc network (fanet): Challenges and routing protocols. *Journal of computational and theoretical nanoscience*, *17*(6), 2575–2581. DOI:10.1166/jctn.2020.8932

[26] Pan, H., Liu, Y., Sun, G., Fan, J., Liang, S., & Yuen, C. (2023). Joint power and 3D trajectory optimization for UAV-enabled wireless powered communication networks with obstacles. *IEEE transactions on communications*, *71*(4), 2364–2380. DOI:10.1109/TCOMM.2023.3240697

[27] Beegum, T. R., Idris, M. Y. I., Ayub, M. N. Bin, & Shehadeh, H. A. (2023). Optimized routing of UAVs using bio-inspired algorithm in FANET: A systematic review. *IEEE access*, *11*, 15588–15622. DOI:10.1109/ACCESS.2023.3244067

[28] Alkadi, R., & Shoufan, A. (2023). Unmanned aerial vehicles traffic management solution using crowd-sensing and blockchain. *IEEE transactions on network and service management*, *20*(1), 201–215. DOI:10.1109/TNSM.2022.3201817

[29] Mohsan, S. A. H., Othman, N. Q. H., Li, Y., Alsharif, M. H., & Khan, M. A. (2023). Unmanned aerial vehicles (UAVs): practical aspects, applications, open challenges, security issues, and future trends. *Intelligent service robotics*, *16*(1), 109–137. DOI:10.1007/s11370-022-00452-4

[30] Bansal, G., Naren, Chamola, V., & Sikdar, B. (2022). SHOTS: scalable secure authentication-attestation protocol using optimal trajectory in UAV swarms. *IEEE transactions on vehicular technology*, *71*(6), 5827–5836. DOI:10.1109/TVT.2022.3162226

[31] Khayat, G., Mavromoustakis, C. X., Pitsillides, A., Batalla, J. M., Markakis, E. K., & Mastorakis, G. (2023). On the weighted cluster s-UAV scheme using latency-oriented trust. *IEEE access*, *11*, 56310–56323. DOI:10.1109/ACCESS.2023.3282441

[32] Wei, W., Wang, J., Fang, Z., Chen, J., Ren, Y., & Dong, Y. (2023). 3U: Joint design of UAV-USV-UUV networks for cooperative target hunting. *IEEE transactions on vehicular technology*, *72*(3), 4085–4090. DOI:10.1109/TVT.2022.3220856

[33] Bastami, H., Moradikia, M., Abdelhadi, A., Behroozi, H., Clerckx, B., & Hanzo, L. (2022). Maximizing the secrecy energy efficiency of the cooperative rate-splitting aided downlink in multi-carrier UAV networks. *IEEE transactions on vehicular technology*, *71*(11), 11803–11819. DOI:10.1109/TVT.2022.3192298

[34] Shimaa S. Mohamed, Ahmed Abdel Monem, & Alshaimaa A. Tantawy. (2023). Neutrosophic MCDM methodology for risk assessment of autonomous underwater vehicles. *Neutrosophic systems with applications*, *5*, 44–52. DOI:10.61356/j.nswa.2023.32

[35] Nada A.Nabeeh, Karam M. Sallam, & Ali Wagdy Mohamed. (2023). An electric vehicle analysis model for sustainable environment in devoicing nationals. *Neutrosophic systems with applications*, *6*, 1–8. DOI:10.61356/j.nswa.2023.26

[36] Maia, A. L. M. D., & Frogeri, R. F. (2023). Optimizing business value via it governance mechanisms: An examination of SMEs in southern minas Gerais, Brazil. *Journal of operational and strategic analytics*, *1*(3), 106–114. DOI:10.56578/josa010301

[37] Pajić, V., & Andrejić, M. (2023). Risk analysis in internal transport: An evaluation of occupational health and Safety using the fine-kinney method. *Journal of operational and strategic analytics*, *1*(4), 147–159. DOI:10.56578/josa010401

[38] Ghanbari Talouki, A., Koochari, A., & Ahmad Edalatpanah, S. (2024). Image completion based on segmentation using neutrosophic sets. *Expert systems with applications*, *238*, 121769. DOI:10.1016/j.eswa.2023.121769

[39] Venugopal, R., Veeramani, C., & Edalatpanah, S. A. (2024). Enhancing daily stock trading with a novel fuzzy indicator: Performance analysis using Z-number based fuzzy TOPSIS method. *Results in control and optimization*, *14*, 100365. DOI:10.1016/j.rico.2023.100365