GRADIENT MONITORING REINFORCEMENT LEARNING FOR JAMMING ATTACK DETECTION IN FANETs

N.S KAVITHA[1] , M.KAVINKUMAR [2] , N. SENTHIL KUMAR [3]

[1]*Associate Professor Grade-I, Department of CSE, Sri Ramakrishna Institute of Technology, Coimbatore, Tamil Nadu , India*
[2 3] *UG students, Department of CSE, Sri Ramakrishna Institute of Technology, Coimbatore, Tamil Nadu , India*

Abstract— As Unmanned Aerial Vehicle (UAV) technology advances, UAVs are becoming more and more common in both military and civilian applications. The term flying ad hoc networks (FANET) is frequently used to describe multi-UAV networks. UAV clustering is a crucial path for UAV network applications since it may enhance network scalability, minimize energy consumption, and maximize network lifetime when multiple UAVs are divided into clusters for management. Additionally, the special features of these systems make it difficult to improve their defences against constantly changing security threats, making security provision in these systems especially complex. We introduced Secure and Hybrid Bio Inspired Optimization (SHBIO) for FANETs, an innovative, effective, and hybrid bioinspired algorithm, in this suggested framework. This research proposes an adaptable, secure, and efficient bio-inspired routing model with the goal of developing a new, trustworthy security framework. For this, it suggests Ant Colony Optimization (ACO), one of the most popular methods for trusted route computing. safe route selection using the ACO method. Among the interrelated parts and layers that comprise the architecture is the Trust Management System, which assesses each drone's reliability based on a variety of trust factors.

Key Terms: Jamming Attack, Gradient Monitoring, Communication Security, Multi-Agent Systems.

I. INTRODUCTION

Unmanned Aerial Vehicles (UAVs), also known as drones, have evolved to the point where they can now communicate and work together by forming ad hoc networks, often called FANETs (Flying Ad Hoc Networks). These types of networks are gaining popularity in many fields like precision farming, package delivery, construction, environmental and climate monitoring, and military operations. Because of all these new and exciting uses, researchers are taking a fresh look at how FANETs work. UAVs can be either remotely controlled by someone on the ground or run independently using onboard systems. They've become a big part of wireless communication setups and are used in a wide range of missions — from defense to agriculture. When multiple UAVs fly together and form a network without needing any fixed infrastructure, it's called a FANET. There are many types of UAVs used in these networks, and they can be categorized based on different factors like size, weight, range, endurance, altitude capability, purpose, flight mechanism, ownership, level of autonomy, and even motor type. Recently, there's been a lot of research exploring how UAV swarms can be integrated with other technologies like VR, edge computing (Flying FOG), mobile networks , and cloud systems in the air. While these integrations offer a lot of potential, they also bring challenges — from technical limitations to legal regulations. Still, with the growing demand and new use cases, FANETs continue to be a hot topic for researchers.

II. SCOPE OF THE PROJECT

The scope of this project can investigate a method based on reinforcement learning to identify and frustrate jam assaults on networks or flying ad hoc. Ensuring the transmission of safe and reliable data is essential given the growing dependence of the UAV for military, surveillance and communication purposes. The suggested model uses adaptive countermeasures and the detection of nonbridal attacks in real time by using gradient monitoring reinforcement learning. Technology improves the safety and efficiency of Fanet communications by continuously evaluating the circumstances of the network and modifying its tactics. Deep reinforcement learning techniques are used in the study to improve decision making in dynamic network scenarios. Through simulations and performance indicators, including detection precision, reaction time and network resilience, research also evaluates how effective the suggested approach is also. Although this method shows encouraging results, problems such as computational complexity and limitations in real world implementation still exist. Future research could concentrate on improving learning algorithms for faster and faster and more effective jam attack and mitigation, as well as blockchain integration for greater security.

III. EXISTING SYSTEM

In earlier works, the routing protocol we used for FANETs is called GWCOOP, which stands for Gray Wolf-based Cooperative Diversity routing. It uses the Gray Wolf Optimizer (GWO), inspired by how gray wolves hunt and interact socially. The protocol is built around the idea of using natural wolf behavior to support the needs of flying network nodes. We first focused on adapting GWO to better suit the flying environment by mimicking how wolves in the wild move and interact. Then we introduced cooperative diversity by using two relay nodes, which helps maintain strong links between the source and destination even if one path fails. This two-relay system combined with a bio-inspired algorithm is a new approach that hasn't been explored in FANETs before. To measure how well GW-COOP works, we compared it with two versions of BAT-COOP (which uses the Bat algorithm along with cooperative diversity) and evaluated them based on performance metrics. In GWO, the core idea is that wolves have a social order—Alpha, Beta, and Delta wolves lead the hunt. Similarly, in the algorithm, the three best candidate solutions guide the rest of the search. The alpha is the best, followed by beta and delta. This structure is used in GW-COOP to make routing decisions more effective by using collaboration and diversity among node

IV. LITERATURE SURVEY

H. Sedjelmaci, et. al,(1) Automated flying vehicles uavs networks have not yet gotten extensive examination consideration in particular security issues are a main issue on the grounds that such organizations which convey imperative data are inclined to different assaults in this paper we plan and carry out an original interruption identification and reaction conspire which works at the uav and ground station levels to identify vindictive oddities that underminethe organization in this plan a bunch of identification and reaction strategies are proposed to screen the uav ways of behaving and order them into the fitting rundown ordinary strange suspect and malignant as per the distinguished digital assault we center around the most deadly digital assaults that can focus on a uav organization specifically misleading data dispersal gps mocking sticking and dark opening and dim opening assaults broad reenactments affirm that the proposed conspire performs well as far as assault location even with an enormous number of uavs and aggressors since it shows a high identification rate a low number of misleading upsides and brief recognition with a low correspondence.

B. Mahalakshmi, et. al, (2) The rising requirement for convenient and adaptable correspondence has clears a way for network development among automated elevated vehicles uavs which is known as fanets also attributable to its elite elements of uavs like recurrence geography high versatility and 3d makes of directing most facing task in fanets with these elements planning based not entirely set in stone as critical element for settling directing emergency from now on this examination explicitly highlight on geography based steering convention named as fluffy based markov chain bunch fmcc with a goal of upgrading productivity of organizations as far as asset usage time delay transmission proportion and asset accessibility at first consider an organization model and the issues related in building an organization without loss of bundle transmission neighborhood development etc in this work reenactment is finished in ns-2 test system and results are broke down in light of start to finish delay throughput group development bunch lifetime etc this strategy portrays better compromise as opposed to winning procedures the 11 data related with the data trade is considered for remodeling the work strongly.

G. Secinti, et. al, (2017) The automated flying vehicular uav networks broaden remote access for gadgets without framework inclusion and furthermore assist with laying out an availability spine duringmilitary observation and debacle occasions this paper centers around the plan of a versatile endto-end network worldview under novel design and situation suppositions in the first place the uavs themselves are outfitted with various connection points that utilization normalized conventions with related variety in information all through reach and spot mistake rates second there might be ill-disposed specialists looking to disturb availability through designated sticking in 3d spaces third we expect an overlay programming characterized control plane where the uavs capability as programming switches ready to execute sending orders and decide favored courses under regulator mandates this proposed approach formulated measurements that impact the decision of the remote point of interaction and loads edges shaped between uav matches further it likewise utilizes a multi facet chart model and makes maximally isolated ways in 3d space to guarantee flexibility to sticking recreation results directed for metropolitan situations uncover 34 improvement in upgraded versatility for start to finish blackouts by compromising 12 expansion in idleness over contending approach.

V. PROPOSED SYSTEM

In this proposed framework, we proposed an algorithms of inspiration, efficient, efficient and hybrids used, namely biography optimization (Shbio) for fans. This work to combine the group and also maintains the safety of flying networks. So basically, this paper suggests a way to organize UAVs into groups using the Binary Whale Optimization Algorithm (BWOA). The process starts by figuring out how many groups are ideal based on things like how much bandwidth is available and how far each node can reach. Once that's done, the algorithm picks cluster heads based on the best number of groups, and the rest of the nodes are grouped by how close they are. There's also a strategy set up to keep these clusters stable and working efficiently over time. Then, the following purpose of this document is to create a new safe and reliable security framework by proposing a bio routing model inspired by insurance and

adaptive efficient. Recommend Ant Col belation (ACO),For this purpose. Safe route selection based on ACO technique.

The trust management system, which evaluates the reliability of each drone using several confidence criteria, is one of the interconnected components and layers that make up the architecture. To make better use of network resources, this work starts by figuring out the best number of UAV groups based on available bandwidth and how far each UAV can cover. To manage these groups more effectively, it introduces a cluster formation method using the Binary Whale Optimization Algorithm (BWOA).

The goal is to avoid constantly reshaping the clusters, so it focuses on picking more stable cluster heads and setting up a smart way to maintain the clusters, which helps extend their overall lifetime and reduce strain on the network. For routing inside and between these clusters, the communication paths are handled separately to balance the load across nodes and keep the routes efficient, which in turn improves the overall network performance.

VI.SYSTEM ARCHITECTURE

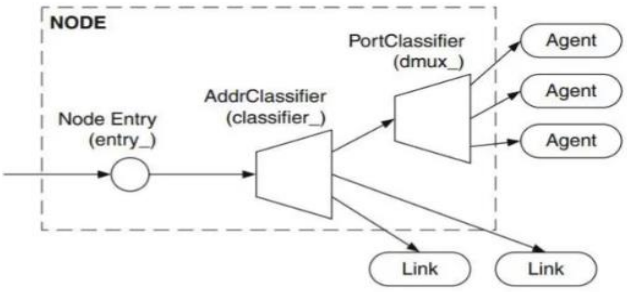

Figure 1: System architecture of node

The given diagram represents a node architecture in a network simulation, probably based on the NS-2 frame (Red-2 simulator). Illustrates how a network node processes incoming packages and directs them to the appropriate destination within the node. The architecture consists of the following key components:

1.Node Entry (entry_)

- This is the main entry point where packets first arrive at the node.
- It serves as the initial processing unit before passing data to the next stage.

2.Address Classifier (classifier_)

- This component determines the destination of incoming packets.
- It checks the packet's destination address and forwards it to the appropriate module inside the node.

3.Port Classifier (dmux_)

- This component directs packets to the appropriate agent within the node.
- It acts as a demultiplexer (dmux), forwarding packets to
- different agents based on their protocol type (e.g., TCP, UDP, or routing agents).

1. Agents

• These represent network layer or transport layer entities that process packages inside the node.

• Agents can be protocols such as TCP, UDP or application level entities that manage packages.

5. Links

• If the package is not intended for this node, it is forwarded to a outgoing link for additional network transmission.

• Links represent network connections between nodes

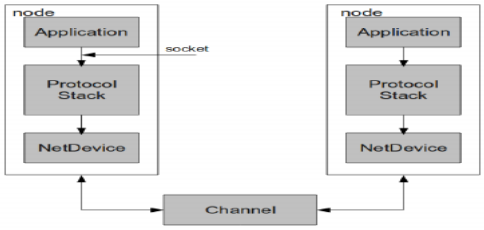

Figure 2: system architecture of NS-3

The image represents a network simulation model, likely based on ns-3 (Network Simulator 3). Here's a breakdown of the components:

1.Node:

- A node is a computer device (such as a computer, a router or mobile device) on a network.
- The diagram shows two nodes.

2. Application:

- This is the highest layer that generates data and interacts with the user.
- Represents network applications (for example, a web browser, video transmission, etc.).

3. Protocol battery:

- This includes network protocols such as TCP/IP or UDP.
- Ensures that the data is transmitted correctly between applications in different nodes. •

4.Netdevice:

- Represents a network interface card (NIC) or a similar hardware component that connects to a network.
- Interact with the physical or simulated network.

5.Channel:

- Represents the means of communication between the two nodes.
- This could be a wired or wireless connection.
- NS3 :: Net device (mentioned in the diagram):
- This is a part of the NS-3 network simulator.
- Provides an interface for network communication between nodes

VII. RESULT AND ANALYSIS

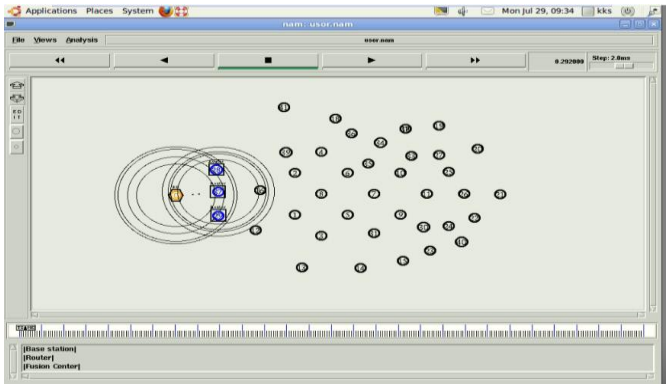

Figure 3

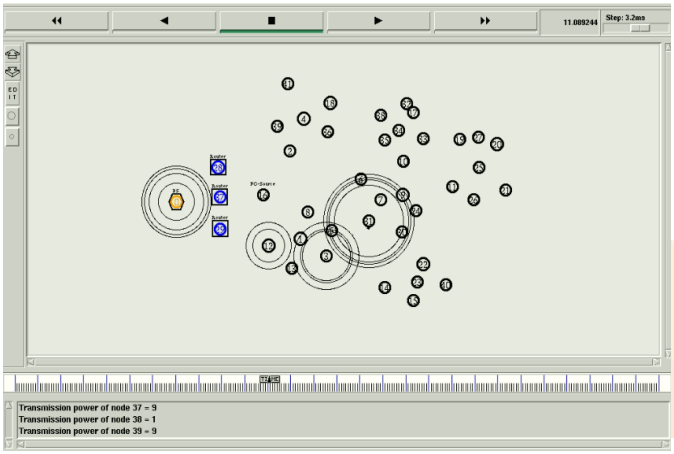

Figure 4

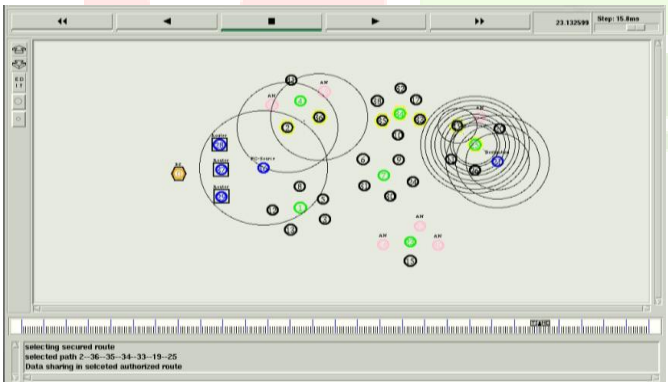

Figure 5

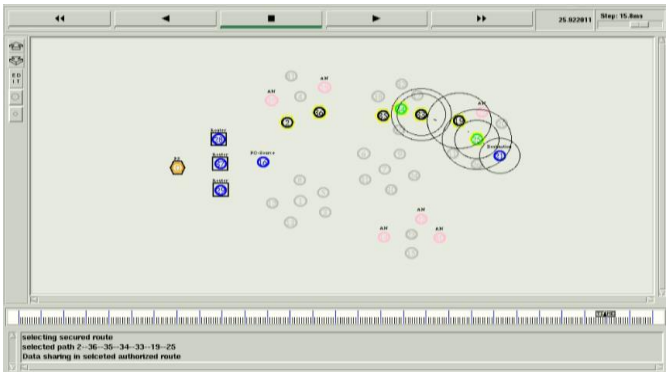

Figure 6

The figure all shows the network simulation output by several and the image shows a wireless network simulation in the network animator (NAM), a tool used in NS-2 (network simulator 2). It shows a set of network nodes, represented as black circles, and some are actively communicated. The most left cluster includes an orange node, which probably serves as a base station or central node, surrounded by blue nodes that can act as routers or cluster heads. Concentric circles indicate the wireless signal coverage of the transmission nodes. The legend of the lower left suggests that the simulation represents a network of wireless sensors (WSN), where the nodes collect and transmit data to a central unit.

7.1 END TO END DELAY

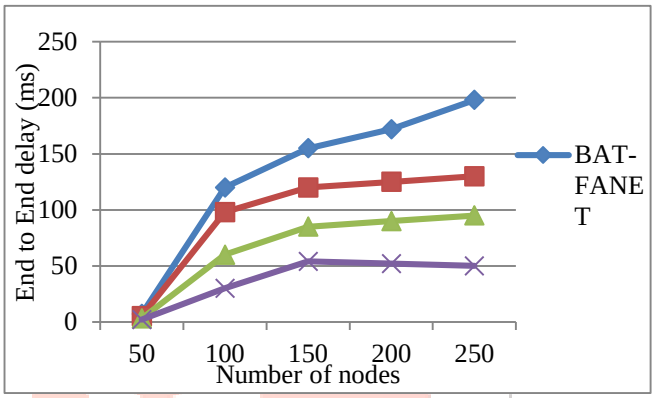

Figure 7.1 End to End delay evaluations

The end -to -end delay is the total time necessary to transmit data from the node of the sender to the recipient node that implies waiting time, execution time. In Figure 7.1 shows the evaluation of the previous and proposed method refers to the end -to -end delay metric. The number of nodes is taken on the X axis and end -to -end values are taken on the Y axis. In the previous method, end -to -end delay values are higher. In the methodology presented, the end-to-end delay value is significantly reduced using the Shbio-Bwoa_aco method. Consequently, it shows that the efficient recognition is done using the proposed method..

7.2 NETWORK LIFETIME

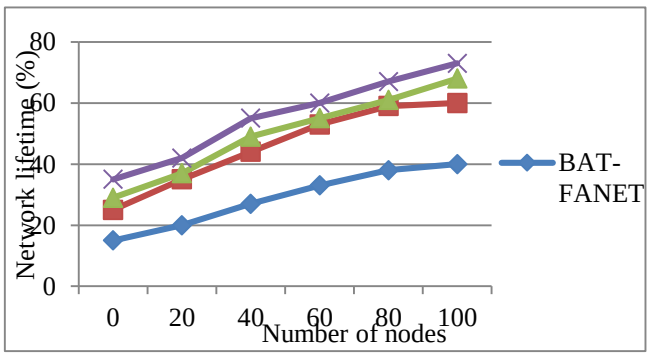

Figure 7.2 Network Lifetime evaluations

Looking at Figure 7.2, you can see how the previous method and the one we proposed compare in terms of network lifetime. The X-axis shows the number of nodes, and the Y axis shows how long the network stays active. In the older method, the network lifetime is lower. But with our new approach, using the Shbio BWOA_ACO technique, the lifetime improves a lot. This shows that the new method does a better job at managing the network and identifying efficient paths.

7.3 THROUGHPUT

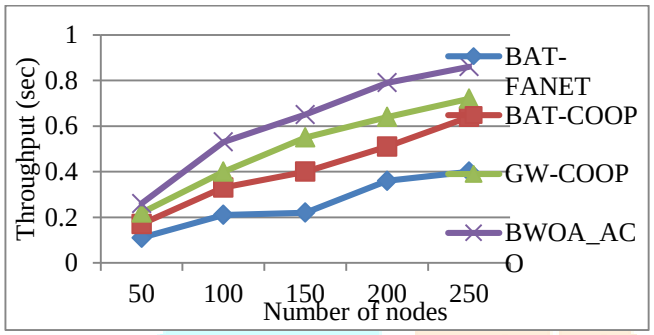

Figure 7.3 Throughput evaluations

According to Figure 7.3, it shows that the evaluation of the previous method and presented with respect to the performance metric. The number of nodes is taken on the X axis and the performance values are taken on the Y axis. In the previous method, the performance values are lower. In the technique presented, the performance value is significantly improved using the Shbio-Bwoa_aco method. Consequently, it shows that efficient identification is done using the proposed method..

7.4 PACKET DELIVERY RATIO

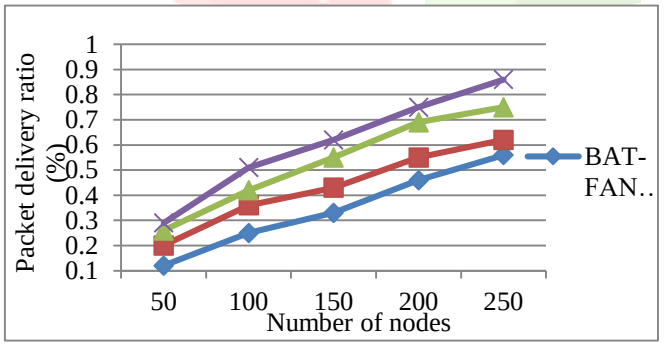

Figure 7.4 Packet delivery ratio evaluations

Looking at Figure 7.4, you can see how the previous method compares to the new one when it comes to packet delivery ratio. The number of nodes is on the X-axis, and the delivery ratio values are on the Y-axis. The older method shows lower delivery rates, but with the proposed ShbioBWOA_ACO approach, the packet delivery ratio improves a lot. This shows the new method is better at identifying efficient paths and managing data delivery.

7.5 PACKET LOSS

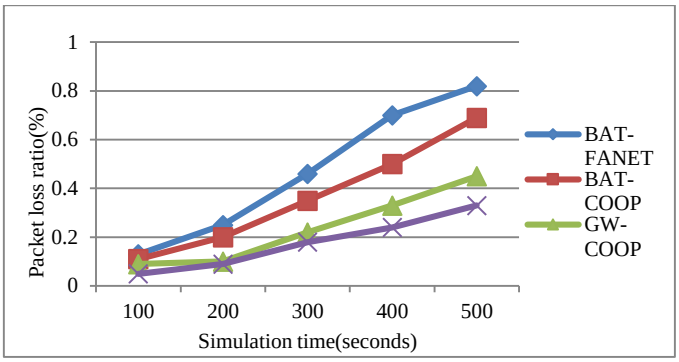

Figure 7.5. Packet loss ratio evaluation

In Figure 7.5, during a 500-second simulation, the proposed Shbio-BWOA_ACO method results in a packet loss of 28.59%. That's 9.59%, 4.95%, and 1.04% less compared to previous methods. So overall, it's clear that this new approach leads to fewer lost packets and performs better in terms of reliability

VIII. CONCLUSION

This article puts forward a clustering approach using the Binary Whale Optimization Algorithm (BWOA) to help reduce energy use in FANETs. First, it figures out the ideal number of cluster heads (CH) based on coverage needs and bandwidth balance. Then, it uses a fitness function that takes into account UAV energy levels, distances within and between clusters, and how balanced the groupings are. The best cluster heads are picked using BWOA. After that, UAVs are grouped based on proximity, and a smart cluster maintenance strategy helps keep everything running efficiently. When it comes to communication, UAVs prefer to forward data to the closest node with the highest remaining energy These algorithms group the UAV available in groups and choose the best control form.

It consists of two main phases: an algorithm based on principles inspired by Bio and a route selection algorithm that considers trust. The first helps create groups with the drones available in Fanet, and the second helps select an adequate leader of them. In addition, this proposed method guarantees that the transfer occurs with the least possible use of energy.

The algorithms help to encrypt the packages effectively throughout the network using the leader's drone for each cluster. This facilitates data forwarding to the planned destination identifying control for each cluster. In addition, the proposed method ensures that the transmission occurs with the lowest feasible energy use. In a different way, the algorithm seeks to minimize the energy consumption of the UAV

IX.REFERENCE

[1] Yan, Y.; Xia, X.; Zhang, L.; Li, Z.; Qin, C. A Clustering Scheme Based on the Binary Whale Optimization Algorithm in FANET. *Entropy* **2022**, *24*, 1366. https://doi.org/10.3390/e24101366

[2] 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.

[3] Shahzad Hameed1, Saleh Alyahya4, Link and Loss Aware GW-COOP Routing Protocol for FANETs," IEEE Access, 2021.

[4] Vijayanandh, R., J. Darshan Kumar, M. Senthil Kumar, L. Ahilla Bharathy, and G. Raj Kumar. "Design and fabrication of solar powered unmanned aerial vehicle for border surveillance." In Proceedings of International Conference on Remote Sensing for Disaster Management, pp. 61-71. Springer, Cham, 2019.

[5] Maimaitijiang, Maitiniyazi, Vasit Sagan, Paheding Sidike, Ahmad M. Daloye, Hasanjan Erkbol, and Felix B. Fritschi. "Crop Monitoring Using Satellite/UAV Data Fusion and Machine Learning." Remote Sensing 12, no. 9 (2020): 1357.

[6] Pantelej, Ekaterina, Nikolay Gusev, George Voshchuk, and Alexander Zhelonkin. "Automated field monitoring by a group of light aircrafttype UAVs." In International Conference on Intelligent Information Technologies for Industry, pp. 350-358. Springer, Cham, 2018.

[7] Odonkor, Philip, Zachary Ball, and Souma Chowdhury. "Distributed operation of collaborating unmanned aerial vehicles for time-sensitive oil spill mapping." Swarm and Evolutionary Computation 46 (2019): 52-68.

[8] Singh, Kuldeep, and Anil Kumar Verma. "Flying adhoc networks concept and challenges." In Advanced methodologies and technologies in network architecture, mobile computing, and data analytics, pp. 903-911. IGI Global, 2019.

[9] Padró, Joan-Cristian, Francisco-Javier Muñoz, Jordi Planas, and Xavier Pons. "Comparison of four UAV georeferencing methods for environmental monitoring purposes focusing on the combined use with airborne and satellite remote sensing platforms." International journal of applied earth observation and geoinformation 75 (2019): 130-140.

[10] Kang, Jin-Gu, Dong-Woo Lim, and Jin-Woo Jung. "Energy-efficient forest fire prediction model based on two-stage adaptive duty-cycled hybrid x-mac protocol." Sensors 18, no. 9 (2018): 2960.

[11] Choudhary, Gaurav, Vishal Sharma, and Ilsun You. "Sustainable and secure trajectories for the military Internet of Drones (IoD) through an efficient Medium Access Control (MAC) protocol." Computers & Electrical Engineering 74 (2019): 59-73.

[12] Stampa, M., Sutorma, A., Jahn, U., Willich, F., Pratzler-Wanczura, S., Thiem, J., ... & Wolff, C. (2020, September). A Scenario for a MultiUAV Mapping and Surveillance System in Emergency Response Applications. In 2020 IEEE 5th International Symposium on Smart and Wireless Systems within the Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS) (pp. 1-6). IEEE.

[13] Zeng, Yong, Rui Zhang, and Teng Joon Lim. "Wireless communications with unmanned aerial vehicles: Opportunities and challenges." IEEE Communications Magazine 54, no. 5 (2016): 36-42.

[14] Hameed, Shahzad, Qurratul-Ain Minhas, Sheeraz Ahmed, Shabana Habib, Mohammad Kamrul Hasan, Muhammad Islam, and Sheroz Khan. "An Improved iBAT-COOP Protocol for Cooperative Diversity in FANETs." CMC-COMPUTERS MATERIALS & CONTINUA 67, no. 2 (2021): 2527-2546.

[15] Guo, Qiang, Jichen Yan, and Wei Xu. "Localized fault tolerant algorithm based on node movement freedom degree in flying ad hoc networks." Symmetry 11, no. 1 (2019): 106