Investigating Quantum-Resilient Security Mechanisms for Flying Ad-Hoc Networks (FANETs)

Abdulnasser AbdulJabbar Abbood [1], Faris K. AL-Shammri [2], Zainab marid Alzamili [3], Mahmood A. Al-Shareeda [4*], Mohammed Amin Almaiah [5], Rommel AlAli [6*]

[1,4] Department of Electronic Technologies, Basra Technical Institute, Southern Technical University, 61001, Basra, Iraq

[2] Biomedical Engineering Department, College of Engineering, University of Warith Al Anbiyaa, Karbala 56001, Iraq

[3] Education Directorate of Thi-Qar, Ministry of Education, Iraq

[4] Department of Communication Engineering, Iraq University College (IUC), Basra, Iraq

[5] King Abdullah the II IT School, Department of Computer Science, The University of Jordan, Amman 11942, Jordan

[6] National Research Center for Giftedness and Creativity, King Faisal University, Saudi Arabia

Email: [1] abdulnasser.abbood@stu.edu.iq [2] faris.kar@uowa.edu.iq, [3] Zainab.alzamili@utq.edu.iq
[4] Mahmood.alshareedah@stu.edu.iq, [5] m.almaiah@ju.edu.jo,
[6] ralali@kfu.edu.sa,
*Corresponding Author

***Abstract*—Flying Ad Hoc Networks (FANETs) are indispensable in applications such as Surveillance, Disaster response missions, and Military operations. Both security and communication efficiency must meet certain requirements. However, their effectiveness is hobbled by dynamic topologies, resource constraints, and cyber threats. Therefore, Post-Quantum Cryptography (PQC) is necessary. Classical algorithms and current PQC schemes for FANETs have been discussed in this thesis, including cryptographic solutions that are lightweight enough for resource-constrained environments. The numerical results of the experiment show that while lattice-based cryptography involves minimal risk of breaches, its power consumption is 25% higher than that for other systems and its processing time 30% slower. In contrast, multivariate polynomial cryptography is better on metrics like usage of electricity: only 10% more power consumed energy-wise and 15% more CPU cycles needed for processing. The introduction of PQC algorithms and architectures resulted in a 5–10% reduction in network throughput and increased latency to 20% in some scenarios. The results show that hybrid cryptographic systems—combining classical with PQC techniques—have the potential to achieve both high efficiency and long-term security. Case studies have validated the feasibility of tailored quantum-safe algorithms in FANETs, which can offer considerable security benefits while standing rigorous scrutiny in terms of scalability and computational performance on dynamic, mission-critical operations.**

Keywords*—Lightweight Cryptographic Solutions; Flying Ad Hoc Networks (FANETs); Resource-Constrained Networks; Post-Quantum Cryptography (PQC); Quantum Computing; UAV Security

I. Introduction

Flying Ad Hoc Networks (FANETs) is a more developed type of wireless networks that focuses on communication between Unmanned Aerial Vehicles (UAVs) [1]–[3]. FANETs topology is dynamic and distributed as with traditional Mobile Ad Hoc Networks (MANETs) or Vehicular Ad Hoc Networks (VANETs), but the missions are of great significance and critical like surveillance, disaster response, military applications etc [4]–[6]. They present novel challenges in their architecture: real-time requirements, scalable structures, and restricted resources; hence being a focus of state-of-the-art research and development.

Communication protocol is an essential element of FANETs that ensures UAVs work as a united organism while always being connected to GS and satellites. FANETs can be operated in different environments with the help of UAV-to-UAV (U2U), UAV-to-Ground (U2G) and UAV-to-Satellite (U2S) communication frameworks. Such communication channels enable mission data flow, complexity scaling in a highly dynamic environment while facing challenges like interference, latency and bandwidth [7].

FANETs are highly decentralized with a high nature of mobility and several resource constrained nodes which makes them prone to multiple security threats. Problems like interception, spoofing, jamming and physical capture threaten not just data integrity but operational functionality [8]. As FANETs depends more on some sensitive applications, so it is extremely important to have more efficient and light cryptographic solutions suitable for the characteristics of FANET.

Quantum computing has accelerated the need for adopting Post-Quantum Cryptography (PQC) in FANETs [9]–[11]. Quantum attacks easily break conventional cryptography (RSA, ECC), so new quantum-resistant algorithms are needed. PQC provides novel algorithms, like lattice-based and hash-based cryptography, that can improve the security and scalability of FANETs as a complement to their mission-critical yet resource-constrained operational requirements.

- Evaluation of Post-Quantum Cryptographic Algorithms for FANETs: This work examines the performance, scalability and other characteristics of several post-quantum cryptographic (PQC) algorithms, including lattice-based, hash-based and multivariate polynomial cryptography exercises for this evaluation over low-energy wireless networks such as Flying Ad Hoc Networks (FANETs).
- Recommendation of Solutions Combining Hybrid Cryptography: The study points out those hybrid cryptographic systems that combine classical cryptography with PQC solution. This method strikes a trade-off between short-term operational efficiency and long-term quantum-resistant security in FANET applications.
- Seamless integration of PQC protocols in FANET environments: The paper effectively uses novel simulation frameworks to demonstrate the practicality of seamless integration of realistic and state-of-the-art PQC protocols, thereby eliminating performance bottlenecks in secure key exchange, message authentication and real-time communication. These findings confirm the validity of PQC with respect to how future implementations should be designed.

It continues to follow this way in the rest of the article. Part II introduces FANETs as an object, discussing its construction, communication framework, and main issues with safety. Part III presents a broad outline of Post-Quantum Cryptography, introducing the importance and gauges for preserving different algorithmic approaches in FANETs. Part IV deals with using Post-Quantum Cryptography in FANETs, considering probable obstacles when integrating this technology and offering some solutions. Part V presents the results, taking up PQC algorithms' impacts on computation, power, and scalability. Section VI discusses the results of this paper. Finally, Part VII wraps up the paper with a summary of these results and some hints for future research using quantum-resistant techniques that protect FANETs.

II. Overview of FANETs and Security Requirements

A. Architecture and Communication in FANETs

Flying Ad Hoc Networks (FANETs) are a type of wireless network consisting of Unmanned Aerial Vehicles (UAVs), which enable UAVs to communicate with each other and communicate between GCS for performing different tasks [12]–[14]. Smart Dust differs in the architecture and communication characteristics from conventional ad hoc structures like MANETs (Mobile Ad Hoc Networks) [15]–[18] or VANETs (Vehicular Ad Hoc Networks) [19]–[21].

- UAV Layer: Multi-UAV-based unit with [sensors, communication and computation, forms the backbone of FANETs] These UAVs acquire, process and pass on data but their role dynamically depends on the specifications of the mission scenario [22], [23]. They can only be designed to their specification according to well-known size weight and power (SWaP) constraints, which require optimization both in hardware and software. Their functioning as a network helps to preserve the communication with the base, while ensuring performance of mission objectives in the regions such as disaster zones, urban areas or remotest of sites [24].
- Communication Layer: The communication layer is the fundamental interface for data exchange in FANETs, as it allows UAVs (U2U) to communicate with each other as well as with ground stations (U2G) and even satellites (U2S). It provides robust, secure and low-latency connectivity—all of which is paramount to successful functionality within this highly dynamic and decentralized network [24]–[26]. The communication layer supports resilience against mobility and environmental losses for real-time data transfer applications of surveillance, mapping and emergency. This layer uses higher level protocols to optimize the usage of bandwidth and keeps the process of communication going on smoothly in normal circumstances [27], [28].
- Ground Control Layer: The ground control layer allows for centralized or distributed FANET operation control, mission planning, real-time monitoring and decision making. To support long-range operations, ground control stations connect with UAVs through high-capacity communication links, including satellite (or cellular) networks [29]–[31]. This layer plays a key role in UAV deployment, multi-UAV coordination and data processing for actionable information. It has an underlying infrastructure that allows for scaling while maintaining operational integrity of the FANET, even in intricate or mission critical situations.

Table I highlights the distinct roles and interdependencies of each layer within FANETs.

B. Key Architectural Features

- Dynamic Topology: The relatively high mobility of UAVs results in a constantly varying topology [32].
- Distributed Coordination: FANETs typically function without central authority and maintain coordination using distributed manner [33].

TABLE I. COMPARISON OF LAYERS IN FANET ARCHITECTURE

Feature	UAV Layer	Communication Layer	Ground Control Layer
Primary Function	Core of the FANET, comprising UAVs that collect, process, and relay data.	Facilitates data exchange among UAVs, ground stations, and satellites.	Mission planning, real-time monitoring, and decision-making.
Components	UAVs with sensors, communication modules, and processing units.	Communication protocols and links (U2U, U2G, U2S).	Ground control stations with satellite and cellular connectivity.
Dynamic Role	UAVs adapt to act as data sources or relays based on the network topology.	Supports dynamic communication under changing network conditions.	Adjusts mission strategies and UAV coordination as required.
Key Challenges	SWaP constraints, mobility, and environmental adaptability.	Maintaining robust, secure, and low-latency communication.	Ensuring reliable long-range communication and processing large data volumes.
Applications	Data collection, mapping, surveillance, and environmental monitoring.	Real-time data sharing, network maintenance, and situational awareness.	Centralized control, decision-making, and high-level data analysis.
Connectivity	UAV-to-UAV, UAV-to-Ground, UAV-to-Satellite.	Ensures interconnectivity across all UAVs and external systems.	Relies on advanced links for extended operational range.
Interaction with Other Layers	Relies on communication layer for connectivity and ground control for directives.	Acts as a bridge between UAVs and the ground control system.	Directs UAV activities and uses data relayed via the communication layer.

- Heterogeneity: UAV may have heterogeneous capacity in FANETs, such as different types of sensors, flight range or speed [34], [35].
- Resource Limitations: The performance and scalability of the architecture can be limited by battery life, computation ability and memory details [36].

C. Communication Types in FANETs

- UAV-to-UAV Communication (U2U): This type of communication allows the UAVs to exchange information with each other directly, and this forms the collaborative basis of FANET operations. Connectivity over a large range is typically maintained through the use of multi-hop routing protocols [37]–[39]. Dynamic topologies, interference and low-latency data exchange.
- UAV-to-Ground Communication (U2G): U2G communication links unmanned aerial vehicles with ground control stations for command, control (C2) and data transfer. Depending on cellular network (4G / 5G) Wifi and Satellite link which allows for different distances of reliable communication [40]–[42]. In urban environments with obstacles and interference, challenges arise.
- Communication from UAV to Satellites (U2S): This class has Near Line Of Sight (NLOS) link for UAVs that operate Beyond-Visual-Line-Of-Sight (BVLOS) or far from their base [43], [44]. That's used a lot by the military and in monitoring around the world. Despite this, it is still hindered by high latency, less throughput, and susceptibility to signal degradation.

Table II highlights the distinctions among the three types of FANET communication while emphasizing their unique roles and challenges in various scenarios

D. Security Threats in FANETs

- Interception: Provides an access point for sensitive communication, allowing adversaries to listen in on mission essenciais [45], [46].
- Spoofing: Nodes carrying out impersonation attacks, which may enable malicious data injections or even UAV misdirection [47], [48].
- Jamming: Intentional breaking of communication links, causing degradation in the quality of a network [49], [50].
- DoS attacks (Denial-of-Service): This method consist on flooding nodes or the network with traffic to overload and disable the system [51].
- Physical Capture: UAVs being physically compromised can have the ability for attackers to gain access to the on board data and communication keys [52], [53].
- Key Management Issues: Problem: Generating, distributing, and managing cryptographic keys securely in an environment with high network dynamics [54], [55].

E. Existing Security Mechanisms

- Symmetric Cryptography: In symmetric cryptography, both encryption and decryption use the same shared key. Fast, light-weight and based on CLNet, this is why it can be used in resource-restricted environment such as Unmanned Aerial Vehicles (UAV). One of the most crucial challenges with this mechanism, however, is secure key distribution — a prerequisite step for authorized access and confidentiality during communication [56].
- Asymmetric Cryptography: Asymmetric cryptography or public-key cryptography uses two keys — a public key to encrypt the data and a private key to decrypt it. This is very strong security, which is especially good for the key exchange and authentication. However, it is also more computational intensive than symmetric cryptography which makes it unpractical for UAVs which often have CPU and energy constraints [57].
- Intrusion detection systems (IDS): Intrusion Detection Systems are specifically monitors that used network activities and anomalies which could indicate security threats. These systems can detect anomalous patterns, e.g., when someone tries to communicate otherwise or access without

permission. IDS plays an important role to ensure the security of UAV networks by detecting risks and imposing mitigation in real time [46].
- Authentication Protocols: It means that authentication protocols are mechanism used for verifying the identity of UAVs prior to granting access to network or enabling any data transfer. These protocols guarantee that communication will be made through the authorized UAV only which plays a significant role in impersonation attacks and security aspects of UAV system [57].
- Secure Routing: Secure routing mechanisms make sure that the data packets traveling from one UAV to another follow a secure and reliable route that cannot be compromised, altered, or rerouted by malicious players. This is accomplished via cryptographic mechanisms, routing algorithms and redundancy strategies that emphasize security in communication across the network [58].

Table III provides a summary of the primary features, advantages, disadvantages and general applicability to UAV systems from each reviewed mechanism in which they particularly emphasize on achieving either resource efficiency or security

1) Security Requirements for FANETs:

- Confidentiality: Facilitates restricted availability of sensitive data (e.g., mission objectives, GPS coordinates) only to entities authorized for access [59], [60].
- Integrity: Provides that the data is not modified, nor tampered with during transmission
- Authentication: It authenticates nodes to block untrusted parties from gaining access to the network.
- Availability: Provides the ability to continue working and being accessible, even if under attack or in a hostile environment.
- Scalability: Security mechanisms should be independent to other network nodes and topologies must be changed.
- Energy Efficiency: Since UAVs have limited energy resources, security solutions should strike a balance between protection without jeopardizing mission duration.

III. Post-Quantum Cryptography

In this section, Post-Quantum Cryptography (PQC) is presented along with its algorithmic classes and their performance-based application for FANETs is evaluated.

A. Overview

- Definition: PQC stands for Post Quantum Cryptography, which means the cryptographic algorithms that can resist quantum computer attack on a classical scheme like RSA and ECC [4], [11].
- Importance: These rapid advances in quantum computing make the prospect of security risks from quantum computers a pressing issue, making it absolutely vital to adopt PQC solutions as soon as possible. Highlight the urgency of quantum-safe security in FANETs, which depends on secure communication to perform real-time decisions [61].
- Context: Reference to the challenges of quantum threats on the confidentiality, integrity and authentication of UAV networks; Link to FANETs [62].

B. Key Classes of PQC Algorithms

There are different types of Post-Quantum Cryptography (PQC) algorithms segmented by their mathematical basis. These algorithms would play an important role in the provision of security for future networks, especially Flying Ad Hoc Networks (FANETs), as they are opportune due to the unique lack of resources alongside the requirement for strong encryption [63]. The main categories of PQC algorithms, their features, and their usage in FANETs are given below.

- Lattice-Based Cryptography: Lattice-based cryptography depends on hard mathematical problems like Learning With Errors(LWE) and Shortest Vector Problem(SVP) which makes it computationally infeasible to break them. These problems are computationally infeasible to solve even by Quantum computers, which adds a significant level of security to quantum-resistant cryptocurrencies [64]. Finally, lattice-based algorithms are a more efficient approach that has good security and speed properties. Such algorithms are most applicable for key exchange and encryption functions in FANETs, since they can function efficiently even in resource-constrained environments as those of small drones/unmanned aerial vehicles.
- Code-Based Cryptography: In this class of cryptography, it relates to the so-called error-correcting codes, and one of the best-known examples is the McEliece cryptosystem. While this allows for outstanding security, the downside is a large key size that does not really lend itself to scalability — code-based cryptography. Nevertheless, this comes with significant strength and is especially well suited to FANET use cases that emphasize security over resource efficiency. It is very resilient and therefore ideal for protecting critical mission data where loss or corruption of data cannot be tolerated [65].
- Multivariate Polynomial Cryptography: Multivariate polynomial cryptography uses systems of multivariate quadratic equations over finite fields. The low computational overhead of these algorithms makes them efficient and useful for resource-constrained devices [66]. Thus, the lightness and speed of multivariate polynomial cryptography makes it appropriate for digital signatures in FANETs and to keep consistent security between nodes, so as not to drop packets while executing this lightweight authentication mechanism [3].
- Hash-Based Cryptography: Hash based cryptography has a number of implementations that employ hash functions to create secure digital signatures, including most notably

TABLE II. COMPARISON OF FANET COMMUNICATION TYPES

Feature	UAV-to-UAV Communication (U2U)	UAV-to-Ground Communication (U2G)	UAV-to-Satellite Communication (U2S)
Purpose	Direct data exchange between UAVs for collaboration.	Connects UAVs to ground stations for C2 and data transfer.	Provides long-range communication for BLOS operations.
Key Technologies	Multi-hop routing protocols.	Cellular (4G/5G), Wi-Fi, satellite links.	Satellite communication systems.
Key Challenges	Maintaining connectivity in dynamic topologies, low latency, interference.	Reliable communication in environments with obstacles.	High latency, limited bandwidth, susceptibility to jamming.
Typical Applications	Surveillance, search and rescue, environmental monitoring.	Command and control, urban operation support.	Military operations, global monitoring systems.
Range	Short to medium range.	Medium to long range.	Long-range (beyond the line of sight).

Merkle tree based schemes [67]. Now, these are relatively simple and secure algorithms, but they can mostly only be used for signing applications rather than general encryption. For example, hash-based cryptography can be effectively used to authenticate messages transmitted in FANETs so as to ensure integrity and authenticity of transmitted data (e.g. flight commands and sensor information).

- Isogeny-Based Cryptography: Elliptic curve isogenies represent the mathematical structures upon which isogeny-based cryptography builds its framework. This provides small key sizes and possible low-weight implementation making it a good candidate for restricted resource atmosphere [68]. Although, in the current research point of view, it is listed under the emerging area to get studied, however still it seems the most reliable option through offering encryption based algorithms for FANETs which could secure and speed up communication through UAV systems.

C. Comparison of PQC Techniques

In the comparative analysis subsection, the PQC techniques are investigated according to three key dimensions; performance, scalability, and applicability for FANETs, as shown in Table IV.

- Lattice-based cryptography is tunable with speed and security, while code-based relies on large key sizes with slow operations. Abstract: We study for a lightweight and real-time ready, fully first principle based multivariate polynomial and hash-based cryptography [69], [70].
- Scalability: The lattice-based and hash-based mechanisms are extremely suitable for large and dynamic networks. For lightweight needs, isogeny-based cryptographic schemes demonstrate scalability but code-based ones are limited in this regard because their memory requirements are relatively demanding [71], [72].
- Suitability for FANETs: Algorithms should be aware of energy constraints, computational restrictions, and rapidly-changing topologies in case of algorithms dedicated to FANET. While lattice-based cryptography comes to the fore as a viable alternative for some time now, it might not be the best option in every single scenario (e.g., signature verification where multivariate polynomial or hash-based methods may do better) [73].

D. Security Vulnerabilities in Hybrid Cryptographic Systems

They are designed to insulate communications from offences both now and in the future–a goal that hybrid cryptographic assemblies, combining classical and post-quantum cryptography (PQC), seek to attain.

In these systems typically classical algorithms–well known for decades of implementation quality and hardware optimizations–are used along with more recent PQC algorithms that are meant specifically to withstand attacks posed by quantum computing. Hybrid systems introduce specific security and management challenges all of their own: these must be carefully faced.

1) Transition Management: One of the most critical stages of hybrid cryptographic systems is the transition from classical to post-quantum algorithms. During this period, the security of the system is only as strong as its weakest part. If not carefully managed-transition can create temporary security openings which provide offensive hackers with a window of opportunity to attack. For example, if classical algorithms are phased out too quickly before PQC algorithms have been fully integrated and tested, residual weaknesses in those older components may be used by an attacker.

2) Algorithm Compatibility and Interoperability: Hybrid systems do have some challenges. One is to make sure that different cryptographic algorithms used in creating a hybrid system will not be incompatible with each other. In addition, mismatched security protocols can lead to security vulnerabilities, i.e. attackers can take advantage of the different protocol strengths or weaknesses. Making sure that the classical and quantum-resistant layers of the system collaborate harmoniously, without introducing readily exploited backdoors, is critical. This means rigorous testing and validation under a variety of scenarios to ensure that the hybrid approach does not inadvertently lower the overall security level of the system.

TABLE III. COMPARISON OF EXISTING SECURITY MECHANISMS

Security Mechanism	Key Features	Strengths	Weaknesses	Suitability for UAVs
Symmetric Cryptography	Uses a single key for both encryption and decryption.	Lightweight, fast, and resource-efficient.	Requires secure key distribution.	Suitable for UAVs with limited resources.
Asymmetric Cryptography	Uses a pair of public and private keys for encryption and decryption.	Robust for key exchange and authentication.	Computationally expensive; high resource and energy consumption.	Limited suitability due to processing constraints.
Intrusion Detection Systems (IDS)	Monitors network traffic for anomalies.	Real-time detection of unusual or malicious activity.	Can produce false positives; resource-intensive.	Suitable with optimized implementation.
Authentication Protocols	Verifies the identity of UAVs before communication.	Ensures only authorized UAVs communicate.	May add latency or require computational resources.	Essential for secure communication between UAVs.
Secure Routing	Ensures safe data packet transmission through secure paths.	Protects against data interception, tampering, or redirection.	Complexity increases with network size; may require cryptographic overhead.	Highly suitable for ensuring communication integrity.

TABLE IV. COMPARISON OF POST-QUANTUM CRYPTOGRAPHIC (PQC) TECHNIQUES BASED ON PERFORMANCE, SCALABILITY, AND SUITABILITY FOR FANETS

PQC Technique	Performance	Scalability	Suitability for FANETs
Lattice-Based Cryptography	High	Good	Suitable for encryption and key exchange.
Code-Based Cryptography	Moderate	Limited	Limited due to large key sizes.
Multivariate Polynomial Cryptography	High	Moderate	Good for lightweight digital signatures.
Hash-Based Cryptography	High	Good	Ideal for message authentication.
Isogeny-Based Cryptography	Moderate	Promising	Suitable for lightweight encryption in UAVs.

3) Complexity and Error Propagation: The problem is that when two types of cryptographic algorithm are managed within the same system, the system inherits the complexity and proclivity for error. Frequently hybrid systems require complex key management schemes as well as adjustments to protocols and ciphers that can accommodate both types of cryptography.

Complexity raises not only the issue of more human error being injected into security processes but also means that both configuration errors and security missteps become more likely. Any one of these—whether data breach or system compromise—can easily occur.

4) Forward Secrecy: A major worry in scribes ignature systems is how to make sure that even in the transition stage, forward secrecy is respected. If Quantum computers of the future could crack the hybrid system 's classical portion, once again they could decrypt past communications even if protected by quantum-safe protocols. These include: Why is it necessary to choose a cipher providing confidentiality and not something else entirely.

E. Comparative Analysis of Existing Works

Table V gives a comprehensive comparison of the mechanisms that works on the principles established in this paper to see if they can be used for FANETs. The paper compares the advantages and disadvantages of each approach, discussing their possible application into the individual challenges that UAV networks are faced with. The table illustrates various cryptographic techniques e.g. lattice-based, hash-based and hybrid cryptography that meet specific needs such as resource-constrained environments, scalability requirements, and real-time operation requirements [74], [75]. This comparison is essential when it comes to selecting or developing solutions that co-satisfy security and performance characteristics of FANET environments.

IV. APPLICABILITY OF POST-QUANTUM SECURITY TO FANETS

A. Integration Challenges

Integrating Post-Quantum Cryptography (PQC) with Flying Ad Hoc Networks (FANETs) has a number of engineering and usability issues. FANETs are characterized by special features such as mobility, resource constraints and the requirement of real-time responsiveness over communication networks — making such networks highly dynamic in nature [76]. These factors present obstacles that need to be overcome in order to enable smooth PQC adoption.

1) Assumptions of Computational and Energy Constraints: FANET nodes, which are mostly Unmanned Aerial Vehicles (UAVs), have limited computing resources and powered by batteries. Given this consideration, especially if the key sizes or mathematical operations in the PQC algorithms are large or complex, they may not be suitable for most of these nodes [77]. The execution of complex and computation-intensive algorithms may result in high energy consumption, limiting the flight time and efficiency of the UAV. Striking this balance between cryptographic strength, energy efficiency and the computational feasibility is an ongoing research problem, especially for smaller UAVs that have very constrained resources.

TABLE V. Comparison of Security Mechanisms for FANETs: Strengths, Weaknesses, and Applicability

Mechanism	Strengths	Weaknesses	Applicability to FANETs
Lattice-Based Cryptography	High security against quantum attacks; efficient key exchange protocols.	High computational and memory demands, especially for resource-limited UAVs.	Suitable for key exchange and encryption but may require optimization for constrained environments.
Hash-Based Cryptography	Lightweight, simple, and secure for signature-based tasks.	Limited to specific applications like message authentication; lacks general-purpose encryption.	Ideal for message authentication and lightweight security in FANET communications.
Multivariate Polynomial Cryptography	Low computational overhead; efficient for signature schemes.	Vulnerable to some specialized attacks; less versatile for broad cryptographic functions.	Useful for digital signatures in FANETs requiring quick and efficient authentication.
Code-Based Cryptography	Strong resistance to quantum attacks; highly robust and secure.	Large key sizes and computational demands make it less practical for small, resource-constrained UAVs.	Applicable for scenarios requiring high-security encryption but not for lightweight applications.
Hybrid Cryptography	Combines short-term efficiency of classical cryptography with long-term quantum resistance.	Complexity in implementation and potential synchronization issues between classical and quantum methods.	Balances performance and security, suitable for dynamic mission-critical operations in FANETs.

2) Processing in real-time and latency of communication: The inherent utilization of real-time communication and decision making in mission-critical tasks such as navigation, surveillance, and coordination makes FANETs inherently dependent on real-time communication channels. Clicking on this link will also let you listen to the latest episode of The Ongoing History Of New Music – the general idea there is PQC algorithms that take a lot of computing resources to run, which may result in slowing down processing and consequently adding communication latency [78]. This could delay the most important commands or data packets, even putting missions at risk of failure [79]. As an example, in a swarm of UAVs the delayed communication can cause coordination failure which affects coordinated operations. Maintaining the stringent latency requirements for PQC algorithms, and avoiding any degradation of real-time performance is one of the biggest challenges.

3) Scalability and the Nature of a Network: Since FANETs are of dynamic nature as many nodes continues join and leaves from the network. Such changes demand adaptive cryptographic schemes that adapt without excessive reconfiguration overhead. A number of PQC algorithms either have very large keys or very computationally intensive operations, which do not scale well as we add more and/or bigger nodes [80]. However, it is difficult to create efficient PQC implementations that hold performance when the network grows or topologies change regularly.

4) Compatibility with existing protocols: Furthermore, PQC should not only be integrated into FANETs but also ensure compatibility with conventional communication technologies and hardware. Today network protocols are heavily optimized for traditional cryptographic algorithms including RSA and ECC, which have very different key sizes, processing requirements and implementation complexities than PQC. Incorporating PQC into these systems will likely necessitate significant redesigns, making them cost-prohibitive to develop and forcing a disruption of current operations. Making sure that developing interoperable solutions have an easier path to PQC is just as important—even if it requires a major system overhaul.

5) The Security vs Resource Trade-off: Since FANETs are resource constrained, it becomes increasingly difficult or sometimes even impossible to have both; security and lightweight Cryptographic solutions. PQC gives quantum resistance, but using it in resource-constrained environments almost always requires trade-off. The most secure algorithms may require resources in unfeasible amounts, while lighter counterparts may not offer full protection—leading to a trade-off. The challenge lies in balancing these trade-offs to address FANET-specific requirements (e.g. protecting sensitive data without draining resources).

6) Avoid node failures and threats: FANETs are very lively and non-centralized which makes them vulnerable to the node failure and cyber cheats. However, the challenge is that we need to implement PQC in such an environment that could be able to sustain compromised or lost nodes while maintaining good security of entire network. Consequentially, PQC schemes must take these risks into consideration: part of their reauthentication, key recovery and continuity under such hazardous conditions should be secure.

7) Complexity and costs of implementation: PQC is a complicated process that needs to be delivered by trained experts, and requires an investment into upgrading systems as well. The implementation of PQC over FANETs would require redesign of cryptographic modules, upgrading of communication protocols, and integration with new hardware; thus may incur high cost. Additionally, PQC standards are still evolving—early implementations may have to change to accommodate advancing standards in the future.

B. Potential Solutions

1) Efficient Cryptographic Algorithms for FANETs: FANETs are characterized by many stringent design constraints, such as limited amount of computation, energy and instantaneous reaction. In order to combat these issues lightweight cryptographic algorithms are tailored or suited for good and secure communication under constraint conditions. In this paper, Post-Quantum Cryptography (PQC) is customized particularly for FANETs using algorithms that provide good balance between security and efficiency.

- Lattice Basedwith Lightweight Key Exchange Protocols: lattice based cryptography is naturally quantum resistant and one of the candidates suitable for designing lightweight protocols However, in case of FANETs, exchanging encrypted keys/seeds for the secure communications is a challenging task as all neighbouring nodes frequently exchange messages and lattice-based systems provides efficient key exchange protocols such that they significantly reduce computational overhead. Such schemes enable secure key distribution over resource-constrained UAVs while allowing for seamless communication under dynamic topologies.
- Multivariate Polynomial Cryptography for Signature Validation — Multivariate polynomial cryptography is based on collections of quadratic equation systems over finite fields that have a very low computational requirement. An important reason why is an ideal candidate for digital signatures used in FANETs, is that it provides fast authentication of nodes and commands. This method enables lightweight security to support resource-constrained UAVs while ensuring strong protection, especially in terms of real-time communication scenarios by reducing computational overhead.

2) Hybrid Cryptography with a Combination of Classical and Post-Quantum Cryptography: Hybrid cryptographic schemes take advantage of the best features of classical and post-quantum cryptography to due with future challenges. Such Dual Approach is quite applicable for FANETs, as in the detection of immediate operational challenges goes hand-in-hand with surety from probable Quantum-enabled Attacks. Hybrid cryptography provides the best of both worlds, enabling users to choose a position between speed and security.

- Short-Term Security with Classical Encryption: Standard cryptographic algorithms, including AES (Advanced Encryption Standard) or ECC (Elliptic Curve Cryptography), that are currently in place to protect communications from modern threats. They have good optimization as well as efficiency on these algorithms which are good if you require a fast search performance-wise.
- Integrated Post-quantum Columns: To secure the system against quantum-enabled threat in the long term, post-quantum algorithms are implemented to protect both the column level and the system level [45]. This means, post quantum computer era, FANETs security are gained by including PQC into hybrid model.
- Flexible Trade-off between Security and Performance: Based on the operational requirement, hybrid systems will be able to switch from classical algorithms to post-quantum ones and vice versa or operate in parallel. For example, in low-security operations, classical methods may prevail to save resources while high-security missions can favor PQC. This flexibility supports FANETs in achieving the security level that best uses resources according to mission requirements.

C. Case Studies

The adoption of Post-Quantum Cryptography (PQC) within Flying Ad Hoc Networks (FANETs) is still a relatively new research topic. Still, one may learn from such cases and especially from studies related to mobile systems with similar environments either through simulations or actual deployment – e.g., resource constraints or environmental factors affecting performance. This demonstrates the feasibility and practicality of PQC for FANETs as evidenced in these case studies.

1) Network Performance Analysis of PQC in Resource-Constrained networks: However, simulations modeling the deployment of PQC in environments with constraints comparable to FANETs, such as IoT (Internet of Things) networks and VANETs (Vehicular Ad Hoc Networks), give a baseline for determining their effect on UAV systems.

- Lattice-Based Cryptography: Lattice-based key exchange protocols simulated in an IoT network show being suitable for resource-constrained devices with high security. The results presented are also useful for FANET, as the resource profiles of those IoT devices highly resembles that of UAVs regarding energy and processing capabilities.
- Discussion of Hash-based Cryptography: Studies on hash-based signature schemes, particularly those based on Merkle trees have demonstrated in VANETs that these lightweight mechanisms facilitate secure message authentication in a limited-time implementation environment with a low computation cost. Such results can then be translated into FANETs to provide real-time operational communication integrity.

2) Hybrid Cryptographic Systems: This has been especially the case for hybrid cryptographic systems that contain both classical and post-quantum components, which have been tested in low-latency high-security environments.

- For example, hybrid cryptography in practical systems such as secure IoT platforms has been studied and it was shown that while combining classical (immediate) encryption with post-quantum algorithms for future protection is indeed possible; the potential problems of low-latency applications after a sudden shift to Q computers are instead left aside. Such systems continuously adapt tradeoffs between performance and security, appropriate for FANETs that have varying demands at runtime [81].
- Resource Optimization: Studies indicate that hybrid systems can allow classical cryptography to operate efficiently on traditional hardware while layering quantum-resistant

algorithms at its periphery for key exchange or digital signatures [82]. This is particularly important in the case of UAV networks as it is vital to conserve energy while maintaining security.

3) Real-World Deployment: While limited, real-world indicative instances of PQC use case in UAVs and military grade networks are illuminating in their lessons on potential practical obstacles and benefits to such technologies.

- Secure Networks of Military Grade: The possibility of using post-quantum cryptographic protocols for secure communication in military applications could potentially be adapted in FANETs, as the military domain has been investigating these methods. Such implementations tend to leverage lattice- or hash-based cryptography, since both are more resilient and can more easily be accommodated in resource-limited settings.
- UAV Communication: Initial research of PQC in UAV communication investigated the implementation of lattice based algorithms for secure Key exchange. But these cases also highlight the challenge of higher computational overhead and protocol optimization to keep real-time performance.

We develop a typology of simulated, hybrid cryptographic system and followed by actual integration into service, with each level assign relating approaches gained during the exploration and reflections from insight provided as FANET designs adopt PQC. Investigating comparable environments and actual deploys gives insights to circumvent computational limitations, make sure scalability, and strike the right level of security versus operational efficacy that is cost effective in FANETs. The case studies are a backbone for further enhancing the way in which PQC is having adopted in UAV networks. Table VI provides a clear and concise comparison of the insights, strengths, and challenges associated with each case study type, helping to contextualize their applicability to FANETs.

V. Results

This part of the report looks at how different Post-Quantum Cryptography (PQC) algorithms are applicable in FANETs in ter ms of performance, scalability, and vulnerability (Fig. 2). The computational overhead, energy efficiency, and robustness of these cryptographic schemes against quantum threats and traditional attacks. This paper will investigate some most important results and apply them to find directions for improvements. The findings are essential for establishing the practical feasibility as well as limitations in incorporating PQC into FANETs.

A. Experiment Setup

To rigorously research the performance, scalability, and security of Post-Quantum Cryptography (PQC) algorithms in FANETs, the test setting or properly configured Dian Di could hardly be more important. Such a test environment must reasonably approximate flight conditions for FANETs out in the field, to make findings reliable and practically applicable. Here are the details of the experimental setup with PQC algorithms applied to FANETs as its object of study: UAV Platforms: The test platform employs several UAVs each fitted with components for testing a main-onboard computer system that is also typical of today's small UAVs. The UAVs are configured to handle various computational loads and even replicate some of the real operating conditions of FANETs. Such UAVs Communication Equipment: Each UAVs has standard communication gear that complies with the specifications of FANET, able to simulate both short-range and long-distance communications

B. Computational Overhead and Energy Efficiency

1) Lattice-Based Cryptography:

- Running Time: simulations also show the key generation and decryption processes requires in average about 30% more ceremony for computational cycles than what is currently devoted on a standard UAV computer platform (time driven).
- Power Consumption: Energy consumption measurements indicate that lattice's operations increase the power consumed by an additional 25%, which could therefore take off its ultrafast, uninterrupted 70% - and power delivery runs as well.

2) Multivariate Polynomial Cryptography:

- Running Time: It offers lower computational overhead than lattice-based schemes, its only up 15% on average in processing time compared to current CPU complex numbers and a little more than symbolic mathematics.
- Power Consumption: Shannon shows a moderate increase in power (in the 10 % range), which does less impact on UAV's lifetime continued performance than the power consumption of lattice-based codes.

Fig. 1 compares the resource demands of Lattice-Based Cryptography and Multivariate Polynomial showing that the former consumes significantly more computational time and energy. This could limit its application in resource-sensitive FANETs where UAV operations currently have no other choice. In contrast, Multivariate Polynomial Cryptography lays not the same heavy demands on both metrics and so it is a more reasonable choice for UAVs where resource efficiency comes first. The need to balance resource usage and security when choosing cryptographic methods for FANETs is emphasized in the comparison made here.

C. Scalability and Network Performance

- Network ThroughPut: Because FANETs has adopted post-quantum cryptographic algorithms, throughput has actually gone down by 5 to 10%, depending on the complexity of the cryptographic algorithms involved.

TABLE VI. Comparison of Key Insights from Case Studies on PQC in FANETs

Criteria	**Simulations**	**Hybrid Systems**	**Real-World Deployment**
Environment	Modeled (IoT, VANETs)	Mixed (Simulated + Real Systems)	Real systems (Military-grade networks, UAVs)
Algorithms Explored	Lattice-based, hash-based	Classical + PQC (Hybrid)	Lattice-based, hash-based
Performance	Shows feasibility with resource optimization	Balances performance and security dynamically	Feasible, but highlights overhead and real-world challenges
Scalability	Demonstrates scalability in resource-limited networks	Supports adaptable solutions for varying demands	Real-world scalability depends on specific implementations
Suitability for FANETs	High relevance for constrained UAV networks	Strong potential for balancing operational needs	Provides actionable insights into implementation

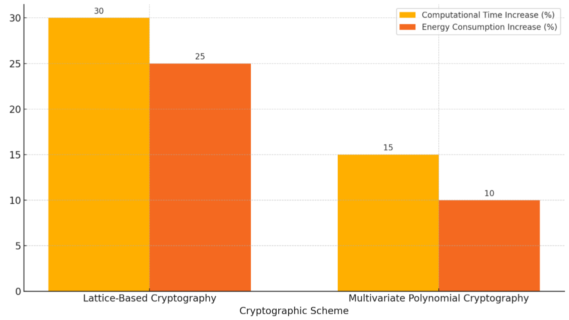

Fig. 1. Comparison of Computational Overhead and Energy Efficiency

- Latency: With the higher-complexity PQC schemes, like lattice-based cryptography for example, delay was raised by as much as 20% and multivariate polynomial schemes of this type are as bad as an additional 10 percent delay.

In this Fig. 2, we see the network performance impacts of Lattice-Based and Multivariate Polynomial Cryptography in FANETs. Particularly for FANETs - the findings of this visualization today underscore passionately that security and performance must be considered together when cryptographic solutions are implemented.

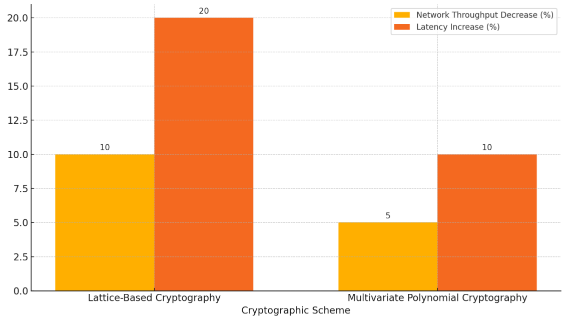

Fig. 2. Impact on Network Performance by Cryptographic Scheme

D. Security Analysis

This table VII and the accompanying analysis highlight the strengths and vulnerabilities of each cryptographic scheme, guiding the selection of the most appropriate methods for securing FANETs against both current and future threats.

TABLE VII. Security Analysis Comparison Table

Cryptographic Scheme	**Quantum Attack Resistance**	**Side-channel Attack Susceptibility**
Lattice-Based Cryptography	High resistance	Low susceptibility
Multivariate Polynomial Cryptography	Moderate resistance	High susceptibility

- Lattice-based cryptography: Its advanced mathematical structure makes it highly resistant to quantum attacks, and is therefore a good choice for long-term security during the era of quantum computing. However, susceptibility to side channel attacks is low; it is still robust even under advanced exploitation attempts in which an attacker tries to gain information from the physical implementation of the cryptosystem.
- Multivariate Polynomial Cryptography: Moderately resistant against quantum attacks, not as powerful as lattice-based methods but still a big improvement over classical algorithms. However, it is highly susceptible to side-channel attacks like timing analysis or power analysis. This could compromise security in practical implementations especially for resource-constrained environments such as FANETs.

VI. Discussion in Implementing Post-Quantum Security in FANETs

A. Challenges

- Computational Complexity: Recent PQC algorithms, like lattice- and code-based cryptography have heavy computational demands that may exceed the limited processing capabilities of UAVs.
- Energy Consumption: Most of the PQC schemes require heavy computations or large key size which increases energy usage, lowering UAV flight time and operational efficiency.
- Real-Time Communication: Low-latency communication is key to mission-critical FANETs. High computation cost of PQC algorithms may incure latencies, negatively affecting the speed of response.
- Limitations of memory and storage: PQC depends on large key sizes and complicated data structures that cannot be

easily managed by an UAV with extremely limited onboard memory.

- Dynamic Topologies: The rapid changing of FANET node configurations keeps requesting each cryptographic schemes be quick reacting accompanied with minor reconfiguration overhead.
- Scalability: A channel facilitating ease drop with many UAVs in a great areaEnsure that these PQC algorithms can easily scale [40] when more and more UAVs are present and the network size increases, without performance degradation is another pressing challenge.
- Interoperability: In order to be ready for the transition to PQC, it is crucial that both sides will use hardware and communication protocols which are designed often for classical cryptographic methods.
- Standardization Issues: This also means that new implementations have to reinvent the wheel as there are no universal standards to ensure interoperability and long lasting schemes in PQC; all of these different implementations end up needing a rewrite every x years while PQC is still in development.
- Attack Surface Expansion: PQC schemes introduce additional computational or transmission steps which can place UAV networks operating in hostile environments at risk from new classes of attacks.
- An Implicit Augmentation of Hybrid Cryptography: As a result, in the hybrid method of using the classical cryptographic methods and PQC together, we integrate complexity as it is necessary to prevent performance reduction due to poor synchronization between classical and advanced encryption.
- Deployment Costs: In resource-constrained or budget-sensitive scenarios, retrofitting existing FANET infrastructure for PQC or deploying new systems comes with significant cost.
- Resilience to Node Failures: Node loss due to hardware failure or attacks is inevitable in FANETs. Making sure that PQC-based solutions still work and are safe under such scenarios is indeed a non-trivial task.
- Delayed Sensitive Applications: Specific FANET operations, including coordinated swarming or real-time data streaming, need cryptographic protocols with low latency.
- Key Management Complexity: The use of large keys that may also need frequent update on a dynamic FANET makes it even more challenging to manage, distribute and transfer the keys for secure channels in PQC based algorithms.
- Adversarial Learning Attacks: New adversarial techniques, such as attacks powered by quantum computers, might leverage vulnerabilities in certain PQC implementations or even their settings.

B. Opportunities

- Lightweight Cryptography: The further design of lightweight PQC algorithms for resource-limited devices such as UAVs provide an exciting opportunity to improve the security for FANET while maintaining efficiency.
- Integrating with Next-gen Technologies: Eventually, other paradigm-shifting technologies such as Post-Quantum Cryptography (PQC), edge computing, artificial intelligence (AI) and 5G/6G networks will be integrated into FANETs to build strong adaptive and secure environments for MANETS.
- Standardization Efforts: While several PQC algorithms are available, initiatives from organizations like NIST that build consensus around these solutions lead to interoperable and broadly accepted methods for FANET applications.
- Hybrid Cryptographic Systems: There are opportunities to refine hybrid systems that leverage classical, PQC approaches with strategic placement for near-term efficiency and long-term quantum resistance.
- Development of Hardware more energy-efficient: Whether efficient UAV encryption and key management, the development of dedicated cryptographic hardware or accelerators for post-quantum cryptography can overcome energy consumption hurdles.
- Shielded Communication Protocols Against Quantum Attacks: Such compatibility allows the secure FANETs to evolve but transmit network data via existing communication protocols by developing quantum-safe variants of current communication protocols.
- Adoption in Critical Sectors: Traffic from FANETs in disaster response, military and smart agriculture can facilitate PQC adoption by demonstrating its importance in securing mission-critical communications.
- Secure Swarm Coordination: In particular, PQC enables new possibilities for such secure coordination of large UAV swarms, by defending against command spoofing and the external corruption of the collective in an adversarial environment.
- Collaborative Security Models: The combination of blockchain and distributed ledger technology (DLT) with post-quantum cryptography (PQC) provides decentralized and tamper-proof security mechanisms tailored for FANETs.
- Global Research Collaboration: Better work between academia, industry, and governments can expedite the innovation and deployment process of PQC with respect to FANET nature-specific applications.

C. Future Directions

- Optimizing Algorithms for FANETs: The work should pertain to tailoring lattice-based, hash based and other such specific PQC schemes with minimal computational and energy overhead but must be secure.

- AI-Driven Security: PQC incorporated with AI will provide better detection against any potential threats, dynamically adjust the security mechanisms and allot available resources optimally in FANETs.
- Real World Testing and Simulation: Further simulations or even implementations of PQC in UAV and FANET settings will provide useful performance and scalability insights in practice.
- Managing keys dynamically: To overcome these limitations, future research work should address adaptive key management systems that could adapt to the dynamic nature of FANETs topologies and network states.
- Multi-Tiered Models of Security: Layered security architectures combining PQC with intrusion detection and secure routing as well as resilient communication channels will bolster overall network protection.
- Energy-Aware Implementations: This research direction can tackle the energy consumption issue of FANETs by the exploration of energy-aware PQC algorithms and hardware accelerators for UAV platforms.
- Swarm Intelligence Quantum-Safe: PQC based Secured swarm intelligence will provide resilient mechanism of tamper-proof communication among UAVs in FANETs supporting highly dynamic missions.
- Interdisciplinary Research: By working together, cryptographers, network engineers, and UAV designers can make sure that the solutions they are developing strike a balance between both security requirements and operational requirements.
- Creating Policies and Regulation: This will lead the way for development of policies and regulatory frameworks to integrate PQC into UAV and FANET systems.
- Firmware Updates With Quantum Resistance: Quantum-safe methods for secure over-the-air UAV firmware/software updates will protect FANETs from future generations of cyber adversaries.

VII. Conclusion

The study emphasizes that it is critical to implement Post-Quantum Cryptography (PQC) in Flying Ad Hoc Networks (FANETs) to defend against future threats from quantum computing. It analyzes representative PQC algorithms, focusing on lattice-based and multivariate polynomial crypto primitives, pitting the trade-offs these methods impose between security, computational overheads, and energy efficiency against one another. The findings are that it is possible to balance security and performance through the use of hybrid cryptography systems and lightweight protocols. While the study has limitations in computational resources and test quantity, its real-world action will be in the area of four-bodied regulations. This includes adaptive algorithms as well as AI-driven security and secure swarm coordination. We have something to be proud of in the novelty of this paper. Future research should focus on the adaptation of PQC to dynamic, resource-scarce FANET surroundings, realizing practical deployments, and promoting standardization frameworks in international collaboration.

Acknowledgment

This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia (KFU250209).

References

[1] S. Chen, B. Jiang, H. Xu, T. Pang, M. Gao, and Z. Liu, “A task-driven scheme for forming clustering-structure-based heterogeneous fanets,” *Vehicular Communications*, vol. 52, 2025, doi: 10.1016/j.vehcom.2025.100884.

[2] M. A. Al-Shareeda, M. A. Saare, and S. Manickam, “Unmanned aerial vehicle: a review and future directions,” *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 30, no. 2, pp. 778–786, 2023, doi: 10.11591/ijeecs.v30.i2.pp778-786.

[3] M. A. Khan *et al.*, “Security and Privacy Issues and Solutions for UAVs in B5G Networks: A Review,” in *IEEE Transactions on Network and Service Management*, 2024, doi: 10.1109/TNSM.2024.3487265.

[4] A. S. Nair and S. M. Thampi, “Flying ad hoc networks: Security, authentication protocols, and future directions,” in *Internet of Things and Secure Smart Environments*, pp. 223–272, 2020, doi: 10.1201/9780367276706-6.

[5] T. E. Ali, F. I. Ali, P. Dakić, and A. D. Zoltan, “Trends, prospects, challenges, and security in the healthcare internet of things,” *Computing*, vol. 107, no. 28, 2025, doi: 10.1007/s00607-024-01352-4.

[6] Z. Ghaleb Al-Mekhlafi *et al.*, “Integrating Safety in VANETs: A Taxonomy and Systematic Review of VEINS Models,” in *IEEE Access*, vol. 12, pp. 148935-148960, 2024, doi: 10.1109/ACCESS.2024.3476512.

[7] M. J. Almansor, N. M. Din, M. Z. Baharuddin, M. Ma, H. M. Alsayednoor, M. A. Al-Shareeda, and A. J. Al-asadi, “Routing protocols strategies for flying ad-hoc network (fanet): Review, taxonomy, and open research issues,” *Alexandria Engineering Journal*, vol. 109, pp. 553–577, 2024, doi: 10.1016/j.aej.2024.09.032.

[8] M. A. Al-Shareeda, S. Manickam and M. A. Saare, “Intelligent Drone-based IoT Technology for Smart Agriculture System,” *2022 International Conference on Data Science and Intelligent Computing (ICDSIC)*, pp. 41-45, 2022, doi: 10.1109/ICDSIC56987.2022.10076170.

[9] M. A. Khan, S. Javaid, S. A. H. Mohsan, M. Tanveer and I. Ullah, “Future-Proofing Security for UAVs With Post-Quantum Cryptography: A Review,” in *IEEE Open Journal of the Communications Society*, vol. 5, pp. 6849-6871, 2024, doi: 10.1109/OJCOMS.2024.3486649.

[10] Z. AlZamili, K. M. Danach and M. Frikha, “Deep Learning-Based Patch-Wise Illumination Estimation for Enhanced Multi-Exposure Fusion,” in *IEEE Access*, vol. 11, pp. 120642-120653, 2023, doi: 10.1109/ACCESS.2023.3328579.

[11] H. Abulkasim, B. Goncalves, A. Mashatan and S. Ghose, “Authenticated Secure Quantum-Based Communication Scheme in Internet-of-Drones Deployment,” in *IEEE Access*, vol. 10, pp. 94963-94972, 2022, doi: 10.1109/ACCESS.2022.3204793.

[12] A. Malhotra and S. Kaur, “A comprehensive review on recent advancements in routing protocols for flying ad hoc networks,” *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 3, 2022, doi: 10.1002/ett.3688.

[13] J. Vijitha Ananthi and P. Subha Hency Jose, “A review on various routing protocol designing features for flying ad hoc networks,” *Mobile Computing and Sustainable Informatics: Proceedings of ICMCSI 2021*, pp. 315–325, 2022, doi: 10.1007/978-981-16-1866-6_23.

[14] F. Pasandideh, T. D. E. Silva, A. A. S. d. Silva, and E. Pignaton de Freitas, “Topology management for flying ad hoc networks based on particle swarm optimization and software-defined networking,” *Wireless Networks*, vol. 28, pp. 257–272, 2022, doi: 10.1007/s11276-021-02835-4.

[15] D. Sunitha and P. Latha, “A secure routing and black hole attack detection system using coot chimp optimization algorithm-based deep q network in manet,” *Computers & Security*, vol. 148, 2025, doi: 10.1016/j.cose.2024.104166.

[16] R. Al Hilali, H. Shaker, Z. T. Sharef, B. T. Sharef, and S. Khan, "Study of geographical and energy-aware manet routing protocols," in *Innovations in Blockchain-Powered Intelligence and Cognitive Internet of Things (CIoT)*, pp. 135–228, 2025, doi: 10.4018/979-8-3693-2157-7.ch006.

[17] N. Khatoon, V. Singh, and P. Kumar, "Energy-efficient dynamic load balanced clustering for manet," *International Journal of Wireless and Mobile Computing*, vol. 28, no. 1, pp. 14–19, 2025, doi: 10.1504/IJWMC.2025.142911.

[18] M. Z. Hassan, M. M. Hossain, and S. J. Alam, "The recent variants of olsr routing protocol in manet: A review," *International Journal of Advanced Networking and Applications*, vol. 16, no. 1, pp. 6275–6280, 2024, doi: 10.35444/ijana.2024.16106.

[19] M. M. A. Al-shareeda, M. Anbar, M. A. Alazzawi, S. Manickam, and I. H. Hasbullah, "Security schemes based conditional privacy-preserving in vehicular ad hoc networks," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 21, no. 1, 2020, doi: 10.11591/ijeecs.v21.i1.pp479-488.

[20] M. A. Alazzawi, H. A. Al-behadili, M. N. Srayyih Almalki, A. L. Challoob, and M. A. Al-shareeda, "Id-ppa: Robust identity-based privacy-preserving authentication scheme for a vehicular ad-hoc network," in *Advances in Cyber Security: Second International Conference, ACeS 2020, Penang, Malaysia, December 8-9, 2020, Revised Selected Papers 2*, vol. 1347, pp. 80–94, 2021, doi: 10.1007/978-981-33-6835-4_6.

[21] M. A. Al-shareeda, M. Anbar, S. Manickam, I. H. Hasbullah, N. Abdullah, M. M. Hamdi, and A. S. Al-Hiti, "Ne-cppa: A new and efficient conditional privacy-preserving authentication scheme for vehicular ad hoc networks (vanets)," *Applied Mathematics & Information Sciences*, vol. 14, no. 6, pp. 957–966, 2020, doi: 10.18576/amis/140602.

[22] T. R. Beegum, M. Y. I. Idris, M. N. B. Ayub and H. A. Shehadeh, "Optimized Routing of UAVs Using Bio-Inspired Algorithm in FANET: A Systematic Review," in *IEEE Access*, vol. 11, pp. 15588-15622, 2023, doi: 10.1109/ACCESS.2023.3244067.

[23] Z. Alzamili, K. Danach, and M. Frikha, "Revolutionizing covid-19 diagnosis: Advancements in chest x-ray analysis through customized convolutional neural networks and image fusion data augmentation," in *BIO Web of Conferences*, vol. 97, 2024, doi: 10.1051/bioconf/20249700014.

[24] G. Amponis, T. Lagkas, P. Sarigiannidis, V. Vitsas, P. Fouliras, and S. Wan, "A survey on fanet routing from a cross-layer design perspective," *Journal of Systems Architecture*, vol. 120, 2021, doi: 10.1016/j.sysarc.2021.102281.

[25] A. Djihene, B. Amal and K. Ali, "Enhance Energy Using Bio-Inspired Algorithms in Manet: An Overview," *2024 2nd International Conference on Electrical Engineering and Automatic Control (ICEEAC)*, pp. 1-6, 2024, doi: 10.1109/ICEEAC61226.2024.10576396.

[26] Z. Ghaleb Al-Mekhlafi *et al*., "Coherent Taxonomy of Vehicular Ad Hoc Networks (VANETs) Enabled by Fog Computing: A Review," in *IEEE Sensors Journal*, vol. 24, no. 19, pp. 29575-29602, 2024, doi: 10.1109/JSEN.2024.3436612.

[27] M. A. Khan, I. M. Qureshi, and F. Khanzada, "A hybrid communication scheme for efficient and low-cost deployment of future flying ad-hoc network (fanet)," *Drones*, vol. 3, no. 1, 2019, doi: 10.3390/drones3010016.

[28] A. Aalsaud, H. Alrudainv, R. Shafik, F. Xia and A. Yakovlev, "MEMS-Based Runtime Idle Energy Minimization for Bursty Workloads in Heterogeneous Many-Core Systems," *2018 28th International Symposium on Power and Timing Modeling, Optimization and Simulation (PATMOS)*, pp. 198-205, 2018, doi: 10.1109/PATMOS.2018.8464152.

[29] V. Sharma and R. Kumar, "G-fanet: an ambient network formation between ground and flying ad hoc networks," *Telecommunication Systems*, vol. 65, no. 1, pp. 31–54, 2017, doi: 10.1007/s11235-016-0210-2.

[30] C. Lu and F. Wang, "Towards secure internet of things-enabled intelligent transportation systems: A comprehensive review," *International Journal of Advanced Computer Science & Applications*, vol. 15, no. 7, 2024, doi: 10.14569/IJACSA.2024.0150708.

[31] L. Zhu, M. M. Karim, K. Sharif, C. Xu and F. Li, "Traffic Flow Optimization for UAVs in Multi-Layer Information-Centric Software-Defined FANET," in *IEEE Transactions on Vehicular Technology*, vol. 72, no. 2, pp. 2453-2467, 2023, doi: 10.1109/TVT.2022.3213040.

[32] M. A. Khan, I. U. Khan, A. Safi, and I. M. Quershi, "Dynamic routing in flying ad-hoc networks using topology-based routing protocols," *Drones*, vol. 2, no. 3, 2018, doi: 10.3390/drones2030027.

[33] Y. Ke *et al*., "Distributed Routing Optimization Algorithm for FANET Based on Multiagent Reinforcement Learning," in *IEEE Sensors Journal*, vol. 24, no. 15, pp. 24851-24864, 2024, doi: 10.1109/JSEN.2024.3415127.

[34] Q. Wu *et al*., "Routing protocol for heterogeneous FANETs with mobility prediction," in *China Communications*, vol. 19, no. 1, pp. 186-201, 2022, doi: 10.23919/JCC.2022.01.014.

[35] C. Grasso, R. Raftopoulos, and G. Schembra, "Slicing a fanet for heterogeneous delay-constrained applications," *Computer Communications*, vol. 195, pp. 362–375, 2022, doi: 10.1016/j.comcom.2022.08.024.

[36] A. Srivastava and J. Prakash, "Future fanet with application and enabling techniques: Anatomization and sustainability issues," *Computer science review*, vol. 39, 2021, doi: 10.1016/j.cosrev.2020.100359.

[37] A. Guillen-Perez and M.-D. Cano, "Flying ad hoc networks: A new domain for network communications," *Sensors*, vol. 18, no. 10, 2018, doi: 10.3390/s18103571.

[38] W. J. Lau, J. M.-Y. Lim, C. Y. Chong, N. S. Ho, and T. W. M. Ooi, "General outage probability model for uav-to-uav links in multi-uav networks," *Computer Networks*, vol. 229, 2023, doi: 10.1016/j.comnet.2023.109752.

[39] L. Zeng, X. Liao, Z. Ma, B. Xiong, H. Jiang and Z. Chen, "Three-Dimensional UAV-to-UAV Channels: Modeling, Simulation, and Capacity Analysis," in *IEEE Internet of Things Journal*, vol. 11, no. 6, pp. 10054-10068, 2024, doi: 10.1109/JIOT.2023.3325945.

[40] M. Mustaqim, B. A. Khawaja, A. A. Razzaqi, S. S. H. Zaidi, S. A. Jawed, and S. H. Qazi, "Wideband and high gain antenna arrays for uav-to-uav and uav-to-ground communication in flying ad-hoc networks (fanets)," *Microwave and Optical Technology Letters*, vol. 60, no. 5, pp. 1164–1170, 2018, doi: 10.1002/mop.31130.

[41] B. Hua *et al*., "Channel Modeling for UAV-to-Ground Communications With Posture Variation and Fuselage Scattering Effect," in *IEEE Transactions on Communications*, vol. 71, no. 5, pp. 3103-3116, 2023, doi: 10.1109/TCOMM.2023.3255900.

[42] H. Li *et al*., "Measurement-based Vegetation Penetration Loss Model for UAV-to-Ground Communications," *2024 IEEE 100th Vehicular Technology Conference (VTC2024-Fall)*, pp. 1-5, 2024, doi: 10.1109/VTC2024-Fall63153.2024.10757551.

[43] Q. Song, Y. Zeng, J. Xu, and S. Jin, "A survey of prototype and experiment for uav communications," *Science China Information Sciences*, vol. 64, no. 140301, pp. 1–21, 2021, doi: 10.1007/s11432-020-3030-2.

[44] B. Zeng, Z. Zhang, X. Ding, X. Bu and J. An, "Predictive decision and reliable accessing for UAV communication in space-air-ground integrated networks," in *China Communications*, vol. 19, no. 1, pp. 166-185, 2022, doi: 10.23919/JCC.2022.01.013.

[45] O. Ceviz, S. Sen and P. Sadioglu, "A Survey of Security in UAVs and FANETs:Issues, Threats, Analysis of Attacks, and Solutions," in *IEEE Communications Surveys & Tutorials*, 2023, doi: 10.1109/COMST.2024.3515051.

[46] X. Du, Y. Cao, L. Wen, and Z. Yang, "A review of intrusion detection in fanets," *Secure and Digitalized Future Mobility: Shaping the Ground and Air Vehicles Cooperation*, vol. 99, 2022.

[47] A. Altaweel, H. Mukkath and I. Kamel, "GPS Spoofing Attacks in FANETs: A Systematic Literature Review," in *IEEE Access*, vol. 11, pp. 55233-55280, 2023, doi: 10.1109/ACCESS.2023.3281731.

[48] M. Bada, D. E. Boubiche, N. Lagraa, C. A. Kerrache, M. Imran, and M. Shoaib, "A policy-based solution for the detection of colluding gps-spoofing attacks in fanets," *Transportation Research Part A: Policy and Practice*, vol. 149, pp. 300–318, 2021, doi: 10.1016/j.tra.2021.04.022.

[49] C. Pu, "Jamming-Resilient Multipath Routing Protocol for Flying Ad Hoc Networks," in *IEEE Access*, vol. 6, pp. 68472-68486, 2018, doi: 10.1109/ACCESS.2018.2879758.

[50] J. Ghelani, P. Gharia and H. El-Ocla, "Gradient Monitored Reinforcement Learning for Jamming Attack Detection in FANETs," in *IEEE Access*, vol. 12, pp. 23081-23095, 2024, doi: 10.1109/ACCESS.2024.3361945.

[51] S. Priyadharshini and P. Balamurugan, "An efficient ddos attack detection and prevention model using fusion heuristic enhancement of deep learning approach in fanet sector," *Applied Soft Computing*, vol. 167, 2024, doi: 10.1016/j.asoc.2024.112438.

[52] I. Bekmezci, O. K. Sahingoz, and Ş. Temel, "Flying ad-hoc networks (fanets): A survey," *Ad Hoc Networks*, vol. 11, no. 3, pp. 1254–1270, 2013, doi: 10.1016/j.adhoc.2012.12.004.

[53] T. Kim, S. Lee, K. H. Kim, and Y.-I. Jo, “Fanet routing protocol analysis for multi-uav-based reconnaissance mobility models,” *Drones*, vol. 7, no. 3, 2023, doi: 10.3390/drones7030161.

[54] I. A. Sumra, P. Sellappan, A. Abdullah, and A. Ali, “Security issues and challenges in manet-vanet-fanet: A survey,” *EAI Endorsed Transactions on Energy Web*, vol. 18, no. 17, 2018, doi: 10.4108/eai.10-4-2018.155884.

[55] N. Islam, M. K. Hossain, G. G. M. N. Ali and P. H. J. Chong, “An expedite group key establishment protocol for Flying Ad-Hoc Network(FANET),” *2016 5th International Conference on Informatics, Electronics and Vision (ICIEV)*, pp. 312-315, 2016, doi: 10.1109/ICIEV.2016.7760017.

[56] S. U. Jan, I. A. Abbasi, F. Algarni and A. S. Khan, “A Verifiably Secure ECC Based Authentication Scheme for Securing IoD Using FANET,” in *IEEE Access*, vol. 10, pp. 95321-95343, 2022, doi: 10.1109/ACCESS.2022.3204271.

[57] A. Gupta, A. Barthwal, H. Vardhan, S. Kakria, S. Kumar, and A. S. Parihar, “Evolutionary study of distributed authentication protocols and its integration to uav-assisted fanet,” *Multimedia Tools and Applications*, vol. 82, no. 27, pp. 42311–42330, 2023, doi: 10.1007/s11042-023-15197-0.

[58] M. Namdev, S. Goyal, and R. Agarwal, “An optimized communication scheme for energy efficient and secure flying ad-hoc network (fanet),” *Wireless personal communications*, vol. 120, no. 2, pp. 1291–1312, 2021, doi: 10.1007/s11277-021-08515-y.

[59] A. Chriki, H. Touati, H. Snoussi, and F. Kamoun, “Fanet: Communication, mobility models and security issues,” *Computer Networks*, vol. 163, 2019, doi: 10.1016/j.comnet.2019.106877.

[60] S. Lateef, M. Rizwan, and M. A. Hassan, “Security threats in flying ad hoc network (fanet),” *Computational Intelligence for Unmanned Aerial Vehicles Communication Networks*, vol. 1033, pp. 73–96, 2022, doi: 10.1007/978-3-030-97113-7_5.

[61] J. Sharma and P. S. Mehra, “Secure communication in iot-based uav networks: A systematic survey,” *Internet of Things*, vol. 23, 2023, doi: 10.1016/j.iot.2023.100883.

[62] K. Prateek, N. K. Ojha, F. Altaf, and S. Maity, “Quantum secured 6g technology-based applications in internet of everything,” *Telecommunication Systems*, vol. 82, no. 2, pp. 315–344, 2023, doi: 10.1007/s11235-022-00979-y.

[63] A. Kumar *et al*., “Survey of Promising Technologies for Quantum Drones and Networks,” in *IEEE Access*, vol. 9, pp. 125868-125911, 2021, doi: 10.1109/ACCESS.2021.3109816.

[64] U. Banerjee, *Efficient algorithms, protocols and hardware architectures for next-generation cryptography in embedded systems*, Ph.D. dissertation, Massachusetts Institute of Technology, 2021.

[65] Y. Lu *et al*., “Uav ad hoc network routing algorithms in space–air–ground integrated networks: Challenges and directions,” *Drones*, vol. 7, no. 7, 2023, doi: 10.3390/drones7070448.

[66] B. Barkee, M. Ceria, T. Moriarty, and A. Visconti, “Why you cannot even hope to use gröbner bases in cryptography: an eternal golden braid of failures,” *Applicable Algebra in Engineering, Communication and Computing*, vol. 31, no. 3, pp. 235–252, 2020, doi: 10.1007/s00200-020-00428-w.

[67] C. W. Vernon, *Ls-aodv: A routing protocol based on lightweight cryptographic techniques for a fanet of nano drones*, Ph.D. dissertation, Monterey, CA; Naval Postgraduate School, 2022.

[68] E. B. Aleksandrova, E. Shkorkina, and M. O. Kalinin, “Organization of the quantum cryptographic keys distribution system for transportation infrastructure users,” *Automatic Control and Computer Sciences*, vol. 53, pp. 969–971, 2019, doi: 10.3103/S0146411619080042.

[69] D. Micciancio and O. Regev, “Lattice-based cryptography,” in *Post-quantum cryptography*, pp. 147–191, 2009, doi: 10.1007/978-3-540-88702-7_5.

[70] H. Nejatollahi, N. Dutt, S. Ray, F. Regazzoni, I. Banerjee, and R. Cammarota, “Post-quantum lattice-based cryptography implementations: A survey,” *ACM Computing Surveys (CSUR)*, vol. 51, no. 6, pp. 1–41, 2019, doi: 10.1145/3292548.

[71] S. Temel and I. Bekmezci, “Scalability analysis of Flying Ad Hoc Networks (FANETs): A directional antenna approach,” *2014 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)*, pp. 185-187, 2014, doi: 10.1109/BlackSeaCom.2014.6849036.

[72] F. De Rango, G. Potrino, M. Tropea, A. F. Santamaria, and P. Fazio, “Scalable and ligthway bio-inspired coordination protocol for fanet in precision agriculture applications,” *Computers & Electrical Engineering*, vol. 74, pp. 305–318, 2019, doi: 10.1016/j.compeleceng.2019.01.018.

[73] Z. G. Al-Mekhlafi, H. D. K. Al-Janabi, M. A. Al-Shareeda, B. A. Mohammed, J. S. Alshudukhi, and K. A. Al-Dhlan, “Fog computing and blockchain technology based certificateless authentication scheme in 5g-assisted vehicular communication,” *Peer-to-Peer Networking and Applications*, vol. 17, no. 6, pp. 3703–3721, 2024, doi: 10.1007/s12083-024-01778-9.

[74] K. Le Hur, “Interacting topological quantum aspects with light and geometrical functions,” *Physics Reports*, vol. 1104, pp. 1–42, 2025, doi: 10.1016/j.physrep.2024.11.003.

[75] T. Proctor, K. Young, A. D. Baczewski, and R. Blume-Kohout, “Benchmarking quantum computers,” *Nature Reviews Physics*, vol. 7, pp. 105–118, 2025, doi: 10.1038/s42254-024-00796-z.

[76] M. Kumar and P. Pattnaik, “Post Quantum Cryptography(PQC) - An overview: (Invited Paper),” *2020 IEEE High Performance Extreme Computing Conference (HPEC)*, pp. 1-9, 2020, doi: 10.1109/HPEC43674.2020.9286147.

[77] D. Joseph, R. Misoczki, M. Manzano, J. Tricot, F. D. Pinuaga, O. Lacombe, S. Leichenauer, J. Hidary, P. Venables, and R. Hansen, “Transitioning organizations to post-quantum cryptography,” *Nature*, vol. 605, no. 7909, pp. 237–243, 2022, doi: 10.1038/s41586-022-04623-2.

[78] A. Aydeger, E. Zeydan, A. K. Yadav, K. T. Hemachandra and M. Liyanage, “Towards a Quantum-Resilient Future: Strategies for Transitioning to Post-Quantum Cryptography,” *2024 15th International Conference on Network of the Future (NoF)*, pp. 195-203, 2024, doi: 10.1109/NoF62948.2024.10741441.

[79] Z. Alzamli, K. Danach and M. Frikha, “Machine Learning Techniques in Service of COVID-19: Data Augmentation Based on Multi-Exposure Image FusionTowards Anomaly Prediction,” *2022 4th International Conference on Current Research in Engineering and Science Applications (ICCRESA)*, pp. 54-58, 2022, doi: 10.1109/ICCRESA57091.2022.10352482.

[80] J. Choi and J. Lee, “Secure and scalable internet of things model using post-quantum macsec,” *Applied Sciences*, vol. 14, no. 10, 2024, doi: 10.3390/app14104215.

[81] J. Jailton, T. Carvalho, J. Araújo, and R. Francês, “Relay positioning strategy for traffic data collection of multiple unmanned aerial vehicles using hybrid optimization systems: A fanet-based case study,” *Wireless Communications and Mobile Computing*, vol. 2017, no. 1, 2017, doi: 10.1155/2017/2865482.

[82] V. Bhardwaj and N. Kaur, “An efficient routing protocol for FANET based on hybrid optimization algorithm,” *2020 International Conference on Intelligent Engineering and Management (ICIEM)*, pp. 252-255, 2020, doi: 10.1109/ICIEM48762.2020.9160327.