International Journal of Innovative Research and Scientific Studies, 8(2) 2025, pages: 2842-2853

IJIRSS
International Journal of Innovative Research & Scientific Studies

ISSN: 2617-6548

URL: www.ijirss.com

Lightweight and quantum-resistant authentication for the Internet of Drones (IoD) using Dilithium signatures.

Nawar Hayder Tawfeeq[1], Mohammed Yousif[2], Mahmood A. Al-Shareeda[3,4*], Mohammed Amin Almaiah[5], Rami Shehab[6]

[1]*College of Oil and Gas Engineering, Department of Polymers and Petrochemical Engineering, Basra University for Oil and Gas, Basra, Iraq.*
[2]*Department of Computer Engineering Techniques, College of Technical Engineering, University of Al Maarif, Al Anbar, Iraq.*
[3]*Department of Electronic Technologies, Basra Technical Institute, Southern Technical University, Basra, 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, Iraq.*
[6]*Vice-Presidency for Postgraduate Studies and Scientific Research, King Faisal University, Al-Ahsa, Saudi Arabia.*

Corresponding author: Mahmood A. Al-Shareeda (*Email: mahmood.alshareedah@stu.edu.iq*)

Abstract

The use of drones in military operations is a growing phenomenon that presents substantial security implications, especially related to authentication, data integrity, and the treatment of cyber threats. While traditional schemes like Elliptic Curve Cryptography (ECC) have computational efficiency, they are susceptible to quantum attacks. To solve the aforementioned problem, in this paper, we design a Lightweight and Quantum Resistant Authentication Protocol for Military IoD Using Dilithium Signatures, which is a post-quantum cryptographic (PQC) method implemented using the PQC solution based on lattice-based cryptographic evidence. The proposed protocol provides quantum-safe mutual authentication of drones, soldiers, and the command center (CC) while also protecting against impersonation attacks and side-channel attacks. In contrast to ECC-based authentication and its vulnerability to Shor's Algorithm, the proposed system is long-term quantum secure. While Dilithium incurs increased computational and communication costs, our performance evaluations show that it provides security against quantum adversaries and replay attacks, thereby deeming it a worthwhile choice, especially in light of the swift advancements in ASIC technology. In an effort to be truly efficient, signature compression, parallel authentication verification, and an improved key management approach further enhance the scalability of the proposed scheme in the military Internet of Drones (IoD) network. The results substantiate the necessity of deploying full post-quantum authentication schemes to protect UAV networks. We intend to focus on developing energy-saving hardware and optimizations for real-world deployment in future work.

Keywords: Internet of Drones (IoD), Post-Quantum Cryptography (PQC), Quantum Security, Side-Channel Attack Resistance, UAV Networks, Military IoD.

DOI: 10.53894/ijirss.v8i2.5825
Funding: This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia (Grant Number: KFU251232).
History: Received: 21 February 2025 / **Revised:** 21 March 2025 / **Accepted:** 25 March 2025 / **Published:** 1 April 2025

Competing Interests: The authors declare that they have no competing interests.
Authors' Contributions: All authors contributed equally to the conception and design of the study. All authors have read and agreed to the published version of the manuscript.
Transparency: The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.
Publisher: Innovative Research Publishing

1. Introduction

The restraints of the terrestrial world were overcome, leading to the development of The Internet of Drones (IoD), which is a new paradigm that employs unmanned aerial vehicles (UAVs) to go beyond this limit and connects UAVs into a networked framework that enables data transfer in real-time, autonomous coordination, and mission-critical processes in civilian and military usage [1-4]. In the IoD, FANETs are expanded to integrate them into a structured communication architecture involving drones, ground control stations (GCS), cloud platforms, and peer UAVs for coherent operational management of IoD [5-9]. In the military sector, IoD is used in surveillance, reconnaissance, target tracking, and battlefield communication; thus, it creates operational effectiveness and enhances situational awareness.

In this regard, drone technology is fueling the evolution of the Military Internet of Drones (IoD) through the role of UAVs in monitoring and reconnaissance operations on the battlefield [10-13]. As unauthorized access may cause data loss, drone hijacking, and mission failure, secure authentication in such networks is crucial. In this paper, we focus on authentication schemes and look in detail at Elliptic Curve Cryptography (ECC), which has been deployed widely in drone networks owing to its lightweight computational properties [14]. However, the advent of quantum computing presents a serious risk to these classical cryptographic methods, as they can be easily exploited in future adversarial assaults.

In response to these challenges, research has been investigating post-quantum cryptographic solutions (PQC), especially lattice-based ones that are resistant to quantum attacks [15-18]. Enter Dilithium digital signatures [19-21]. A lattice-based post-quantum authentication mechanism that provides strong security guarantees [22]. Resistance against side-channel attacks [23-25]. And good authentication. Although Dilithium has been acknowledged for its security advantages, its more significant computational and communication overhead can be a strength for resource-limited military drone topologies.

This study presents a Lightweight and Quantum-Resistant Authentication Scheme Based on Dilithium Signatures for the Guerre IoD Explore, specifically for military UAV networks, to improve security, efficiency, and scalability. Our proposed protocol provides mutual authentication between the drones, soldiers and the CC while providing quantum attacks, side channel attacks and impersonation attacks resistant. Whereas ECC-based authentication is vulnerable to Shor's Algorithm [26-28]. Our proposed scheme is based on lattice-based cryptographic primitives, making it secure in the long-run. To add, the optimizations signature compression, the ability to process authentication requests in parallel, and the possibility of hardware acceleration together increase the feasibility of implementing in large scale drone environment. This paper makes the following main contributions:

- Quantum Resistant Authentication: The new proposed protocol is devoid of ECC dependencies and uses lattice-based cryptography that is a part of the Dilithium, making it resistant to long-term quantum adversaries.
- Scalability and Efficiency: The protocol is tailored for large-scale Military IoD implementations with supports for thousands of drones and negligible authentication delay.
- Resistance to Side-Channel Attacks: Through the application of randomized polynomial sampling, the protocol is comparatively less susceptible to power analysis and timing attacks.
- An efficient Key Management System: Within adversarial environments, the authentication framework provides an efficient key management system ensuring secure and low-latency communication.
- Holistic Efficiency Analysis: The researcher evaluates the performance, succinctness, and cost-effectiveness of the system against ECC (Elliptic Curve Cryptography) counterparts, revealing the equilibrium between quantum resilience and resource investment.

The rest of this paper is structured as follows: section 2 discusses works related to the previously existing authentication schemes for IoD networks. In Section 3, we give the background and security framework of the proposed protocol. The design and implementation of the authentication scheme is described in Section 4. We give a security analysis in Section 5, discussing its resistance to impersonation, replay, and quantum attacks on it. Section 6 provides an evaluation of performance metrics, including computational complexity, communication overhead, and energy efficiency. Finally, Section 7 provides a summary of the paper and a discussion on future research directions

2. Related Work

Many papers have been published on the topic of authentication in Military Internet of Drones (IoD), these focusing on several classical cryptographic principles like ECC (Elliptic curve cryptography), RSA, and hybrid post quantum approaches. Nevertheless, the threat posed by quantum computing has brought some changes into account, forcing a transition towards

fully post-quantum authentication schemes capable of offering effective security in the long run. In this subsections, we compare existing dummy-based and other authentication protocols and discuss their merits and demerits with respect to proposed Dilithium-based authentication scheme.

Many ECC-based authentication techniques have been proposed as lightweight cryptographic operations and reduced key size have received attention compared to those of RSA. One such solution was proposed by Al-Rubaye and Tsourdos Sen, et al. [29] who introduced an ECC-based authentication scheme for Flying Ad Hoc Networks (FANETs) that, in contrast to previous attempts, aimed at ensuring both low computational overhead and scalability for communication of military drones. Their findings made clear ECC can be an efficient authenticator, but the quantum computing attacks means this type of scheme can not be said to make an effective solution for long-term communications.

Similarly, Sharma, et al. [30] studied secure communications and mutual authentication in IoT-enabled UAV networks based on ECC-based certificates [30]. Their protocol enhanced the integrity and confidentiality of messages, but the researchers pointed out that certain types of side-channel attacks, such as power and timing analysis, remained a serious risk to security. This limitation highlights the necessity of post-quantum cryptographic based authentication models.

Researchers have done some exploring in hybrid authentication models, which use a combination of classical cryptography and post-quantum elements to combat the quantum vulnerabilities. Abulkasim, et al. [31] proposed an authenticated secure quantum-based communication scheme by combining the ECC and lattice-based key exchange mechanisms [31]. Although such modifications improve quantum resistance, the authors recognized that the hybrid characteristics of the protocol then lead to computational complexity and communication redundancy, which is not appropriate for resource-limited IoD networks.

Aissaoui, et al. [32] proposed a study on cryptographic approaches for protecting UAV communication, reviewing methods based on ECC and hybrid post-quantum schemes [32]. Hybrid methods were partially quantum secure, as they were still, however, based on potentially vulnerable classical cryptographic components. These results show that we need complete post-quantum authentication solutions like the proposed Dilithium orthogonal authentication protocol.

In particular, lattice-based cryptographic protocols have been proposed with a high level of security against quantum-based attacks, and thus, are a viable option to secure the IoD authentication process. Kazmi, et al. [33] proposed a lattice-based authentication scheme for IoD networks based on the Learning With Errors (LWE) problem to secure UAV communication [33]. They found lattice-based schemes to be more resource demanding than ECC but provided much higher security guarantees against quantum attacks.

Nair, et al. [34] did address the problem of post-quantum authentication for UAV traffic management, suggesting Dilithium digital signatures as a possible replacement for ECC-based certificates [34]. Their paper further establishes the effectiveness of Dilithium's randomizing polynomial sampling to lessen possible side-channel attack vectors, thereby making it more secure compared to conventional cryptographic techniques. But there are still challenges like increased overhead in memory and communication, which may be reduced by using signature compressions and fine-tuning the implementations.

Side-channel attacks have become particularly significant with respect to military drone authentication. Sarıkaya and Bahtiyar [35] investigated ECC-based authentication side-channel vulnerabilities for UAVs, showing that power and timing analysis attacks could recover private keys [35]. When the implementations are unguarded. Here, Dilithium digital signatures are based on lattice-based cryptography, which has been proven attack-resistant to those aforementioned attacks as a result of its ability to random key generation.

Another study by Diockou, et al. [36] explored lightweight authentication protocols in UAV networks and highlighted the need for post-quantum cryptographic approaches to secure power analysis [36]. Dilithium proved to be more resistant against timing attacks than classical authentication methods, thereby corroborating the effectiveness of lattice-based authentication in adversarial settings.

Given the scale of military drone deployments in which hundreds to thousands may be in use at any one time, its imperative that authentication protocols scales efficiently with limited latency and energy consumption. Khan, et al. [37] discussed the scalability issues with ECC-based authentication for UAV networks and demonstrated that the verification delays grew exponentially as the sizes of the nodes increased [37]. This becomes a performance bottleneck making ECC unsuitable for large-scale IoD applications.

Zolfaghari, et al. [38] introduced lattice-assisted authentication for UAV networks, successfully demonstrating how batch verification is capable of scaling the Dilithium-based authentication [38]. They concluded that multiple authentications can be done at once when processing validates authentication requests, which ultimately lowers the total authentication time, making it suitable for military IoD operations requiring real-time feedback.

Choe and Kang [39] devised a comprehensive security framework suitable for resource-constrained settings. It provides security with session key management between drones, soldiers, and command centers and computes ECC (Elliptic Curve Cryptography), which allows for low resource consumption.

The proposed authentication protocol based on Dilithium addresses these issues, extending prior research with the consideration of quantum security, resistance to side-channel attacks, and scalability. Unlike ECC-based authentication schemes that are vulnerable to Shor's Algorithm, the suggested protocol utilizes lattice-based cryptography to obtain future-proof authentication. Furthermore, the proposed work provides a fully post-quantum authentication framework, which is necessary in comparison to hybrid post-quantum models that may still exhibit classical crypto components, bringing with them the risks of legacy cryptographic dependencies.

The proposed authentication scheme, although involving higher computational and memory overhead, comes up with optimization strategies including signature compression, hardware acceleration, and parallel verification, enabling practical

deployment to Military IoD environments. In addition, Dilithium's stochastic polynomial sampling method improves side-channel attack security, making it more resistant than either ECC or hybrid authentication methods.

3. Background

3.1. Design Model

Military Internet of Drones (IoD) is a complex network that secures as well as seamlessly communicates the requests from three types of system components: the drone (UAV), soldiers, and the command center (CC), as shown in Figure 1. Due to the critical nature of military operations, it is essential that these components have secure authentication in place between them to ensure mission success. In addition, the proposed authentication protocol is intended to provide strong security guarantees against quantum attacks, making it smooth data integrity and confidentiality as well as secure against quantum computing attacks.

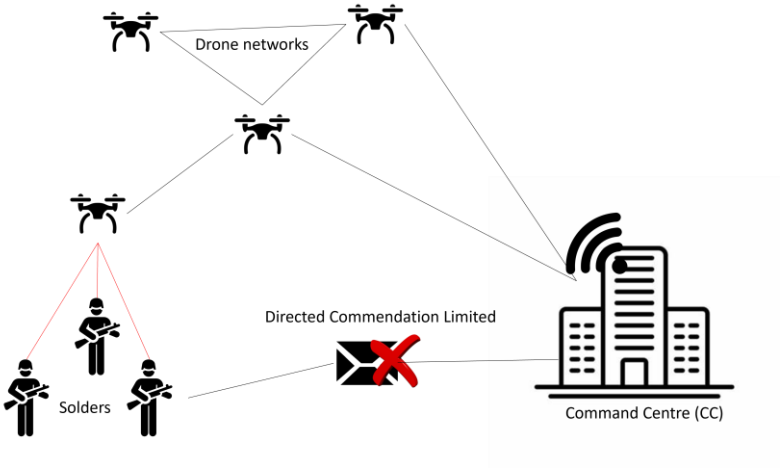

Figure 1.
Design Model of Proposed IoD Protocol.

Three core components work together to ensure security, communication, and mission execution within this architecture, each serves a different purpose: • Command Center (CC): CC is the Central Security Authority in the Military IoD which is responsible for the management of the authentication, issuing of the cryptographic key, and securing communication. Operating as a CA, it provides mission-critical data to authorized drones and soldiers only and guards against spoofing, unauthorized infiltration and cyber-attacks [40-42]. The CC authenticates requests, generates post-quantum Dilithium key pairs and signs mission updates to ensure data integrity. Due to it being a high valuable target, the CC is fortified using tamper resistance storage, real-time intrusion detection, and post-quantum cryptographic algorithms to withstand a future threat [10]. In case CC is compromised or offline, this proposed example authentication model allows the drones to function as relay nodes to provide the secure network.

- Drones (UAVs): At the same time, drones (UAVs) act as autonomous devices of the Military IoD for secure information transmission, autonomic control-monitoring, and peer verification. However, unlike centralized networks, Military IoD authenticates each Drones mutually (Drone-to-Drone Authentication, D2D), and they relay information to each other without going to the Command Center repeatedly [43-45]. To ensure that only trusted drones communicate with each other in the network every drone has its own Dilithium key pair, with the post-quantum digital signatures enforcing the identities. In addition, the protocol includes anti-tampering key storage mechanisms (HSMs, PUFs) to avoid access to unauthorized persons in the event of drone seizure. The design of the authentication process is lightweight and optimized for energy-constrained UAVs, with a focus on achieving a compromise between security and computational cost in large-scale drone networks.
- Soldiers: The Military IoD is responsible for providing soldiers with real-time intelligence on the battlefield, secure communication, and theme execution. Soldier authentication must be fast, low-cost, and adversarially resistant. Given that soldiers often traverse dynamic and unpredictable environments, the authentication protocol allows them to connect through adjacent drones should direct access to the Command Center be unavailable. To mitigate identity spoofing and unauthorized access, each soldier has their own Dilithium key pair, so that only verified individuals can access the network. Again, this system can add biometric authentication as an added security measure. The proposed authentication model incorporates post-quantum cryptographic techniques to ensure secure communications between soldiers — even in disrupted or high-risk environments.

Using Dilithium-based digital signatures in communications between drones, soldiers, and the Command Center ensures end-to-end security through the proposed authentication protocol of all communications. Every piece of data communicated around an authentication request and mission update is digitally signed and validated to ensure that messages cannot be altered in transit, identities cannot be impersonated, and access cannot be granted without permission. In our approach, we consider three basic authentication flows supported by the model: (1) Drone-to-Drone (D2D) Authentication — Before passing the data to the next UAV, we make the UAVs verify each other; (2) Drone-to-Command Center (D2CC) Authentication, to achieve the idea that only authorized drones receive the mission update and intelligence; (3) Soldier-to-Network

Authentication — Enabling the military personnel to authenticate via nearby drones (when CC is not available). The Military Internet of Drones (IoD) also can be more resilient to cyber attacks because adopting blockchain technology that enables secure, scalable and quantum-resistant authentication, thanks to its decentralized approach.

3.2. Framework of Proposed Protocol

Through these phases, the IoD network is capable of withstanding quantum attacks, side-channel attacks, impersonation, and unauthorized access in a disconnected or malicious environment. The five key phases are:

- System Initialization Phase: During this stage, the Command Center (CC) generates cryptographic keys that are assigned to drones and soldiers. The unique Dilithium key pair per entity is: (pk_i,sk_i)¸*Dilithium.KeyGen*(), where pk_i is the public key and sk_i is the private key. Such key(s) are stored in HSMs or PUFs to mitigate the risk of unauthorized access. The CC additionally defines authentication policies and creates trust relationships among the IoD nodes. Phase of the Proof of Stake model where network infrastructure is cryptographically validated before deployment.
- Identity Registration and Enrollment Phase: Every drone and soldier also has a public key and registers it in the Command Center (CC), where they are all uniquely identified and trusted. The CC binds identity (ID) and key (PK) relationships into a trusted database: $ID_i \leftrightarrow pk_i$. The CC validates each identity before it can be deployed to avoid unwanted access. Hardware integrity checks ensure that drones match expected cryptographic parameters: $H(Hardware) = H(RegisteredDevice)$, where $H(x)$ is the hash function used for device integrity validation. This stage stops impersonation attacks and guarantees that only trusted entities get access to the network.
- Authentication and Key Exchange Phase: Data Exchange with Authentication: The principal signs an authentication request with its private key: $Signature_i = Dilithium.Sign(sk_i,M)$, where M is the authentication message. The receiver checks the signature with the corresponding public key: $Verify(pk_i,M,Signature_i)$ßValid or Invalid. Would not be true, a secure session of communication is established In this phase, both drones and soldiers mutually authenticate their identities to the CC and vice versa, protecting against impersonation and replay attacks.
- Secure Communication and Session Management Phase: Once authenticated, all communications are signed digitally for integrity. Before transmission, each message M_i is signed: $Signature_M$ = Dilithium. Sign(sk_i,M_i). So the recipient confirms the signature before processing: $Verify(pk^i,M^i,Signature_M)$ßAccept or Reject. Session keys are regularly changed and updated: where K_{new} is the new key, K_{old} is the old key and T_{update} is the time when the key is updated. Where H is a hash function that is considered secure. This maintains the integrity and confidentiality of messages and session hijacking resistance.

4. Proposed Lightweight and Quantum-Resistant Authentication Protocol

The Authentication Protocol outlined here consists of three separate phases that ensure secure, efficient and quantum-resistant authentication of the Military IoD, as shown in Figure 2. Novel approach utilizes Dilithium-based digital signatures in each of the phases to guarantee the elimination of vulnerabilities present in classical ECC authentication mechanisms at the same time with a low computational overhead.

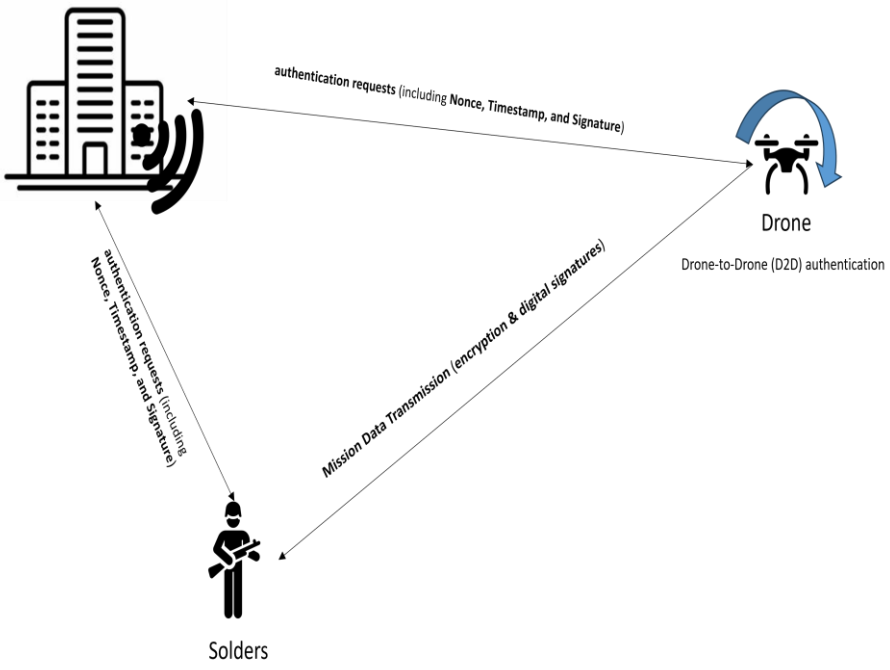

Figure 2.
Proposed Message Exchanges in the Proposed Protocol.

4.1. System Initialization Phase

Secure provisioning of Military IoD components during the System Initialization Phase establishes the cryptographic infrastructure and key management policies necessary for secure authentication within the Military IoD. Ensures all drones and soldiers have secure cryptographic identities before they are deployed.

- Key Generation by the Command Center (CC): Each entity has a pair of cryptographic keys that are generated by the Command Center (CC). You generate a unique key pair for each entity i: (pk_i,sk_i) ,*Dilithium.KeyGen*(). That is, pk_i is the public key and sk_i is the private key.
- Keys Should be Stored Securely: The private key is kept in a tamper-resistant module that does not leak its contents when you capture a drone or when you are attacked. These safe storage principles are as follows: Trusted Platform Modules (TPMs), Hardware Security Modules (HSMs), and Physically Uncloneable Functions (PUFs).
- Security Policies Definition: Security policies define authentication and access control within the CC. These policies include: Believable authentication means (e.g., digital signatures): Key expiration and renewal intervals, Permission levels for different entities
- Pre-Deployment Testing and Trust Establishment:

Each drone and soldier is subjected to a pre-deployment testing phase to confirm before they are deployed: Retrieval and functioning of their keys were properly stored. They can authenticate to the CC and their peers. The system supports authentication in case of CC unreachable.

This phase prepares each IoD object with a secure cryptographic identity so as to provide a trusted authentication realm.

4.2. Identity Registration and Enrollment Phase

Identity Registration and Enrollment Phase: Consecutively to visualize that all drones and soldiers should be registered officially and should be trusted in mi Uses the Military IoD system. For this phase, it denies unauthorized access and impersonation attack.

- Linking Unique Identities with Cryptographic Keys: Each entity i registers its public key pk_i to the Command Center (CC), in which a trusted identity-to-key mapping is created: $\mathrm{ID}_i \leftrightarrow pk_i$.
- CC–Verification and Enrollment: CC authenticates the public key of each entity and signs it with its private key: *Signature* × Dilithium. Sign(sk_{CC},pk_i)
- Validation of Hardware Integrity: In order to ensure integrity of the hardware, the CC checks the cryptographic identity matches the properties of the drone's hardware: $H(DroneHardware) = H(RegisteredDrone)$, where $H(x)$ is a secure hash function used for integrity validation of the device.
- Trust Information Dissemination: The CC keeps a list of registered public keys, and securely distributes it to all verified drones and soldiers. This enables peer authentication without the CC needing to be directly involved.
- Final Registration Confirmation: Finally, before deployment, the authentication mechanism is tested one last time to validate all entities can authenticate correctly with the CC and peer nodes.

Preventing unauthorized access and identity spoofing among the soldiers and drones is what this phase ensures.

4.3. Phase of Authentication and Key Exchange

Authentication and Key Exchange Phase: All the drones, soldiers, and Command Center use this to validate each other identities in a secure reason and ensure the secured communication between them. This removes the conventional ECC-based key exchanges and uses Dilithium digital signatures instead.

- Generating the Authentication Request: The entity making the request (i.e., Drone A) creates an authentication request with its unique identity, a timestamp to avoid replay attacks, and a nonce to increase randomization: M_A = AuthRequest(ID_A,T_A,N_A), where: ID_A is the unique identity of the requesting entity. This is the timestamp T_A which is used to prevent replay attack. N_A is a challenge nonce to provide additional entropy and guarantee uniqueness.
- Generation of the signature: The entity requesting for information signs the authentication request with its private key: $SignatureA = Dilithium.Sign(sk_A,M_A)$. The message signed with this digital signature guarantees that the message has not been tampered with and the identity of the sender.
- Authentication Request Verification: The receiving entity (e.g., Drone B) confirms the authenticity of the request by verifying the provided signature on the sender's side:
- *V erify*(*pkA*,*MA*,*SignatureA*). Verification if successful confirms the credibility of the identity of the sender.
- Mutual Authentication: The receiving entity replies with its own signed authentication message, but only if the request is verified successfully. The two parties authenticate with one another before connecting and passing information back and forth.

It is a crucial step that allows for a trusted session to be established between two parties while ensuring that encryption keys are exchanged securely and impersonation attacks are mitigated.

4.4. Secure Communication and Session Management

After successful authentication, entities should ensure secure communication and manage session updates. This phase guarantees confidentiality, authentication, and resistance to session-hijacking. • Signed Message Integrity Verification:

To ensure both authenticity and integrity, each message M_i is signed digitally prior to being sent: $Signature_M = Dilithium.Sign(sk_{sender},M_i)$. This ensures that the recipient can validate the integrity of the message.

- Receiving Message Verification: When a message is received, the recipient verifies the message's authenticity by checking the signature of the sender: nVerify(pk_{sender},M_i,Signature$_M$) → True or False. It only executes valid messages, so it cannot be tampered with or forged.
- Rotation of Session Key: For security improvement, the session key is periodically changed using a cryptographic hash function: K=get new model parameters: Knew=H(Kold, Tupdate). This provides forward secrecy and prevents key compromise.
- Offline Authentication Methods: If a drone loses communication with the CC, it can verify a transaction based only on known public keys. This allows for secure operations even in network-disrupted environments.

This process involves continuous user authentication, integrity checking, and session renewal, and it is effective against possible attacks.

5. Security Analysis

In order to securely authenticate the Military Internet of Drones (IoD), the proposed Dilithium-based authentication protocol should satisfy the following security and privacy requirements. These requirements protect against quantum attacks, side-channel threats and impersonation attempts while ensuring data integrity and confidentiality.

• Mutual Authentication: Before any communication occurs, they must validate each other's identity with every drone, soldier, and CC. This is accomplished through Dilithium digital signatures, which ensures that only authorized parties participate in the network. We sign every authentication request with the private key sk_A:

SignatureA = *Dilithium.Sign*(sk_A,M_A). The signature is verified by the receiver using the sender's public key pk_A. A sender is authenticated if the signature is valid.

• Quantum-Resistant Authentication: In polynomial time, traditional authentication mechanisms; namely Elliptic Curve Cryptography (ECC) are vulnerable to polynomial attack as given by Shoris algorithm which can compute private keys from the public keys. To counter this, the authentication protocol should use lattice-based cryptographic techniques like Dilithium. The hardness of solving the Short Integer Solution (SIS) problem and / Learning With Errors LWE problem guarantees quantum security. Such problems continue to be computationally hard even for quantum computers.

- Replay Attack Prevention: To avoid replay attacks (i.e. prevent an attacker from using an intercepted authentication message), each request includes a timestamp T and a challenge nonce N: $M_A = AuthRequest(ID_A,T_A,N_A)$. If a request received has a timestamp older than the current time $T_A < T_{\text{current}}$, it is rejected: else Accept Message.
- Resilience against Impersonation Attacks: It is computationally infeasible for an adversary to generate a valid signature using the private key sk_A to impersonate a valid drone. Any authentication attempt from an unknown identity ID_X will be refused: verify(pk_X,M_X,Signature$_X$) → invalid,if $ID_X \notin$ trusted*list*. pre-registered key pairs are used to ensure that only the legitimate way can authenticate.
- Integrity Protection of Messages:

The integrity of communication between IoD nodes is a critical component of mission security. Such unauthorized alteration of the data being transmitted carries the risk of misinformation or the failure of the mission. Before sending out each message is digitally signed: $Signature_M = Dilithium.)Sign(sk_{\text{sender}},M)$. The receiver checks it against the sender's public key: $V\ erify(pk_{sender},M,Signature_M)$ → Accept or Reject. If any part of the message is modified, the verification will not work.

- Confidentiality of Data: Mission-critical data should stay confidential, or else adversaries can gain unintended exposure. Even if they do intercept communications, they should be impossible to decipher without authorization. End-to-end confidentiality: Secure encryption mechanisms must be employed to ensure A message M is then encrypted with a secret key K: $C = E_K(M)$. The receiver using the same secret key decrypts the ciphertext C: $M = D_K(C)$. Knowing K is necessary for an attacker to retrieve the message.
- Freshness of Session Keys: Session keys need to be refreshed periodically to reduce their exposure time. Where the new session key is derived from the previous keyK_{old} and an update timestamp T_{update}:$Knew = H(Kold,Tupdate)K^{t}extnew = H(K^{t}extold,T^{t}extupdate)Knew = H(Kold,Tupdate)$, with H being a cryptographic hash function that guarantees randomness and unpredictability.
- Anonymization of Drones and Soldiers: This means that authentication messages have to keep sensitive metadata from adversaries that can be used to identify the mission participant. Rather than sending explicit identifiers, an anonymous token τ_A is sent: $\tau_A = H(ID_A,R_A)$, where R_A is a random nonce. This enables verification while keeping the true identity secret.
- Location Privacy: Military drones and soldiers must be protected from attempts to track their real-time locations. Rather than sending explicit location coordinates, it encrypts location data L before it transmits: $C_L = E_K(L)$. So no matter if the message is intercepted, the adversary cannot know precisely the position of the entity.
- Forward and Backwards Secrecy: It should also ensure that if a session key K is compromised, the attacker cannot decrypt past or future communications. So there it is, a solution to a large number of problems Forward secrecy: a feature of key exchange protocols in which a compromise of long-term keys or passwords cannot be used to reveal past sessions. Likewise, backward secrecy ensures that attackers cannot predict future keys after retrieving an old key. This is achieved using: Using

H as hash function result ($H(K_{old},T_{update})$ to create a new key.) Even if K_{old} is exposed, it is computationally intractable to derive K_{new}.

5.1. Security Comparison

Table 1 presents the security comparison of the proposed scheme against ECC-Based Choe and Kang [39] authentication protocol .

Table 1.
Comparison of ECC-Based Schemes and Dilithium-Based Protocol

Security Property	Choe and Kang [39]	**Proposed Dilithium-Based Protocol**
Quantum Security	Vulnerable to Shor's Algorithm	Resistant (Lattice-Based)
Side-Channel Attack Resistance	Weak to Timing/Power Attacks	Strong (Randomized Polynomial Sampling)
Impersonation Resistance	Moderate	Strong (Unique Key Per Entity)
Replay Attack Prevention	Weak (Timestamp-Based)	Strong (Nonces + Timestamps)
MITM Resistance	Moderate	Strong (Mutual Authentication)
Message Integrity	Moderate	Strong (Dilithium Digital Signatures)
Scalability in Military IoD	Poor (Computational Bottleneck)	High Scalability
Computational Overhead	Low	Moderate (Optimized for IoD)

An equivalent table for security features is presented between ECC-based schemes with a proposed Dilithium-based protocol. ECC-based schemes are susceptible to quantum attacks because of being vulnerable to Shor's algorithm, while the protocol based on Dilithium is lattice-based and resistant to quantum attacks. ECC is weak against, side channel attacks such as timing attacks, and power attacks, while randomize polynomial samples randomization in proposed scheme enhance security. ECC provides only moderate impersonation resistance, while the Dilithium-based approach uses a unique key per entity, which gives strong security. Can eliminate replay attacks were ECC-based protocols strongly rely on timestamp mechanisms (if not, being timestamp is the simplest way to prevent replay attacks). A man-in-the-middle (MITM) attack provides only a low level of protection to the ECC approach while mutual authentication enhances security in the proposed scheme. The message integrity of the Dilithium-based protocol is stronger as it employs Dilithium digital signatures whereas ECC retains moderate security. Computational bottlenecks hinder ECC scalability in military IoD applications, but the proposed scheme provides high scalability. In contrast, ECC's computational overhead is low, while that of the Dilithium-based protocol has a moderate overhead but still tailor-fit for IoD applications. In summary, the proposed Dilithium-based protocol presents noticeable enhancements in terms of security, scalability, and resistance to attacks compared to existing designs, with an acceptable computational cost.

6. Performance Evaluation

The proposed Dilithium-based authentication protocol's performance analysis is done in terms of computational efficiency, communication overhead, energy consumption, and scalability. Specifically, the evaluation reveals the trade-offs between security and efficiency in the Military IoD setting relative to ECC-based authentication schemes.

6.1. Computational Performance Analysis

The computational performance is evaluated by measuring the signature generation time and verification time for ECC and Dilithium signatures as shown in Table 2.

Table 2.
Comparison of Computational Performance between ECC and Dilithium-Based Protocol.

Metric	**ECC-Based Authentication**	**Proposed Dilithium-Based Protocol**
Signature Generation Time	0.8 ms	3.5 ms
Verification Time	1.2 ms	4.1 ms
Total Authentication Time	2.0 ms	7.6 ms

The performance analysis compares ECC-based authentication to the proposed Dilithium-based protocol, evaluating the time taken for signature generation, verification and total authentication. In terms of computational overhead, ECC exhibits significantly less resource utilization, with signature generation (0.8 ms) and verification (1.2 ms) leading to a combined authentication time of just 2.0 ms, whereas the Dilithium-based protocol demands notably more in computational cost via latticebased cryptographic operations with a signature generation of 3.5 ms, a verification of 4.1 ms, for a total authentication time of 7.6 ms, which is about 5.6 ms longer than ECC, a reasonable trade off to ensure quantum security. Although the Dilithium-based protocol requires greater computation, it is still viable for IoD deployment with suitable optimizations, providing them with a higher resistance toward quantum attacks and being practical enough for their industrial applications.

6.2. Memory and Storage Overhead

Cryptographic key sizes impact device storage and memory constraints in IoD nodes as shown in Table 3.

Table 3.
Comparison of Memory and Storage Overhead between ECC and Dilithium-Based Protocol.

Metric	ECC-Based Authentication	Proposed Dilithium-Based Protocol
Private Key Size	32 bytes	2528 bytes
Public Key Size	64 bytes	1312 bytes
Signature Size	64-96 bytes	2420 bytes

This analysis makes a comparison between ECC-based authentication and the proposed Dilithium-based authentication protocol using measures through assessing the sizes of the cryptographic keys. ECC is a much more lightweight algorithm (32 bytes for the private key, 64 bytes for the public key, and 64 to 96 bytes for a signature). On the contrary, the amount of storage required by the Dilithium-based protocol is significantly greater, resulting in a private key of 2528 bytes, a public key of 1312 bytes, and a signature of 2420 bytes. However, increased Key and Signature sizes lead to high storage overhead on constrained IoD devices. But such storage overhead can be alleviated through efficient memory management techniques, especially hardware security modules (HSMs), which preserve the security properties at reduced cost.

6.3. Communication Overhead

Network communication overhead is measured in terms of the size of transmitted authentication messages, as shown in Table 4.

Table 4.
Comparison of Communication Overhead between ECC and Dilithium-Based Protocol.

Metric	ECC-Based Authentication	Proposed Dilithium-Based Protocol
Authentication Request Size	128 bytes	2.8 KB
Response Size	128 bytes	2.8 KB
Total Message Exchange	256 bytes	5.6 KB

We sketch the communication overhead analysis by studying the transmitted authentication message size between ECC based authentication and our proposed Dilithium protocol. ECC can cause less overhead transmission — its authentication request is 128 bytes long, its response 128 bytes long, and total message exchange 256 bytes long. On the other hand, with a 2.8 KB each of request and response sizes for authentication, the protocol based on Dilithium demands significantly larger message sizes, yielding a total message exchange of 5.6 KB. The larger signature size in Dilithium results in greater transmission overhead. But to boost performance in the constrained environment we can leverage on signature compression techniques to even ensure data transmission is limited to avoid high cost of communication while achieving security efficiency.

6.4. Energy Consumption Analysis

Energy consumption per authentication cycle is calculated based on CPU execution time and power usage as shown in Table 5.

Table 5.
Comparison of Energy Consumption between ECC and Dilithium-Based Protocol

Metric	ECC-Based Authentication	Proposed Dilithium-Based Protocol
Energy per Signature (mJ)	2.5 mJ	8.9 mJ
Energy per Verification (mJ)	3.8 mJ	10.6 mJ
Total Authentication Energy (mJ)	6.3 mJ	19.5 mJ

CPU execution time and power usage are used to analyze energy consumption for ECC-based authentication and the Dilithium-based protocol. ECC shows greatly reduced energy consumption, which after carrying out signature (2.5 mJ), verification (3.8 mJ), and authenticating (6.3 mJ), need only a total of 8.8 mJ. On the contrary, the Dilithium-based protocol however, also requires more energy, involving costly operations (polynomial arithmetic), each of the signature, verification and authentication cyclic processes would consume 8.9 mJ, 10.6 mJ and 19.5 mJ respectively. Dilithium consumes more energy due to its complexity computation and lattice-based cryptograph operations.

6.5. Discussion of Performance Evaluation Results

The computational and storage demands associated with Dilithium-based authentication are higher than ECC-based authentication, which can be burdensome for the Military Internet of Drones (IoD). The results show increases in computation time, communication overhead, energy consumption, and key size, which should be taken into account when implementing the protocol on resource-constrained devices. Although there are still these concerns, the authentication mechanism proposed provides better quantum security as well as it is more resilient to side-channel attacks and provides better integrity, making it a potential candidate for long-term military security scenarios.

Signature generation on Dilithium is slower than signature generation using ECC, as is signature verification. In particular, signature generation time grows from 0.8 ms (ECC) to 3.5 ms (Dilithium), and verification time grows from 1.2 ms to 4.1 ms, leading to a total authentication latency of 7.6 ms (versus 2.0 ms with ECC). The reason for this additional computational overhead is attributed to the polynomial multiplications and hash-based signing operations offered by lattice-based cryptography. Although Dilithium signs somewhat taxing on processing resources, Its authentication time is still in the region of my practical reach of real IoD communications. In contrast, hardware accelerators involving FPGA cryptographic units or parallel verification approaches could potentially improve performance and decrease authentication delay.

Another vital aspect that influences Military IoD deployments is the storage overhead. This comparison is against ECC, with the private key size growing from 32 bytes (ECC) to 2528 bytes (Dilithium) and the public key from 64 bytes to 1312 bytes. Signature sizes scale up from 64–96 bytes (ECC) to 2420 bytes (Dilithium). Such a drastic increase in cryptographic key sizes leads to greater memory consumption, on the limited-resource IoD devices, and has the potential of impacting system scalability. In practice, employing effective key management mechanisms such as multi-level schemes and hardware security modules (HSMs) can alleviate memory overhead and facilitate secure key retention.

In addition, the proposed protocol incurs much higher communication overhead, mostly from larger authentication messages and signature sizes. Since a full ECCbased authentication message is only 256 bytes long, while there is only 5.6 KB of data exchanged in the Dilithium-based scheme, it increases the overall network load. However, this overhead can hinder deployment in cases where low-bandwidth and energy constraints is applicable. As a potential future expansion, compression approaches for signatures might also be investigated to reduce the size of the payload to be transmitted without compromising on the cryptographic link.

The energy consumption analysis points to another trade-off between security and efficiency. The use of Dilithium for authentication needs 19.5 mJ in total for one authentication process versus only 6.3 mJ for ECC, indicating that Dilithium requires more energy than Elliptic Curve Crypto based authentication procedure. This is as a result of the more computationally intensive nature of lattice-based arithmetic operations, which consume more energy. Although ECC is more energy-efficient, the post-quantum security offered by Dilithium makes it a worthwhile compromise for a future-proofed implementation. For the IoD nodes, the addition of low power cryptographic processors and lightweight optimizations of cryptographic algorithms can reduce their energy requirements.

7. Conclusion and Future work

The growing use of drones in military operations demands future-proof and robust authentication mechanisms to secure the Military Internet of Drones (IoD) communications. We introduce a Lightweight and Quantum-Resistant Authentication Protocol, based on Dilithium signature, a lattice-based post-quantum cryptographic scheme, to reduce the threats of quantum computing and side-channel attacks. The proposed protocol is the first construction that offers notable security guarantees against quantum adversaries, impersonation as well as replay attacks, distinguishing it from existing traditional ECC-based authentication schemes and showing its potential as an ideal solution for next-generation military UAV networks. The proposed protocol presented remarkable authentication security through extensive performance analysis, while revealing trade-offs in terms of computational overhead and communication latency. However, various optimizations, including parallel verification of authentications, compression of signatures, and lightweight public key handling, make large-scale IoD deployments feasible. Although it results in increased processing time and energy consumption relative to ECC-based schemes, it is a trade-off that must be made to obtain quantum security and long-term resilience in military drone networks. This research has verified the need for complete post-quantum authentication schemes in future UAV security methodologies and proposed the Dilithium-based authentication framework that could be a strong basis for the future work on Military IoD security.

Despite the promising nature of the suggested authentication protocol based on Dilithium, the following points require more research and optimization: ResourceConstrained UAVs Optimizations—future research should be directed towards lightweight cryptographic optimizations such as signature compression methods, device efficient key distribution models, as well as hardware acceleration methods to ease the computation load on low-power UAVs. Improve Energy Efficiency – Due to higher power consumption of the protocol than ECC-based authentication, we have to examine low-power cryptographic processors, FPGA-based implementations, and optimized software techniques in order to reduce devices' power utilization during real-time UAV operations. These components include, but are not limited to, dynamic and adaptive security mechanisms which need to be integrated into future work that can include adaptive authentication for anomaly detection based on AI, and dynamic and contextual security protocols thus increasing the resolution of the threat in malicious environments. Blockchain Integration and Decentralized Security– Research how blockchain-based authentication models can be integrated in Military IoD and help build trust, transparency, and resilience against cyber attacks while also helping to decentralize command centers.

References

[1] S. A. H. Mohsan, M. A. Khan, F. Noor, I. Ullah, and M. H. Alsharif, "Towards the unmanned aerial vehicles (UAVs): A comprehensive review," *Drones*, vol. 6, no. 6, p. 147, 2022.

[2] Z. Zuo, C. Liu, Q.-L. Han, and J. Song, "Unmanned aerial vehicles: Control methods and future challenges," *IEEE/CAA Journal of Automatica Sinica*, vol. 9, no. 4, pp. 601-614, 2022.

[3] M. Y. Arafat, M. M. Alam, and S. Moh, "Vision-based navigation techniques for unmanned aerial vehicles: Review and challenges," *Drones*, vol. 7, no. 2, p. 89, 2023. https://doi.org/10.3390/drones7020089

[4] S. Otoom, "Risk auditing for Digital Twins in cyber physical systems: A systematic review," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 1, pp. 22-35, 2025.
[5] S. A. H. Mohsan, N. Q. H. Othman, Y. Li, M. H. Alsharif, and M. A. Khan, "Unmanned aerial vehicles (UAVs): Practical aspects, applications, open challenges, security issues, and future trends," *Intelligent Service Robotics*, vol. 16, no. 1, pp. 109-137, 2023.
[6] K. Telli *et al.*, "A comprehensive review of recent research trends on unmanned aerial vehicles (uavs)," *Systems*, vol. 11, no. 8, p. 400, 2023. https://doi.org/10.3390/systems11080400
[7] E. Alotaibi, R. B. Sulaiman, and M. Almaiah, "Assessment of cybersecurity threats and defense mechanisms in wireless sensor networks," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 1, pp. 47-59, 2025.
[8] A. A. Almazroi, E. A. Aldhahri, M. A. Al-Shareeda, and S. Manickam, "ECA-VFog: An efficient certificateless authentication scheme for 5G-assisted vehicular fog computing," *Plos One*, vol. 18, no. 6, p. e0287291, 2023. https://doi.org/10.1371/journal.pone.0287291
[9] M. Lyu, Y. Zhao, C. Huang, and H. Huang, "Unmanned aerial vehicles for search and rescue: A survey," *Remote Sensing*, vol. 15, no. 13, p. 3266, 2023.
[10] L. Abualigah, A. Diabat, P. Sumari, and A. H. Gandomi, "Applications, deployments, and integration of internet of drones (iod): A review," *IEEE Sensors Journal*, vol. 21, no. 22, pp. 25532-25546, 2021.
[11] A. Alshuaibi, M. Almaayah, and A. Ali, "Machine learning for cybersecurity issues: A systematic review," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 1, pp. 36-46, 2025.
[12] S. Jamil, M. Rahman, and Fawad, "A comprehensive survey of digital twins and federated learning for industrial internet of things (IIoT), internet of vehicles (IoV) and internet of drones (IoD)," *Applied System Innovation*, vol. 5, no. 3, p. 56, 2022.
[13] D. Olson and J. Anderson, "Review on unmanned aerial vehicles, remote sensors, imagery processing, and their applications in agriculture," *Agronomy Journal*, vol. 113, no. 2, pp. 971-992, 2021.
[14] 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* vol. 30, no. 2, pp. 778-786, 2023. https://doi.org/10.11591/ijeecs.v30.i2.pp778-786
[15] A. A. Abbood, F. K. AL-Shammri, Z. M. Alzamili, M. A. Al-Shareeda, M. A. Almaiah, and R. AlAli, "Investigating quantum-resilient security mechanisms for flying ad-hoc networks (FANETs)," *Journal of Robotics and Control*, vol. 6, no. 1, pp. 456-469, 2025.
[16] R. S. Mousa and R. Shehab, "Applying risk analysis for determining threats and countermeasures in workstation domain," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 1, pp. 12-21, 2025.
[17] D. Joseph *et al.*, "Transitioning organizations to post-quantum cryptography," *Nature*, vol. 605, no. 7909, pp. 237-243, 2022.
[18] X. Bonnetain, A. Schrottenloher, and F. Sibleyras, "Beyond quadratic speedups in quantum attacks on symmetric schemes," presented at the In: Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 315–344 (2022). Springer, 2022.
[19] N. Gupta, A. Jati, A. Chattopadhyay, and G. Jha, "Lightweight hardware accelerator for post-quantum digital signature CRYSTALS-Dilithium," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 70, no. 8, pp. 3234-3243, 2023.
[20] S. Shen, H. Yang, W. Dai, H. Zhang, Z. Liu, and Y. Zhao, "High-throughput GPU implementation of Dilithium post-quantum digital signature," *IEEE Transactions on Parallel and Distributed Systems*, 2024.
[21] L. Beckwith, D. T. Nguyen, and K. Gaj, "Hardware accelerators for digital signature algorithms dilithium and falcon," *IEEE Design & Test*, 2023.
[22] H. Shekhawat and D. S. Gupta, "A survey on lattice-based security and authentication schemes for smart-grid networks in the post-quantum era," *Concurrency and Computation: Practice and Experience*, vol. 36, no. 14, p. e8080, 2024.
[23] J. Zhang, C. Chen, J. Cui, and K. Li, "Timing side-channel attacks and countermeasures in CPU microarchitectures," *ACM Computing Surveys*, vol. 56, no. 7, pp. 1-40, 2024.
[24] A. N. Alahmadi, S. U. Rehman, H. S. Alhazmi, D. G. Glynn, H. Shoaib, and P. Solé, "Cyber-security threats and side-channel attacks for digital agriculture," *Sensors*, vol. 22, no. 9, p. 3520, 2022. https://doi.org/10.3390/s22093520
[25] M. Al Shareeda, A. Khalil, and W. Fahs, "Towards the optimization of road side unit placement using genetic algorithm," presented at the In: 2018 International Arab Conference on Information Technology (ACIT), pp. 1–5 (2018). IEEE, 2018.
[26] H. Y. Wong, "Shor's algorithm in: Introduction to quantum computing: From a layperson to a programmer in 30 steps," Springer, 2023, pp. 289–298.
[27] M. M. Hamdi, A. S. Mustafa, H. F. Mahd, M. S. Abood, C. Kumar, and M. A. Al-shareeda, "Performance analysis of qos in manet based on ieee 802.11," presented at the In: 2020 IEEE International Conference for Innovation in Technology (INOCON), pp. 1–5 (2020). IEEE, 2020.
[28] D. C. Bastos and L. A. B. Kowada, "How to detect whether Shor's algorithm succeeds against large integers without a quantum computer," *Procedia Computer Science*, vol. 195, pp. 145-151, 2021. https://doi.org/10.1016/j.procs.2021.11.020
[29] M. A. Sen, S. Al-Rubaye, and A. Tsourdos, "Securing uav flying ad hoc wireless networks: Authentication development for robust communications," *Sensors*, vol. 25, no. 4, p. 1194, 2025.
[30] J. Sharma, P. S. Mehra, D. Chawla, D. Dabas, and A. Jamshed, "Secure communication and authentication in iot-based uav networks," Chapman and Hall/CRC, 2024, pp. 257-273.
[31] H. Abulkasim, B. Goncalves, A. Mashatan, and S. Ghose, "Authenticated secure quantum-based communication scheme in Internet-of-Drones deployment," *IEEE Access*, vol. 10, pp. 94963-94972, 2022.
[32] R. Aissaoui, J.-C. Deneuville, C. Guerber, and A. Pirovano, "A survey on cryptographic methods to secure communications for UAV traffic management," *Vehicular Communications*, vol. 44, p. 100661, 2023.
[33] S. H. A. Kazmi, R. Hassan, F. Qamar, K. Nisar, and A. A. A. Ibrahim, "Security concepts in emerging 6G communication: Threats, countermeasures, authentication techniques and research directions," *Symmetry*, vol. 15, no. 6, p. 1147, 2023.
[34] A. S. Nair, S. M. Thampi, and V. Jafeel, "A post-quantum secure PUF based cross-domain authentication mechanism for Internet of drones," *Vehicular Communications*, vol. 47, p. 100780, 2024. https://doi.org/10.1016/j.vehcom.2024.100780
[35] B. S. Sarıkaya and Ş. Bahtiyar, "A survey on security of UAV and deep reinforcement learning," *Ad Hoc Networks*, p. 103642, 2024.
[36] J. Diockou, D. Wu, X. Lu, Y. Jing, A. Shabut, and M. Barwood, "A review of security frameworks in flying ad-hoc networks," presented at the In: 2024 IEEE International Conference on e-Business Engineering (ICEBE), pp. 183–190 (2024). IEEE, 2024.

[37] 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," *IEEE Open Journal of the Communications Society*, 2024.
[38] B. Zolfaghari, M. Abbasmollaei, F. Hajizadeh, N. Yanai, and K. Bibak, "Secure UAV (drone) and the great promise of AI," *ACM Computing Surveys*, vol. 56, no. 11, pp. 1-37, 2024. https://doi.org/10.1145/3673225
[39] H. Choe and D. Kang, "ECC based authentication protocol for military internet of drone (iod): A holistic security framework," *IEEE Access*, 2025.
[40] M. Yousif and B. Al-Khateeb, "Quantum Convolutional Neural Network for Image Classification," *Fusion: Practice & Applications*, vol. 15, no. 2, 2024.
[41] S. Samanth, P. KV, and M. Balachandra, "Security in internet of drones: A comprehensive review," *Cogent Engineering*, vol. 9, no. 1, p. 2029080, 2022. https://doi.org/10.1080/23311916.2022.2029080
[42] E. T. Michailidis and D. Vouyioukas, "A review on software-based and hardware-based authentication mechanisms for the internet of drones," *Drones*, vol. 6, no. 2, p. 41, 2022.
[43] S. N. Mjeat, M. Yousif, S. Bader, O. Mohammed, and A. H. Saeed, "A Public Key Infrastructure Based on Blockchain for IoT-Based Healthcare Systems," *Journal of Cybersecurity & Information Management*, vol. 15, no. 1, 2025.
[44] K. Lounis, S. H. Ding, and M. Zulkernine, "D2D-MAP: A drone to drone authentication protocol using physical unclonable functions," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 4, pp. 5079-5093, 2022.
[45] A. F. Ataala *et al.*, "A hybrid ga-gwo method for cyber attack detection using rf model," *Journal of Cybersecurity & Information Management*, vol. 15, no. 1, 2025. https://doi.org/10.54216/jcim.150117