Review

Secure Communication in Drone Networks: A Comprehensive Survey of Lightweight Encryption and Key Management Techniques

Sayani Sarkar [*] , Sima Shafaei , Trishtanya Jones , Michael Totaro

Posted Date: 17 July 2025

doi: 10.20944/preprints202507.1503.v1

Keywords: UAV communication; lightweight encryption; key management; blockchain; physical layer security; post-quantum cryptography

Review

Secure Communication in Drone Networks: A Comprehensive Survey of Lightweight Encryption and Key Management Techniques

Sayani Sarkar [1,*,†], Sima Shafaei [1], Trishtanya S Jones [2] and Michael W Totaro [2]

[1] Bellarmine University, USA; sshafeai@bellarmine.edu
[2] University of Louisiana at Lafayette, USA; trishtanya.jones1@louisiana.ed (T.S.J.); michael.totaro@louisiana.edu (M.W.T.)
[*] Correspondence: ssarkar@bellarmine.edu
[†] Current address: 2001 Newburg Rd, Louisville, KY 40205.

Abstract

Deployment of Unmanned Aerial Vehicles (UAVs) continues to expand rapidly across a wide range of applications, including environmental monitoring, military surveillance, precision agriculture, and disaster response. Despite their increasing ubiquity, UAVs remain inherently vulnerable to security threats due to resource-constrained hardware, energy limitations, and reliance on open wireless communication channels. These factors render traditional cryptographic solutions impractical, thereby necessitating the development of lightweight, UAV-specific security mechanisms. This review presents a comprehensive analysis of lightweight encryption techniques and key management strategies designed for energy-efficient and secure UAV communication. Special emphasis is placed on recent cryptographic advancements, including the adoption of the ASCON family of ciphers and the emergence of post-quantum algorithms that can secure UAV networks against future quantum threats. Key management techniques such as blockchain-based decentralized key exchange, Physical Unclonable Function (PUF)-based authentication, and hierarchical clustering schemes are evaluated for their performance and scalability. To ensure comprehensive protection, this review introduces a multilayer security framework addressing vulnerabilities from the physical to the application layer. Comparative analysis of lightweight cryptographic algorithms and multiple key distribution approaches is conducted based on energy consumption, latency, memory usage, and deployment feasibility in dynamic aerial environments. Our review also identifies key research challenges, including secure and efficient rekeying during flight, resilience to cross-layer attacks, and the need for standardized frameworks supporting post-quantum cryptography in UAV swarms. By synthesizing current advancements and highlighting research gaps, this study aims to provide a foundation for future secure communication architectures tailored to the unique operational constraints of UAV networks.

Keywords: UAV communication; lightweight encryption; key management; blockchain; physical layer security; post-quantum cryptography

1. Introduction

UAVs have evolved from specialized military assets to ubiquitous platforms that support various civilian and military applications, including aerial surveillance, disaster response, environmental monitoring, precision agriculture, and autonomous logistics [1]. Their operational advantages - high maneuverability, reduced operational costs and the ability to operate in harsh or inaccessible environments - have driven exponential growth in both research initiatives and commercial deployment across multiple domains [2]. As UAVs become increasingly integrated into critical infrastructure and multi-agent systems, the volume and sensitivity of their data exchanges continue to expand, making secure and reliable communication within UAV networks a paramount challenge for both industry and academia [3].

Despite their growing adoption, UAV communication systems remain fundamentally constrained by hardware limitations, energy capacity restrictions, and dynamic network topologies. UAVs operate with limited computational resources on board, making traditional cryptographic approaches, such as full-scale RSA, TLS implementations, or computationally intensive AES variants, impractical for real-time aerial operations [4]. Additionally, UAV networks frequently operate in self-organized, highly dynamic configurations, particularly in swarm deployments where coordinated systems of potentially hundreds of drones must perform missions autonomously with minimal human oversight [5]. These operational conditions introduce significant complexities in key management, authentication, and data confidentiality protocols [6].

The emergence of quantum computing poses an additional and unprecedented threat to UAV communication security. Quantum computers, leveraging Shor's and Grover's algorithms, have the potential to break conventional cryptographic methods, including both symmetric and asymmetric schemes that currently secure UAV communications [7]. This quantum threat necessitates the adoption of post-quantum cryptography (PQC) algorithms specifically designed to remain secure against quantum attacks while maintaining efficiency suitable for resource-constrained UAV platforms [8]. Recent developments in lightweight post-quantum algorithms, including lattice-based cryptography and code-based cryptography, offer promising solutions for future-proofing UAV security [7].

Recent research efforts have explored innovative approaches to UAV security, including the integration of blockchain technology for decentralized identity and key management in drone swarms [9]. Blockchain-based authentication schemes, such as BETA-UAV, exploit the inherent properties of immutability and decentralization to establish secure communication sessions while reducing reliance on centralized trust infrastructures [10]. Similarly, Physical Unclonable Function (PUF)-based authentication protocols have emerged as lightweight alternatives that eliminate the need for storing sensitive cryptographic keys on UAV devices, thereby mitigating key storage vulnerabilities [11].

The advent of the ASCON family of authenticated encryption algorithms, selected as the NIST lightweight cryptography standard, represents a significant milestone for UAV security [12]. ASCON's sponge-based design offers superior performance metrics compared to traditional AES implementations while maintaining robust security properties suitable for resource-constrained environments [4]. Performance evaluations demonstrate that ASCON-128a provides optimal balance between efficiency and security for UAV communication systems, achieving comparable throughput to AES with significantly reduced memory footprint and energy consumption [13].

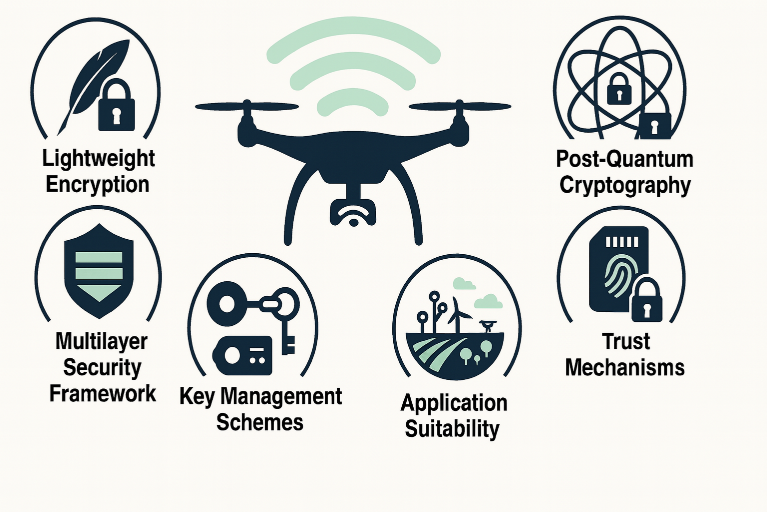

Figure 1. Multilayer Security Focus Areas for UAV Communications: Lightweight Encryption, Post-Quantum Cryptography, Trust Mechanisms, Application Suitability, Key Management Schemes, and a Multilayer Security Framework.

Regulatory developments further underscore the urgency of implementing robust UAV security measures. The Federal Aviation Administration (FAA) has proposed new cybersecurity regulations requiring design approval applicants to identify, assess, and mitigate risks from intentional unauthorized electronic interactions (IUEI) in transport category aircraft, including UAV systems [14]. Similarly, the European Union Aviation Safety Agency (EASA) has issued draft policies mandating secure data transmission and resilient control link architectures in civilian UAV operations [15]. These regulatory frameworks emphasize the need for standardized, lightweight security solutions that can be effectively deployed across diverse UAV platforms.

Contemporary UAV security research has predominantly focused on single-layer defensive mechanisms or narrow application domains, lacking comprehensive frameworks that address the full spectrum of security challenges across multiple communication layers [16]. While recent surveys have examined specific aspects such as physical layer security or blockchain applications in UAV networks, there remains a critical gap in understanding how lightweight cryptographic techniques, scalable key management strategies, and cross-layer security mechanisms can be integrated into unified security architectures [17,18]. This fragmentation limits the development of holistic security solutions capable of addressing the complex, multi-faceted threat landscape facing modern UAV deployments.

The rapid evolution of UAV swarm technology further complicates the security landscape. Modern swarm systems can coordinate hundreds of autonomous drones using distributed control algorithms and real-time communication protocols. These swarms leverage artificial intelligence and machine learning to navigate complex environments while maintaining synchronized operations, but they also present new attack vectors and scalability challenges for traditional security mechanisms [19]. Energy-efficient communication protocols, including non-orthogonal multiple access (NOMA) schemes, must be carefully designed to balance performance optimization with security requirements [20].

This comprehensive review addresses these critical gaps by providing an integrated analysis of secure communication techniques for UAV networks, with particular emphasis on lightweight encryption methods and efficient key management schemes tailored to resource-constrained aerial platforms. The review critically examines recent advances in symmetric and asymmetric cryptography suitable for constrained devices, evaluates the feasibility of decentralized trust infrastructures such as blockchain, and explores post-quantum solutions that anticipate future computational threats. Furthermore, this work expands the discussion to encompass security threats and defenses across multiple communication layers, from physical channel obfuscation to application-layer authentication protocols. Through a multilayer security framework and a performance analysis of lightweight cryptographic algorithms, this review offers practical guidance for researchers and system designers developing secure UAV architectures that meet real-world operational constraints and mission requirements.

To support this analysis, the paper is organized as follows. Section 2 provides background on UAV communication challenges and reviews existing survey studies in the field. Section 3 outlines the computational, energy, and storage constraints of UAV platforms and introduces key metrics for evaluating lightweight cryptographic solutions. Section 4 discusses the fundamental requirements and design trade-offs of lightweight cryptographic systems. Section 5 surveys a range of encryption techniques, including symmetric, asymmetric, and post-quantum cryptography, that are optimized for UAV deployment. Section 6 presents key management strategies, including static, dynamic, and hardware-assisted approaches. Section 7 introduces a multilayer security framework for UAV communication systems. Section 8 evaluates the suitability of these techniques across different UAV application scenarios. Section 9 highlights current limitations and outlines emerging research directions. Section 10 concludes the paper with a synthesis of findings and future outlook.

2. Background and Related Survey Studies

UAV communication security has become a prominent area of research due to the increasing reliance on drones for surveillance, delivery, and mission-critical operations. A substantial number of survey papers have explored security challenges by addressing threats, countermeasures, and architectural models for secure UAV networking. However, these surveys tend to examine isolated components such as detection techniques [2], physical-layer vulnerabilities [22], or specific cryptographic schemes [4,7], rather than offering a unified framework that spans the entire communication and control stack. This fragmented treatment limits the ability to develop end-to-end, secure, and efficient UAV systems tailored to real-world deployment constraints.

Table 1 offers a structured comparison of existing survey literature, mapping each study's contributions across six essential security dimensions: lightweight encryption (LWE), key management (KM), post-quantum cryptography (PQC), blockchain or PUF-based trust mechanisms (B/P), multilayer security frameworks (MLS), and application suitability (APS). Early foundational works, such as those by Abro et al. [2] and Yassine et al. [22], provide general overviews of UAV detection and privacy concerns, yet overlook critical emerging domains such as lightweight cryptography, quantum-safe encryption, and scalable key exchange. Similarly, studies like Patel et al. [4] emphasize efficient encryption algorithms but do not incorporate key management or trust frameworks.

Table 1. Comparison of related survey works on UAV security topics

Authors	Year	Focus	LWE	KM	PQC	B/P	MLS	APS
Abro et al. [2]	2022	UAV detection and security overview	✗	✗	✗	✗	✓	✓
Abdelaziz et al. [21]	2023	Comprehensive UAV cybersecurity analysis	✓	✓	✗	✓	✓	✓
Patel et al. [4]	2025	ASCON lightweight cryptography analysis	✓	✗	✗	✗	✗	✓
Yassine et al. [22]	2023	Security and privacy issues across four levels	✗	✗	✗	✗	✓	✓
Khan et al. [7]	2024	PQC for UAVs	✗	✓	✓	✗	✗	✓
Felix [23]	2023	Internet of Drones security challenges	✗	✗	✗	✓	✓	✓
Rugo et al. [24]	2022	UAVNet threats and countermeasures	✗	✗	✗	✓	✓	✓
Tang [25]	2021	Cybersecurity vulnerabilities for UAM	✗	✗	✗	✓	✓	✓
Mishra et al. [26]	2022	Systematic literature review on UAV security	✗	✗	✗	✗	✓	✓
Niyonsaba et al. [27]	2022	Systematic literature review on UAV security	✗	✗	✗	✗	✓	✓
Xia et al. [8]	2024	Kyber-based PQC authentication for UAVs	✗	✓	✓	✗	✗	✓
Hafeez et al. [10]	2024	Blockchain-based secure UAV communication (BETA-UAV)	✗	✓	✗	✓	✓	✓
Choi et al. [28]	2025	PUF-based secure key agreement for Internet of Drones	✗	✓	✓	✗	✓	✓
Tlili et al. [29]	2024	AI-enhanced UAV security and adaptive frameworks	✗	✗	✗	✗	✓	✓
Aissaoui et al. [30]	2024	Evaluation of PQC protocols for UAV networks	✗	✓	✓	✗	✗	✓
Gu et al. [31]	2021	UAV energy-efficient edge security with optimization	✓	✗	✗	✗	✓	✓
This Paper	2025	Secure communication in UAVs	✓	✓	✓	✓	✓	✓

Legend: ✓= Fully Covered, ✗= Not Covered. **Abbreviations: LWE:** Lightweight Encryption Techniques, **KM:** Key Management Schemes, **PQC:** Post-Quantum Cryptography, **B/P:** Blockchain/PUF Trust Mechanisms, **MLS:** Multilayer Security Framework, **APS:** Application Suitability.

Recent surveys have begun to bridge these gaps. For instance, Khan et al. [7], Xia et al. [8], and Aissaoui et al. [30] explore post-quantum cryptographic solutions suitable for UAV contexts. Hafeez et al. [10] and Choi et al. [28] integrate blockchain and PUF-based trust mechanisms to enhance authentication and key agreement. Abdelaziz et al. [21] and Rugo et al. [24] extend their coverage across multiple layers but still do not unify these elements into a cohesive framework. As summarized in Table 1, none of the reviewed works simultaneously address all six dimensions of UAV security, leaving a gap in the literature for holistic, future-proof solutions.

This review addresses the identified limitations by presenting a unified analysis of secure UAV communication technologies. It integrates lightweight encryption techniques, scalable key management methods, post-quantum secure protocols, and blockchain or PUF-based trust solutions within a multilayer security architecture. In addition, it evaluates these technologies against operational factors such as latency, computational overhead, and mission-specific constraints. By offering a comprehensive framework that spans cryptographic design to system-level deployment, this work aims to guide future research and implementation of secure, scalable, and resilient UAV communication networks.

3. Threat Landscape in Drone Networks

UAVs are increasingly used across diverse domains such as military reconnaissance, precision agriculture, logistics, and disaster response. These autonomous or semi-autonomous systems rely heavily on wireless communication to exchange commands and application data within dynamic and often decentralized network environments. However, UAVs are particularly vulnerable to cyberattacks due to their reliance on open-air interfaces, constrained energy and computational resources, and constant mobility. To contextualize these vulnerabilities, this section presents a threat analysis mapped to the OSI model, highlighting critical attacks such as eavesdropping, spoofing, jamming, and routing manipulation, and explores how contemporary cryptographic algorithms are employed to mitigate these risks in real-world UAV deployments.

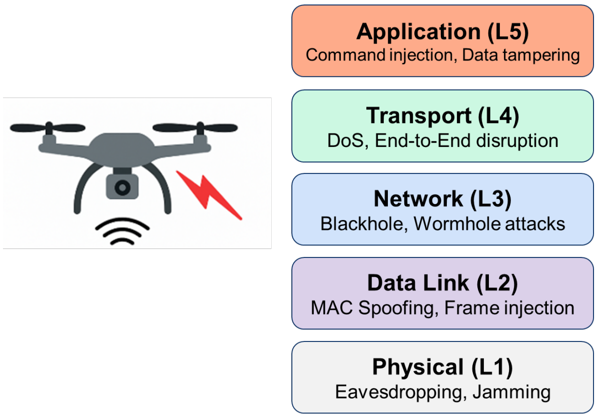
Application (L5)
Command injection, Data tampering
Transport (L4)
DoS, End-to-End disruption
Network (L3)
Blackhole, Wormhole attacks
Data Link (L2)
MAC Spoofing, Frame injection
Physical (L1)
Eavesdropping, Jamming

Figure 2. Security threats mapped to the five-layer OSI model for UAV networks.

As illustrated in Figure 3, each OSI layer is associated with specific threat types—ranging from physical-layer jamming to application-layer command injection. Correspondingly, Table 2 summarizes cryptographic countermeasures tailored to each layer, demonstrating the layered approach required for securing UAV communications.

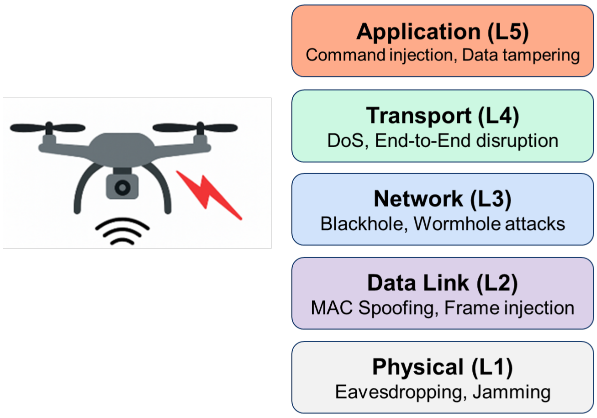
Application (L5)
Command injection, Data tampering
Transport (L4)
DoS, End-to-End disruption
Network (L3)
Blackhole, Wormhole attacks
Data Link (L2)
MAC Spoofing, Frame injection
Physical (L1)
Eavesdropping, Jamming

Figure 3. Security threats mapped to the five-layer OSI model for UAV networks.

Table 2. Cryptographic Countermeasures Across OSI Layers in UAV Networks

OSI Layer	Primary Threats	Cryptographic Defenses
Physical (L1)	Eavesdropping, Jamming	Trivium, Grain-128a, Frequency hopping, Quantum resilience
Data Link (L2)	MAC Spoofing, Frame Injection	ASCON, Hash chains, Synchronized MACs
Network (L3)	Sybil, Blackhole, Wormhole attacks	Blockchain routing, ECC, Kyber
Transport (L4)	DoS, End-to-End Disruption	AES-GCM, Ephemeral keys, Packet filtering
Application (L5)	Command Injection, Data Tampering, Access Violations	Kyber, ECC Signatures, RBAC, Secure APIs
Cross-Layer	Multi-layer Cascaded Failures	Blockchain + PUF, Secure boot, Dynamic key refresh

3.1. Threats at the Physical Layer

The physical layer (L1) governs radio frequency communication and is particularly susceptible to attacks due to its open and broadcast nature. Among the most critical threats at this layer are jamming and eavesdropping, both of which can severely disrupt mission-critical operations or compromise sensitive information. In surveillance and military contexts, adversaries may exploit these vulnerabilities to intercept or jam UAV communication links, potentially derailing operations or rendering drones uncontrollable [32,33].

Jamming involves the deliberate transmission of disruptive signals that degrade the UAV's communication channel, resulting in a denial of control or data loss. To counteract this, frequency hopping, spread-spectrum techniques, and cognitive radio approaches are employed to adapt transmission parameters in real time. Meanwhile, eavesdropping exploits the open nature of UAV broadcasts, allowing adversaries to passively intercept data streams. In response, physical layer security (PLS) methods such as artificial noise injection, cooperative jamming, and secure beamforming have been adopted to improve confidentiality without relying solely on upper-layer encryption [18,34].

The characteristics of aerial-to-ground (A2G) channels further exacerbate these vulnerabilities. High mobility, Doppler shifts, multipath fading, and variable line-of-sight conditions present challenges for both communication reliability and security. These dynamic propagation environments are difficult to secure through static cryptographic approaches and demand real-time adaptation [18]. Moreover, UAVs themselves can serve as mobile adversaries, launching eavesdropping or jamming attacks against terrestrial networks. Due to their elevation and maneuverability, malicious UAVs can maintain advantageous positions for longer durations, enhancing the impact of their attacks [35].

3.2. MAC and Data Link Layer Attacks

The Medium Access Control (MAC) and data link layers (L2) are fundamental to identity management, address resolution, and intra-network communication in UAV systems. These layers are particularly susceptible to spoofing, injection, and protocol-based attacks, which can severely disrupt communication integrity, cause misrouting, or lead to drone isolation and mission failure [36,37].

Spoofing attacks at the MAC layer involve an adversary falsifying a legitimate MAC address or control signal to impersonate a trusted device. In UAV networks, this can mislead drones into communicating with a malicious ground station or unauthorized peer. The consequences may include command hijacking, loss of situational awareness, or control redirection, potentially culminating in mid-air collision or disconnection from the swarm [38].

Frame injection attacks are a significant threat, wherein attackers craft and transmit unauthorized MAC frames to UAVs. These frames may include forged control commands, fake telemetry updates, or disarm signals that alter the UAV's behavior without detection. The risk is particularly high in autonomous or semi-autonomous missions, where UAVs depend on continuous and authenticated command streams [39]. Studies have demonstrated that flooding UAV networks with repeated spoofed control packets, such as ARP replies or disarm requests, can lead to denial-of-service (DoS) scenarios or force active drones to ground [40].

Data link layer vulnerabilities are further amplified by using lightweight, often unencrypted communication protocols like MAVLink. As MAVLink messages are typically transmitted in plaintext, attackers can eavesdrop on or alter control flows using simple packet sniffing tools. ARP spoofing and dictionary attacks on these links allow adversaries to gain full access to flight commands, location updates, and mission logs [39]. Replay attacks and message fabrication are also possible, especially when cryptographic protections are absent or improperly implemented.

Tactical data links used in military UAV operations also face threats. Attackers may exploit vulnerabilities in protocol headers, frequency allocation, or channel access patterns to inject falsified control messages or jam signal propagation. In some proposed architectures, the removal of MAC overhead in relay-based designs aims to optimize link reliability, but also opens new attack surfaces [41]. Such designs require careful threat modeling to avoid exposure to spoofing, flooding, and timing manipulation attacks.

Overall, attacks at the MAC and data link layers can cause message interception, redirection, impersonation, or channel disruption. These vulnerabilities form a critical attack surface in UAV communications and must be addressed in parallel with upper-layer defenses.

3.3. Network and Transport Layer Attacks

UAV networks are highly susceptible to sophisticated attacks at the network (L3) and transport (L4) layers, particularly in decentralized mission scenarios such as military swarms or search and rescue operations. These vulnerabilities are exacerbated by the inherent mobility, dynamic topologies, and wireless communication dependencies of UAV systems, making them attractive targets for attackers aiming to disrupt routing protocols or interfere with end-to-end data exchange [36,42].

At the network layer, some of the most disruptive attacks include Sybil, black hole, and wormhole attacks. In a Sybil attack, a malicious UAV or ground node assumes multiple false identities to manipulate routing paths and gain disproportionate influence over the network. Black hole attacks involve compromised nodes that falsely advertise optimal routes to attract and then drop all passing packets, effectively severing communication links. Wormhole attacks, on the other hand, tunnel packets between two distant malicious nodes to distort the network topology, bypass security checks, or redirect traffic through adversarial paths [36,43].

In collaborative threat scenarios, Sybil identities may be used to enable black hole nodes to bypass detection systems, or wormhole nodes may help propagate false routes more rapidly. Such multi-vector attacks are particularly concerning in UAV swarms, where synchronized communication and consistent routing are vital for mission success. The compromise of even a small subset of drones can lead to misdirection, isolation, or mission-wide disruption.

The transport layer is equally vulnerable. DoS attacks pose a significant threat by flooding UAV communication links, leading to loss of connectivity between aerial units and ground control stations. These attacks can overwhelm bandwidth-constrained links, degrade telemetry reporting, and interrupt the transmission of critical commands. Session hijacking at this layer allows attackers to intercept and manipulate session information, including control packets and encryption keys. Once hijacked, adversaries can inject falsified data, suppress legitimate commands, or seize full control of UAVs mid-flight [4,44].

In environments where UAVs operate with constrained energy and compute resources, these transport-layer threats are especially damaging. The lack of persistent session validation and the reliance on lightweight, low-latency protocols makes session-based exploits more feasible for attackers with modest capabilities. Furthermore, vulnerabilities in key exchange protocols or sequence number synchronization can open UAV communication systems to replay attacks and connection resets.

These L3 and L4 threats highlight the necessity of designing UAV networks that account for adversarial manipulation of both routing logic and transport-layer session integrity. Effective detection and response mechanisms must be layered into the network stack to address both individual and collaborative adversarial behaviors before they propagate across the fleet.

3.4. Application Layer Vulnerabilities

The application layer (L5) in UAV networks is a prime target for cyber-attacks due to its role in facilitating mission-critical tasks such as remote command execution, software updates, mission planning, and data offloading. These operations typically involve communication between UAVs and cloud services or ground control stations, introducing multiple vectors for application-layer compromise [36,37].

One of the most pressing threats is unauthorized access to cloud-connected UAV services. When authentication mechanisms or access control protocols are insufficient, adversaries may intercept or manipulate mission data, gain control over drone navigation, or extract sensitive information from flight logs. These vulnerabilities are especially prevalent in multi-UAV systems that lack granular access restrictions or encrypt communication inconsistently [45].

Software update processes also present significant risks. UAVs commonly perform over-the-air (OTA) firmware and software updates, which, if not properly authenticated, can be hijacked by attackers. In such scenarios, malicious payloads may be inserted during the update process, granting adversaries persistent access to UAV systems or allowing them to install backdoors for future exploitation [46,47].

Command injection attacks represent another critical threat. These attacks involve the manipulation of application interfaces to reroute drones, alter payload delivery destinations, or disrupt mission objectives. For example, in logistics operations, attackers could exploit unsecured control channels to redirect a stolen UAV to an unauthorized location, leading to physical asset loss or theft [48].

In many UAV deployments, sensitive credentials such as FTP login details or update server keys are stored in plaintext within application-level code or configuration files. This creates a vulnerability in which attackers can extract these credentials to gain persistent control over the UAV, exfiltrate stored data, or intercept telemetry streams. Plaintext storage and hardcoded keys also simplify offline credential guessing and replay attacks.

Together, these application-layer threats represent a high-impact attack surface, particularly in commercial and civilian UAV operations that interface with cloud infrastructure, third-party APIs, and remote configuration systems. As the reliance on remote UAV management continues to increase, addressing these vulnerabilities is essential for ensuring operational trust and mission assurance.

3.5. Cross-Layer Attack Vectors

UAV networks are increasingly exposed to cross-layer attacks, in which adversaries exploit interdependencies between protocol layers to amplify the scope and severity of their disruption. Unlike conventional single-layer threats, cross-layer attacks are characterized by their ability to trigger cascading failures across multiple layers of the communication stack, ultimately compromising mission-critical functionality [24,49].

One prominent example involves a jamming attack launched at the physical layer (L1), which disrupts wireless signal integrity and impedes packet transmission. This seemingly localized interference can propagate to the network layer (L3), where it prevents timely updates of routing tables or neighbor discovery processes. In turn, the disrupted network layer can cause malfunctions at the application layer (L5), such as the failure of real-time video streaming or interruption of command-and-control channels. These cascading effects are particularly dangerous in multi-UAV swarms, where node interdependence and tight synchronization are essential to maintaining formation, coverage, and cooperative behavior [34].

Cross-layer threats are further exacerbated by the operational constraints of UAVs, including mobility, limited energy, and dynamic topologies. In such environments, attackers may leverage time-synchronized or coordinated strategies that simultaneously target multiple layers, leading to complex failure patterns that are difficult to detect using traditional, layer-specific intrusion detection systems. For instance, adversaries may combine physical-layer jamming with transport-layer flooding or spoofing to overload processing pipelines and disrupt system state consistency [36].

Compromises at lower layers can also undermine higher-level trust and authentication mechanisms. A breach of link-layer synchronization may degrade encryption performance or create misalignment in session management protocols. Similarly, manipulation of timing information across MAC and network layers can enable routing misdirection or replay of sensitive telemetry data, thus undermining situational awareness and UAV coordination.

These multi-faceted threats illustrate that cross-layer attack vectors are not only more disruptive but also harder to mitigate, particularly in autonomous or semi-autonomous UAV deployments. Given their ability to mask indicators across layers, cross-layer attacks challenge the assumptions of modular defense frameworks and demand unified monitoring and anomaly correlation across the protocol stack.

To consolidate the insights presented across the OSI layers, Table 3 provides a high-level summary of the threat landscape in UAV networks. It maps each layer to its dominant vulnerabilities, common attack vectors, and the corresponding impact on UAV operations. This overview not only highlights the multidimensional nature of cyber threats but also underscores the necessity of a layered and context-aware defense strategy in UAV system design.

Table 3. Summary of Threat Landscape Across OSI Layers in UAV Networks

OSI Layer	Primary Threats	Common Attack Vectors	Impact on UAV Operations
Physical (L1)	Jamming, Eavesdropping	RF interference, passive sniffing	Communication loss, mission disruption, control hijack
Data Link (L2)	MAC spoofing, Frame injection	ARP spoofing, fake control packets, DoS floods	Identity theft, drone misrouting, premature grounding
Network (L3)	Sybil, Blackhole, Wormhole	Fake route advertisement, malicious relay tunnels	Packet loss, routing failure, drone isolation
Transport (L4)	Session hijacking, DoS	TCP flooding, replay attacks, connection reset	Command interception, session loss, delayed control
Application (L5)	Command injection, Update tampering, Credential theft	API misuse, OTA update spoofing, plaintext key access	UAV capture, data exfiltration, remote control takeover
Cross-Layer	Coordinated disruption across L1–L5	Synchronized jamming + flooding, timing manipulation	Cascade failure, swarm desynchronization, stealth attack masking

Securing UAV communication against the broad spectrum of threats identified across the OSI model requires the integration of robust cryptographic mechanisms. However, conventional encryption protocols often exceed the computational and energy capabilities of UAV platforms, especially in swarm-based or long-duration deployments. This necessitates a shift toward cryptographic techniques specifically optimized for constrained environments. The following section explores the core requirements, design principles, and evaluation metrics for lightweight cryptography, which has emerged as a viable solution for achieving secure, real-time communication in UAV systems under resource limitations.

4. Overview of Lightweight Cryptographic Requirements

The increasing deployment of digital systems in resource-constrained environments, such as UAVs, IoT devices, and embedded platforms, has increased the demand for cryptographic solutions that are both secure and efficient. Traditional encryption algorithms often prove unsuitable for these platforms due to limitations in memory, processing speed, throughput, energy consumption, and implementation cost. To overcome these challenges, lightweight cryptography has emerged as a promising approach, offering an optimal balance between security and resource efficiency, particularly for real-time and low-power operations [50,51].

A foundational consideration in this domain is the characterization of what constitutes "lightweight" cryptography. Although such schemes are typically simpler and faster than conventional algorithms, these benefits may entail reduced performance margins or lower cryptographic strength [50,51]. Accordingly, a clear understanding of the core design requirements is essential for evaluating and selecting algorithms suitable for UAV applications.

The literature consistently highlights four principal metrics for lightweight cryptographic systems: (1) *computational complexity*, defined by the number of logical operations required for encryption or decryption [52]; (2) *memory footprint*, which encompasses both code size (ROM) and working memory (RAM) [53]; (3) *energy consumption*, which is critical for battery-operated or energy-harvesting UAVs [54,55]; and (4) *latency*, the time needed to compute a single encryption or decryption block, which is particularly important in time-sensitive missions [53,56].

To address these requirements, a diverse set of lightweight cryptographic primitives has been developed. Prominent among them are lightweight block ciphers such as PRESENT [57], SPECK, and SIMON [58,59], which are optimized for compact implementations on constrained devices. Similarly, lightweight stream ciphers including Trivium [60] and Grain [61] provide rapid, low-overhead encryption suitable for continuous data streams. For public-key operations, Elliptic Curve Cryptography (ECC) [62,63] remains a leading choice due to its high security-to-resource ratio and reduced key sizes compared to RSA or DSA [64].

The remainder of this section is structured as follows: Section 4.1 explores the computational and energy constraints inherent to UAV platforms. Section 4.2 outlines the standard evaluation metrics for lightweight cryptography, and Section 4.3 discusses design principles and performance-security trade-offs that influence algorithm selection.

4.1. Resource Constraints in UAV Platforms

Recent advancements in UAV technologies have led to their widespread adoption across numerous public and industrial sectors. UAVs are now deployed in diverse domains, including surveillance [65], environmental monitoring [66], disaster response [67], delivery services [68,69], military operations [70], traffic monitoring [71], and precision agriculture [72]. Each application imposes unique demands on UAV platforms, often under stringent resource constraints. For instance, UAVs used in real-time video surveillance or disaster response typically capture and transmit high-resolution images or video, requiring low-latency communication and fast data processing, all while operating on limited battery power [73,74]. In contrast, agricultural UAVs conducting periodic mapping may prioritize data storage and secure network connectivity over computational speed [75]. For delivery UAVs, energy efficiency is critical for maximizing flight range, while stable communication ensures reliable navigation and real-time tracking, particularly in dynamic environments such as urban areas or traffic congestion [76].

Despite their growing utility, UAVs are inherently constrained by limited energy, processing capability, memory, latency tolerance, and communication bandwidth. Energy efficiency is particularly challenging, as UAVs are typically battery-powered and may not have opportunities to recharge during extended missions [77]. Power-intensive operations significantly reduce flight time. Most UAVs rely on low-power microcontrollers that are not suitable for computationally demanding tasks. Memory is also limited, particularly in small and nano-scale UAVs, restricting the deployment of large datasets or advanced algorithms. Furthermore, many UAV applications require on-board, real-time processing and low-latency response, especially in mission-critical operations such as object tracking or autonomous navigation [78]. Cryptographic functions and control algorithms must therefore be computationally lightweight to avoid introducing delays. Communication bandwidth can also be limited or highly variable, requiring compact and efficient encryption protocols. These challenges are especially pronounced in lightweight UAVs, which are chosen for their mobility and ease of deployment, but often lack advanced hardware support. Consequently, both hardware and software components must be optimized to meet operational demands without compromising system performance or mission success.

Table 4 highlights selected studies that emphasize various resource limitations in UAV systems.

Table 4. Sample of studies addressing various UAV resource constraints

		Constraint Type					
Reference	Application	Energy	Communication	Latency	Memory	CPU Power	Summary
[79]	General	✓	✗	✗	✗	✗	Classifies existing energy-efficient technologies for UAVs
[80]	General	✓	✗	✗	✗	✗	Classifies various energy optimization techniques and algorithms
[81]	General	✓	✗	✗	✗	✗	Reviews the Energy Consumption Models in different flight scenarios
[82]	General	✓	✓	✗	✗	✗	Characteristics of UAV communication networks and their issues
[83]	General	✗	✓	✓	✗	✗	Investigates the blocklengths and UAV trajectory optimization
[84]	General	✓	✓	✓	✗	✗	A joint optimization of bandwidth, transmit power, and trajectory.
[85]	General	✗	✗	✓	✓	✗	A methodology for evaluating runtime memory, and timing.
[86]	Multimedia	✗	✓	✓	✗	✓	A framework to maximize the amount of acquired and uploaded data
[87]	Tracking, Mapping	✓	✗	✗	✗	✓	An approach to balance communication and computation energy
[88]	Disaster	✓	✗	✗	✗	✓	A model to maximize computational efficiency under energy constraints
[89]	Surveillance	✗	✗	✓	✓	✗	Minimize decision-making latency considering UAV mobility

4.2. Definition and Metrics of Lightweight Cryptography

To assess the suitability of lightweight cryptographic algorithms for constrained platforms, it is necessary to evaluate not only their security strength but also their performance under limited computational and energy budgets. Figure 4 summarizes key operational challenges and the corresponding metrics used to evaluate algorithm efficiency.

A primary consideration is hardware cost, which is often expressed using metrics such as silicon area, slice usage, area per bit [90], or gate equivalents (GE) [91,92]. GE represents the area needed to implement an algorithm on an integrated circuit and serves as a proxy for cost and complexity.

Latency is another essential metric, representing the time taken from the start of an operation to the generation of output [91]. It can be measured in clock cycles per operation [93,94], peak execution time, or average execution time [4,95]. For evaluating throughput, which measures the volume of data processed per unit time, hardware performance is typically evaluated at 100 kHz, while software implementations use 4 MHz CPU frequencies [96,97].

In battery-powered systems, energy and power consumption are critical. Metrics such as energy per bit [90,92,98] or energy per operation [96] directly impact the longevity of UAV missions.

Memory usage is also a key constraint. This includes RAM for runtime operations and ROM for storing constants, such as S-boxes or precomputed keys [91,95]. Evaluation metrics such as code size, key size, and block size are commonly used to estimate storage requirements [45,96].

Given the limited processing capabilities of UAV hardware, computational efficiency must also be assessed. Metrics such as CPU cycles per operation [98], CPU utilization percentage [45], and CPU execution time [95] provide a quantitative basis for comparison.

In networked environments, communication overhead must be minimized. Metrics such as message size [93,98], number of transmissions [98], transfer speed [45], and bandwidth utilization [95] help assess the communication efficiency of cryptographic protocols.

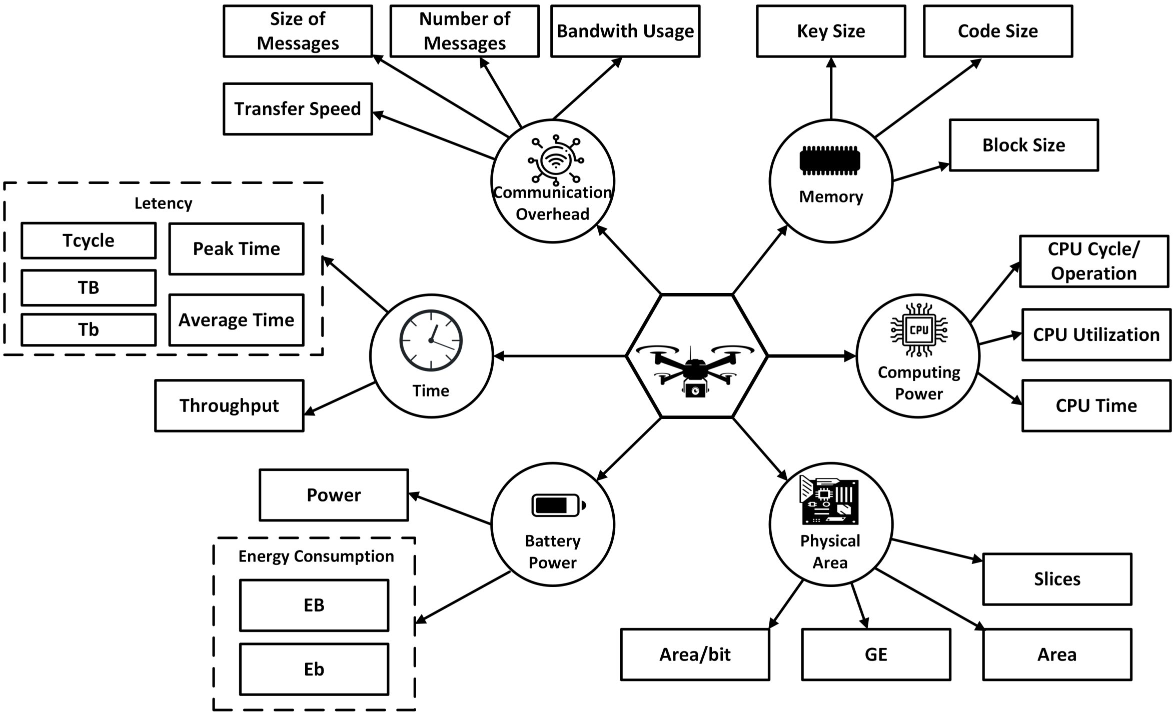

Figure 4. Key challenges in lightweight cryptography and the corresponding evaluation metrics they impose

While reducing resource consumption, cryptographic algorithms must continue to meet essential security requirements. Standard internal structures used to achieve this include Substitution-Permutation Networks (SPN), Feistel Networks (FN), Generalized Feistel Networks (GFN), Add-Rotate-XOR (ARX), Nonlinear Feedback Shift Registers (NLFSR), and hybrid models. Security is typically quantified in terms of minimum strength (in bits) and resistance to side-channel and fault injection attacks [95,96].

Tables 5 and 6 summarize key evaluation metrics and studies that have applied them.

Table 5. Key metrics for evaluating lightweight cryptography algorithms.

Metric	Definition	Unit
CPU Utilization	The percentage of CPU resources used by a process [45].	percentage
CPU Time	The amount of time the CPU spends executing a process [95].	ms
Throughput	The rate of producing new outputs (e.g., authentication tags or ciphertext) and obtained by Total data processed divided by the total time taken to process it [4,91].	bits/second
Key Size	The length of the cryptographic key (e.g., 64-bit, 128-bit) [53].	bytes
Code Size	The amount of memory required for algorithm's code [53].	bytes
Area/bit	Ratio of the design area over the block size [90].	μm^2
EB	Energy to encrypt one block [90].	joules
Eb	Energy to encrypt a single text bit [53,90].	joules
Power	The amount of power required by the circuit to process the algorithm [96].	µW
TB	Time to encrypt one block [90].	ms
Tb	Time to encrypt a single text bit [90].	ms
Tcycle	Cycle time [90].	ms
Peak Execution Time	The maximum execution time observed across all instances of a specific process [4].	ms
Average Execution Time	The average execution time measured over all instances of a specific process [4].	ms
Transfer Speed	The number of packets transmitted per second [45].	packets/s
Number of Messages	Total number of messages exchanged among the UAV, control server, and user [98].	count
Message Size	Average size of messages sent during a process [93,98].	bytes

Table 6. Sample of selected studies and the metrics they applied to evaluate lightweight cryptographic methods.

Reference	Time per Operation	Peak Execution Times	Average Execution Times	Throughput	Memory Usage	Transfer Speed	CPU Utilization	Number of Messages	Size of Messages	Energy Consumption	CPU Time
[4]		✓	✓	✓							
[95]		✓									✓
[45]					✓	✓	✓				
[98]			✓					✓	✓	✓	✓
[93]	✓								✓		✓
[94]	✓		✓			✓		✓	✓		

NIST's [91] Lightweight Cryptography Project serves as a standard reference to evaluate various algorithms. [99] was the first to use both NIST and ISO standards as benchmarks for selecting optimal lightweight authentication cryptographic ciphers. This study develops evaluation metrics and criteria based on various requirements and then applies hybrid multi-criteria decision-making (MCDM) methods, such as CRITIC and TOPSIS, to objectively weight the criteria and rank the alternatives. Therefore, it provides a valuable benchmark for the assessment and ranking of lightweight cryptographic ciphers.

4.3. Design Principles: Trade-offs and Optimization

Designing lightweight cryptographic algorithms for UAVs involves balancing security requirements with constraints on energy, memory, and computational power. As discussed in previous sections, these limitations restrict the use of conventional cryptographic approaches. Therefore, designers must evaluate trade-offs between performance, cost, and security to create algorithms that meet operational demands without overburdening system resources [90,100].

While lightweight cryptographic algorithms are expected to be simpler and faster than conventional schemes, they may offer reduced security margins [50]. Figure 5 illustrates the typical trade-offs in designing such algorithms. Enhancing security through longer keys, additional rounds, or added integrity checks increases computational demand and latency. High-speed encryption may require additional memory for storing intermediate values or lookup tables. Conversely, memory-optimized schemes reduce speed due to serialized processing. Parallelization improves throughput but consumes more area and power. Similarly, minimizing latency through higher clock rates increases energy consumption. In hardware implementations, higher throughput often results in increased gate count, while minimizing area generally reduces performance.

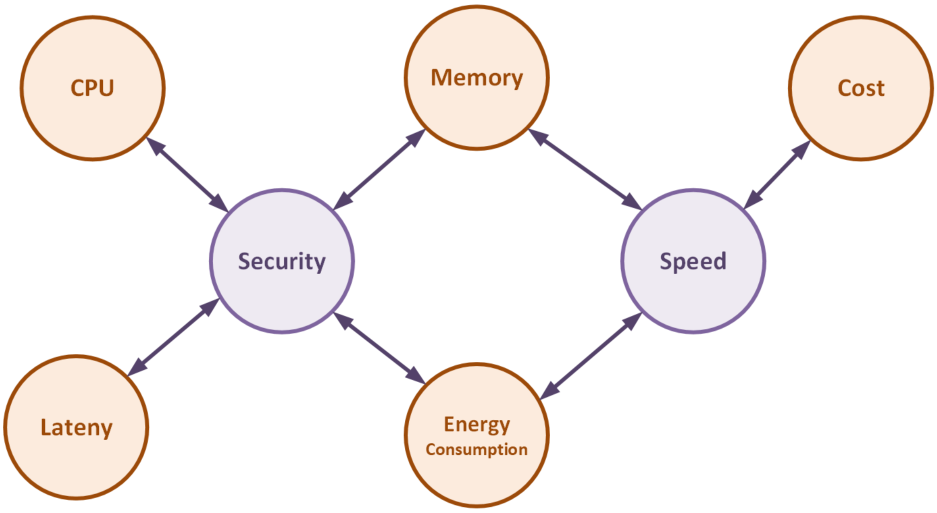

Figure 5. Trade-offs involved in designing and implementing lightweight cryptographic algorithms.

Several strategies are used to optimize lightweight cryptographic designs:

- Algorithmic simplification by reducing rounds or using basic operations [58].
- Bit-serial processing to minimize hardware complexity [57].
- Substitution-Permutation Networks (SPNs) optimized for hardware efficiency [57].
- Platform-specific customization based on target architectures (e.g., 8-bit or 32-bit processors).

These approaches help ensure acceptable security while remaining deployable on constrained hardware platforms. The choice of design technique is often guided by the application context, requiring careful trade-off decisions among competing metrics.

5. Survey of Lightweight Encryption Techniques

Building upon the cryptographic requirements, performance metrics, and design considerations presented in Section 4, this section provides a structured survey of lightweight encryption techniques tailored for UAV platforms. These techniques are designed to meet the stringent resource constraints of UAVs while ensuring essential security services such as confidentiality, integrity, and authentication [101].

UAVs operate in dynamic and often adversarial environments, where reliable and secure communication is critical to mission success. Due to limited processing power, energy reserves, and onboard memory, traditional encryption schemes are often impractical. In response, lightweight cryptography has emerged as a viable solution for protecting UAV data exchanges without imposing significant performance overhead.

To secure UAV communications, a comprehensive suite of cryptographic services must be in place. As shown in Figure 6, the core services include confidentiality, integrity, authentication, nonrepudiation, and availability. Additionally, UAV systems must be resilient against targeted threats such as node capture, impersonation, data duplication, and forensic attacks. Properly selected lightweight cryptographic primitives form the basis for defending against such vulnerabilities [64,102].

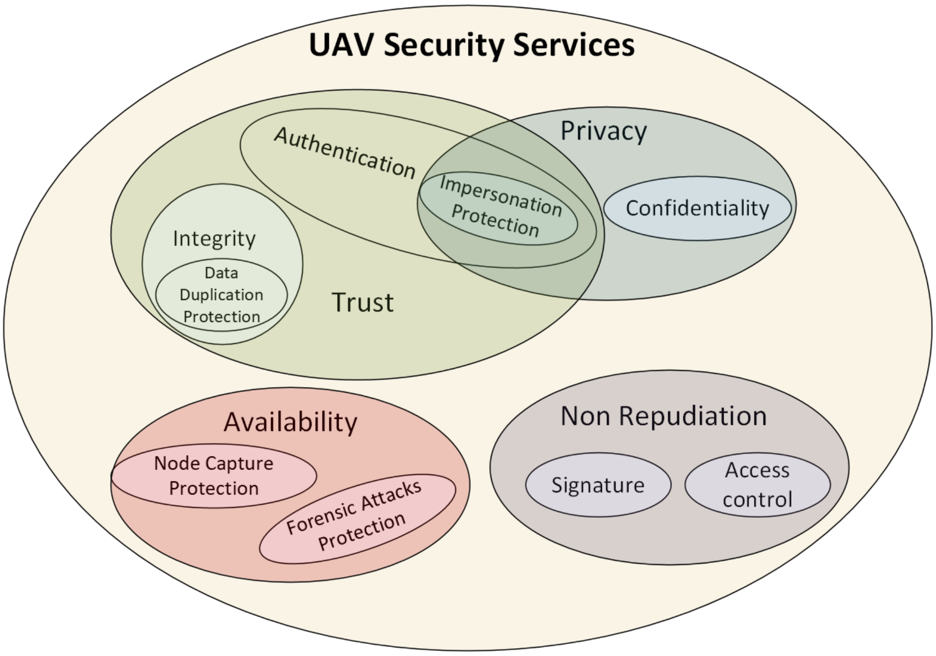

Figure 6. Most important security services required in UAVs

At the core of cryptographic security lies the use of keyed algorithms, which rely on secret values for encryption and decryption. These algorithms fall into two broad categories: symmetric key cryptography and asymmetric key cryptography. Symmetric algorithms use a single shared key for both encryption and decryption, making them computationally efficient and well-suited for constrained platforms. They support confidentiality, data integrity, and authentication, although secure key distribution remains a challenge. This limitation is often addressed by pre-sharing keys through trusted mechanisms. In contrast, asymmetric algorithms use separate public and private keys, offering greater flexibility for tasks such as digital signatures and key exchange, but at the cost of higher computational complexity [64,96].

In symmetric lightweight cryptography, a range of primitives has been developed to achieve specific security objectives while minimizing resource usage. These primitives are tailored for constrained environments like UAV platforms, where computational and energy efficiency is critical. As illustrated in Figure 7, the primary categories include:

- *Lightweight Block Ciphers (LWBC)*: Designed for encrypting fixed-size blocks of data with minimal overhead.
- *Lightweight Stream Ciphers (LWSC)*: Operate on continuous data streams and are well-suited for real-time encryption tasks.
- *Lightweight Hash Functions (LWHF)*: Ensure data integrity and are commonly used in digital signature schemes and authentication protocols.
- *Lightweight Message Authentication Codes (MACs)*: Authenticate messages and verify their origin using minimal computational resources.
- *Lightweight Authenticated Encryption (AE)*: Provide combined confidentiality and integrity in a single operation [91,102,103].

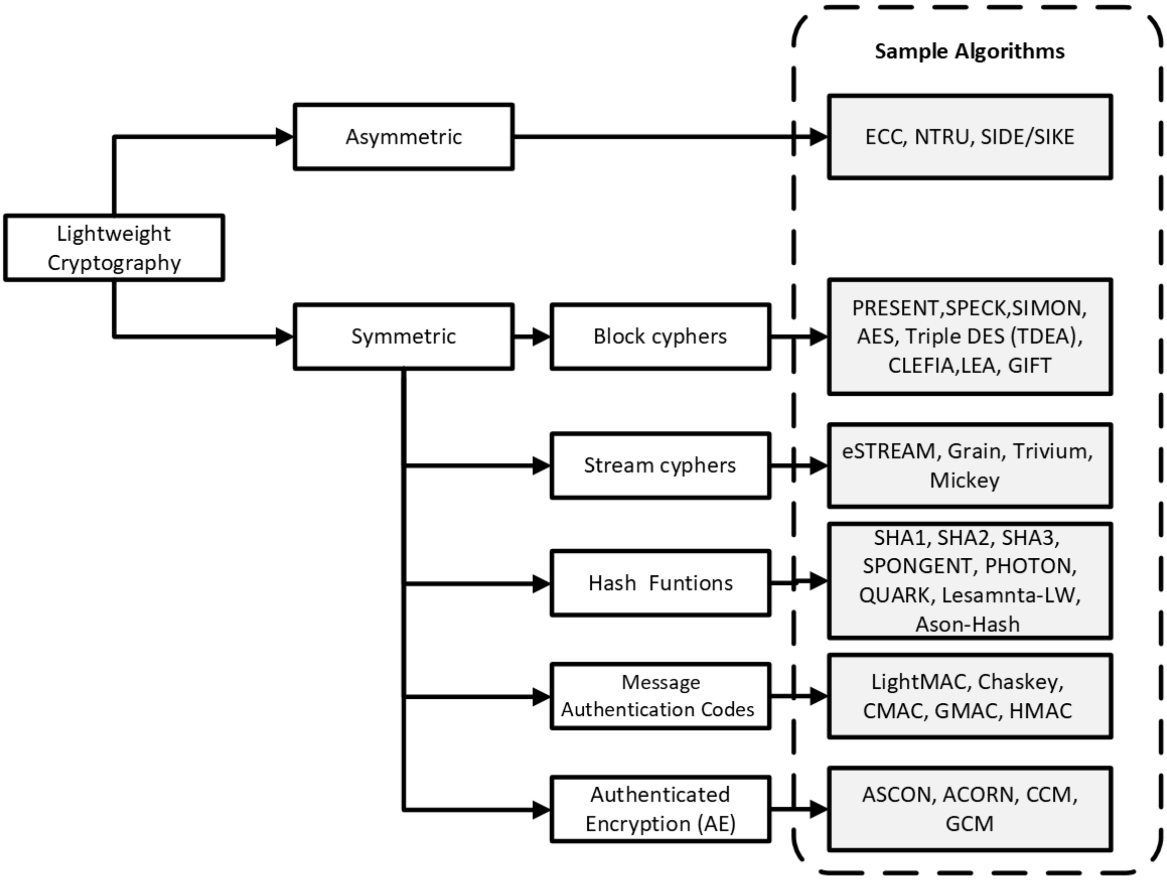
Sample Algorithms
Lightweight Cryptography
Asymmetric
ECC, NTRU, SIDE/SIKE
Symmetric
Block cyphers
PRESENT,SPECK,SIMON, AES, Triple DES (TDEA), CLEFIA,LEA, GIFT
Stream cyphers
eSTREAM, Grain, Trivium, Mickey
Hash Funtions
SHA1, SHA2, SHA3, SPONGENT, PHOTON, QUARK, Lesamnta-LW, Ason-Hash
Message Authentication Codes
LightMAC, Chaskey, CMAC, GMAC, HMAC
Authenticated Encryption (AE)
ASCON, ACORN, CCM, GCM

Figure 7. Categories of lightweight cryptographic primitives

5.1. Lightweight Block Ciphers

Block cipher cryptography is grounded in two core principles: confusion and diffusion. Confusion aims to obscure the relationship between the ciphertext and the encryption key, typically achieved through substitution operations such as S-boxes. Diffusion, on the other hand, spreads the influence of individual plaintext bits across the ciphertext using permutation mechanisms [53,96,104,105]. In a block cipher, encryption and decryption are performed on fixed-size data blocks, generally 64 bits or larger [96].

Figure 8 categorizes block ciphers based on their internal structures, including Substitution-Permutation Networks (SPNs), Feistel Networks, Generalized Feistel Networks (GFNs), Add-Rotate-XOR (ARX) architectures, Nonlinear Feedback Shift Register (NLFSR)-based designs, and hybrid models. Examples of widely used ciphers within these categories include AES (SPN), DES (Feistel), TWINE (GFN), IDEA (ARX), KeeLoq (NLFSR-based), and the Hummingbird family (hybrid) [53,96].

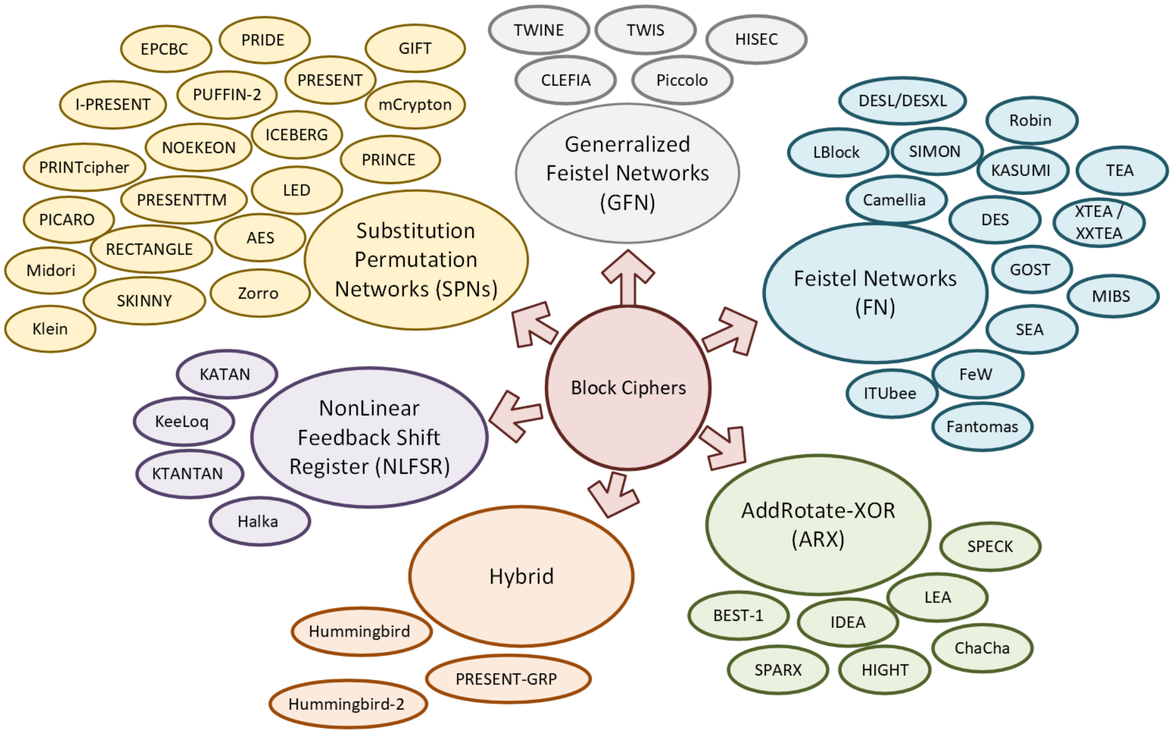

Figure 8. Basic types of block ciphers based on internal structure

Each architectural model presents unique design advantages and trade-offs. SPNs apply iterative substitution and permutation layers, which facilitate efficient serialization and minimal datapath widths [53,96]. A notable example is PRESENT [57], a highly compact SPN cipher developed for embedded systems. It incorporates 31 lightweight rounds, each consisting of a substitution layer, a permutation layer, and round key integration [106].

Feistel networks operate by dividing input data into halves, applying a round function to one half, and recombining the result with the other half through XOR operations. While this structure increases hardware cost slightly, it simplifies decryption by mirroring the encryption process. The Generalized Feistel Network (GFN) extends this model by partitioning input into multiple sub-blocks, enhancing flexibility and allowing for diverse round functions and shifting patterns.

ARX-based ciphers utilize only modular addition, bitwise rotation, and XOR operations. These primitives enable fast and compact implementations but are generally less scrutinized in terms of cryptanalytic robustness. AES-128, for instance, has been adapted into a compact software form that uses processor registers to store the internal state and the mix column step, while storing the key in RAM. This implementation requires approximately 1659 bytes of ROM and 4557 cycles to encrypt a 128-bit block [53,107].

NLFSR-based ciphers, which originate from stream cipher structures, are predominantly used in hardware implementations. Their security depends on nonlinear feedback shift register configurations commonly analyzed in stream cipher design. Hybrid architectures combine features from multiple cipher structures to optimize specific performance or security metrics. The effectiveness of these designs is determined by the selection and integration of component mechanisms [53,96].

5.2. Stream Ciphers and Real-Time Encryption

Stream ciphers are symmetric encryption algorithms that process data as a continuous stream, encrypting bit by bit or word by word rather than in fixed-size blocks. This design enables high-speed and low-latency encryption, making stream ciphers particularly well-suited for resource-constrained environments. Unlike block ciphers, which leverage both confusion and diffusion properties, stream ciphers primarily employ confusion through simple operations such as bitwise XOR [96]. As a result, they are generally less complex, easier to implement in hardware, and more efficient in scenarios where processing power and energy are limited.

Lightweight stream ciphers typically generate keystreams using structures such as Linear Feedback Shift Registers (LFSRs) or Nonlinear Feedback Shift Registers (NLFSRs). These designs support high-speed and low-power operations, making them ideal for use in wireless networks and mobile platforms, including UAVs [108].

The theoretical foundation of stream ciphers is based on the one-time pad (OTP) model, which offers perfect secrecy when a truly random keystream of the same length as the plaintext is used [109]. However, the challenges of generating and securely distributing such keystreams have led to the adoption of pseudorandom keystream generators. In lightweight stream ciphers, encryption is performed by XORing the plaintext with a pseudorandom keystream derived from a secret key and initialization vector (IV). While this method offers efficiency, it also introduces vulnerabilities such as key reuse and synchronization issues, necessitating robust key and IV management strategies. Despite these challenges, stream ciphers remain a strong candidate for real-time encryption in UAV systems, where data is transmitted continuously and low latency is essential.

To promote the development of secure and efficient stream ciphers, the eSTREAM project was launched under the European Network of Excellence in Cryptology II [110]. The project evaluated 34 candidate algorithms and selected a portfolio of ciphers suitable for deployment in both software and hardware-constrained environments. Two implementation profiles were defined: Profile 1 targeted high-throughput software ciphers, including Salsa20/12, Rabbit, LEX, and SOSEMANUK; Profile 2 focused on compact hardware implementations, featuring Grain, Trivium, and MICKEY 2.0. These ciphers were benchmarked on microcontroller platforms and extensively analyzed in the context of wireless sensor networks. While some candidates were disqualified due to security vulnerabilities, the remaining finalists demonstrated resilience against all known attacks exceeding brute-force complexity [109].

Among the selected ciphers, Trivium and Grain are notable for their lightweight hardware design and strong efficiency. Trivium [60], standardized under ISO/IEC 29192-3:2012, is a synchronous, bit-oriented cipher utilizing 80-bit keys and IVs. It employs three interdependent shift registers to achieve nonlinearity, maintaining a minimal hardware footprint of approximately 749 gate equivalents (GE), while also offering reasonable software performance. However, its simplicity makes it susceptible to certain fault injection attacks.

Grain [61] combines both LFSR and NFSR components to generate a secure keystream. It features a bit-oriented architecture and produces between 1 and 32 bits per cycle, depending on configuration. Grain-128a, an enhanced version, supports 128-bit keys and allows for adjustable authentication tag sizes, making it suitable for applications requiring both confidentiality and integrity [108,109].

Salsa20 [111], a Profile 1 finalist, was developed for efficient software encryption and uses modular addition, XOR, and bit rotation operations. It supports 256-bit keys and 128-bit IVs, with variants such as Salsa20/8, Salsa20/12, and Salsa20/20 offering trade-offs between performance and security. Although it performs well in software, its relatively large hardware footprint limits its applicability in highly constrained systems. ChaCha [112], a variant of Salsa20, enhances diffusion and cryptographic strength and is widely adopted due to its speed and robustness.

MICKEY 2.0 (Mutual Irregular Clocking KEYstream generator) employs irregularly clocked Galois LFSRs and NFSRs to improve keystream randomness. It supports 80-bit keys and variable IVs, offering secure encryption with a higher implementation complexity of over 3000 GE. The extended version, MICKEY-128 2.0, supports larger keys and improved throughput but has also shown vulnerability to related-key and fault injection attacks [108]. Despite such limitations, these ciphers continue to serve as reference benchmarks for real-time secure communication in UAV networks and other resource-limited systems.

5.3. Asymmetric Encryption

Asymmetric cryptography, also known as Public Key Cryptography (PKC), plays a critical role in securing communication within networked systems such as UAVs. Unlike symmetric encryption, which uses a single shared key, PKC employs a key pair consisting of a public key for encryption and a private key for decryption. These keys are generated using mathematical functions designed to make it computationally infeasible to derive the private key from the public one [64]. This cryptographic paradigm supports essential security services, including confidentiality, data integrity, authentication, non-repudiation, availability, and access control [64,96]. In practical implementations, a sender encrypts data using the recipient's public key, while digital signatures are created with the sender's private key and verified using the corresponding public key [96].

Despite its robustness, asymmetric cryptography presents challenges in resource-constrained environments. Operations often involve large key sizes and computationally intensive arithmetic over algebraic structures, with operands reaching lengths of thousands of bits. These requirements can strain the limited processing, memory, and energy resources of UAV platforms [64,113].

Among existing PKC schemes, Elliptic Curve Cryptography (ECC) is widely considered the most suitable for constrained systems. ECC achieves comparable security to classical methods such as RSA, while requiring significantly smaller key sizes, reduced memory footprint, and lower computational load. It is commonly adopted for key exchange, digital signature generation, and authentication in lightweight environments, and is standardized under ISO/IEC 29192 [113].

The efficiency of ECC in constrained settings is enabled through implementation-specific optimizations. Although ECC itself is not inherently lightweight, lightweight elliptic curve cryptography (ECLC) leverages design decisions across protocol, algorithm, architecture, and circuit levels to meet performance and energy constraints. These optimizations include using efficient point representations (such as projective or mixed coordinates), selecting specialized curve models (including Koblitz, Edwards [114], and Montgomery curves [115]), and tailoring implementations to the underlying hardware [64].

A notable extension of ECC in the lightweight cryptography domain is Identity-Based Encryption (IBE), which simplifies key management by deriving public keys from unique identifiers (e.g., email addresses). In contrast to RSA, where key pairs are generated independently, IBE enables a public key to be deterministically generated from an identity string, while the corresponding private key is issued by a trusted authority. The Boneh-Franklin IBE scheme, one of the earliest and most influential constructions, employs elliptic curve cryptography and uses Weil pairing to achieve chosen ciphertext security under the elliptic curve variant of the Computational Diffie-Hellman assumption [116]. To improve resilience and decentralization, this scheme can also support threshold cryptography for distributed key generation without requiring a centralized master key.

To further adapt IBE for resource-limited platforms such as UAVs, lightweight variants like IBE-Lite have been introduced [117]. IBE-Lite retains the core functionality of identity-based public key derivation and secure private key distribution while minimizing computational and memory demands. Built upon the ECC framework, it provides a practical and secure public key infrastructure alternative for embedded and low-power environments.

5.4. Post-Quantum Cryptography

Classical cryptographic systems are built on the computational hardness of problems such as the Integer Factorization Problem (IFP), the Discrete Logarithm Problem (DLP), and the Elliptic Curve Discrete Logarithm Problem (ECDLP). However, the development of quantum computing poses a significant threat to these systems. Algorithms such as Shor's and Grover's, when implemented on a sufficiently powerful quantum computer, can efficiently break traditional encryption and key exchange mechanisms. In response, the field of post-quantum cryptography (PQC)—also referred to as quantum-resistant or quantum-safe cryptography—has emerged as a critical area of research to ensure secure communication in the quantum era [118,119].

As illustrated in Figure 9, PQC encompasses five primary categories of cryptographic schemes: code-based, lattice-based, hash-based, isogeny-based, and multivariate-based cryptosystems.

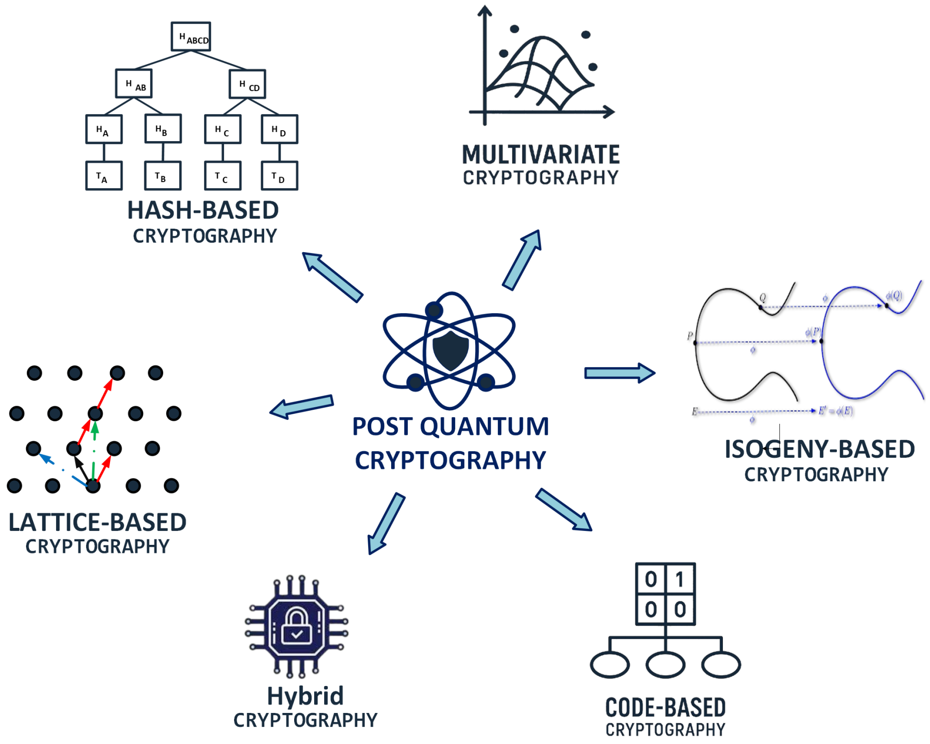

Figure 9. Different categories of post-quantum cryptographic methods

To identify viable quantum-resistant algorithms, the National Institute of Standards and Technology (NIST) launched a multi-round standardization effort. The process began in 2017 with 69 algorithm submissions. Through successive rounds of evaluation—focused on robustness, performance, and implementation feasibility—a subset of algorithms advanced to the final stages. By the conclusion of Round 3 in 2022, NIST had selected a set of finalists and alternate candidates for future standardization [120]. Although not all candidates are suitable for resource-limited platforms such as UAVs, the selected algorithms have undergone extensive public scrutiny and represent the most promising approaches for real-world deployment [121].

Figure 10 presents an overview of the algorithms evaluated throughout the competition, organized by cryptographic category. Many of these schemes remain unsuitable for UAVs due to their computational and memory requirements.

The following subsections provide a brief overview of the major classes of PQC schemes and their applicability to UAV platforms [119,122].

- **Code-Based Cryptosystems:** These systems are grounded in the use of error-correcting codes. Security is achieved by deliberately introducing errors into messages, rendering them unintelligible without a private decoding key [123]. A canonical example is the McEliece cryptosystem [124], which uses a structured code (e.g., a Goppa code [125]) that is scrambled to produce a public key. The private key consists of the unscrambled, structured version, known only to the recipient [126,127]. McEliece is attractive for UAV applications due to its fast encryption and decryption, but suffers from very large key sizes—often exceeding 100 KB—posing significant storage and transmission challenges. Research efforts have explored more compact alternatives, such as low-density parity-check (LDPC), moderate-density parity-check (MDPC), and quasi-cyclic variants [121].

- **Lattice-Based Cryptosystems:** These systems rely on the hardness of problems like the Shortest Vector Problem (SVP) and Learning with Errors (LWE), defined over multidimensional lattices [126,128]. Lattice-based schemes are considered among the most promising for quantum resistance due to their strong security proofs and relatively efficient implementations. However, key and ciphertext sizes remain a concern. Compared to code-based cryptography, they require less storage but still impose nontrivial computational costs. Leading candidates such as NTRU [129] and NewHope [130] offer a favorable balance between security and efficiency. Signature schemes based on the Short Integer Solution (SIS) problem have also shown promise, though most remain in early testing stages on constrained hardware. UAV-specific adaptations may benefit from compression techniques and optimized hardware-aware implementations [121].
- **Hash-Based Cryptosystems:** These systems use the cryptographic properties of hash functions—namely, collision resistance and pre-image resistance—to build secure digital signature schemes [123,126]. Hash-based signatures typically generate one-time-use secret keys from a master key and organize them using tree-based structures, such as Merkle trees [131,132]. While highly secure and resistant to quantum attacks, such systems require careful management of key states and may involve large tree structures. Stateless variants reduce the risk of key reuse but come with increased computational overhead. Although hash-based signatures are computationally lightweight, their implementation complexity and management requirements have limited adoption in UAVs [133].
- **Multivariate Cryptosystems:** Multivariate public-key schemes are based on the difficulty of solving systems of multivariate polynomial equations over finite fields [122]. These systems use simple operations like addition and multiplication, making them computationally attractive for constrained environments [126]. Well-known schemes include Hidden Field Equations (HFE) [134] and Unbalanced Oil and Vinegar (UOV), which have been applied in both encryption and signature protocols. Despite their efficiency, multivariate cryptosystems often involve large public keys and ciphertexts, which can limit practical deployment in UAVs. Variants like Rainbow, QUARTZ, QUAD, and Tame Transformation Signatures (TTS) have demonstrated success on low-power devices, but key sizes remain a challenge. For example, a Rainbow implementation with parameters $n = 42, m = 24, q = 256$ yields a public key size of approximately 22,680 bytes [7,121]. Compression techniques and parameter tuning are essential for making these schemes viable for UAV systems.
- **Isogeny-Based Cryptosystems:** Isogeny-based cryptography leverages the mathematical properties of isogenies, or structure-preserving maps between elliptic curves [135]. Supersingular elliptic curves, which lack a commutative endomorphism ring, offer strong resistance to quantum attacks [136]. The Supersingular Isogeny Key Encapsulation (SIKE) protocol has been among the most studied candidates in this category [126,137]. While isogeny-based schemes are appealing due to their relatively small key sizes, they often require intensive computations and are sensitive to side-channel and fault injection attacks. These limitations present challenges for deployment on UAV platforms with tight power and timing constraints [121].
- **Hybrid Cryptosystems:** Hybrid approaches combine classical and post-quantum algorithms to provide defense-in-depth during the transition period. For example, Google's CECPQ1 and CECPQ2 protocols integrated post-quantum key exchange alongside traditional TLS mechanisms. Although hybrid systems offer an additional layer of protection, they are often not suitable for UAVs due to the increased computational and memory demands required to run two cryptographic systems concurrently [121].

According to Fernandez-Carames and Fraga-Lamas [121], the most promising post-quantum cryptographic candidates for UAVs are code-based and lattice-based schemes. Most code-based proposals are derived from McEliece or Niederreiter structures, often using quasi-cyclic enhancements. In contrast, lattice-based approaches typically rely on solving the Learning with Errors (LWE) or Learning with Rounding (LWR) problems, and offer a favorable balance between security and implementation feasibility for lightweight platforms.

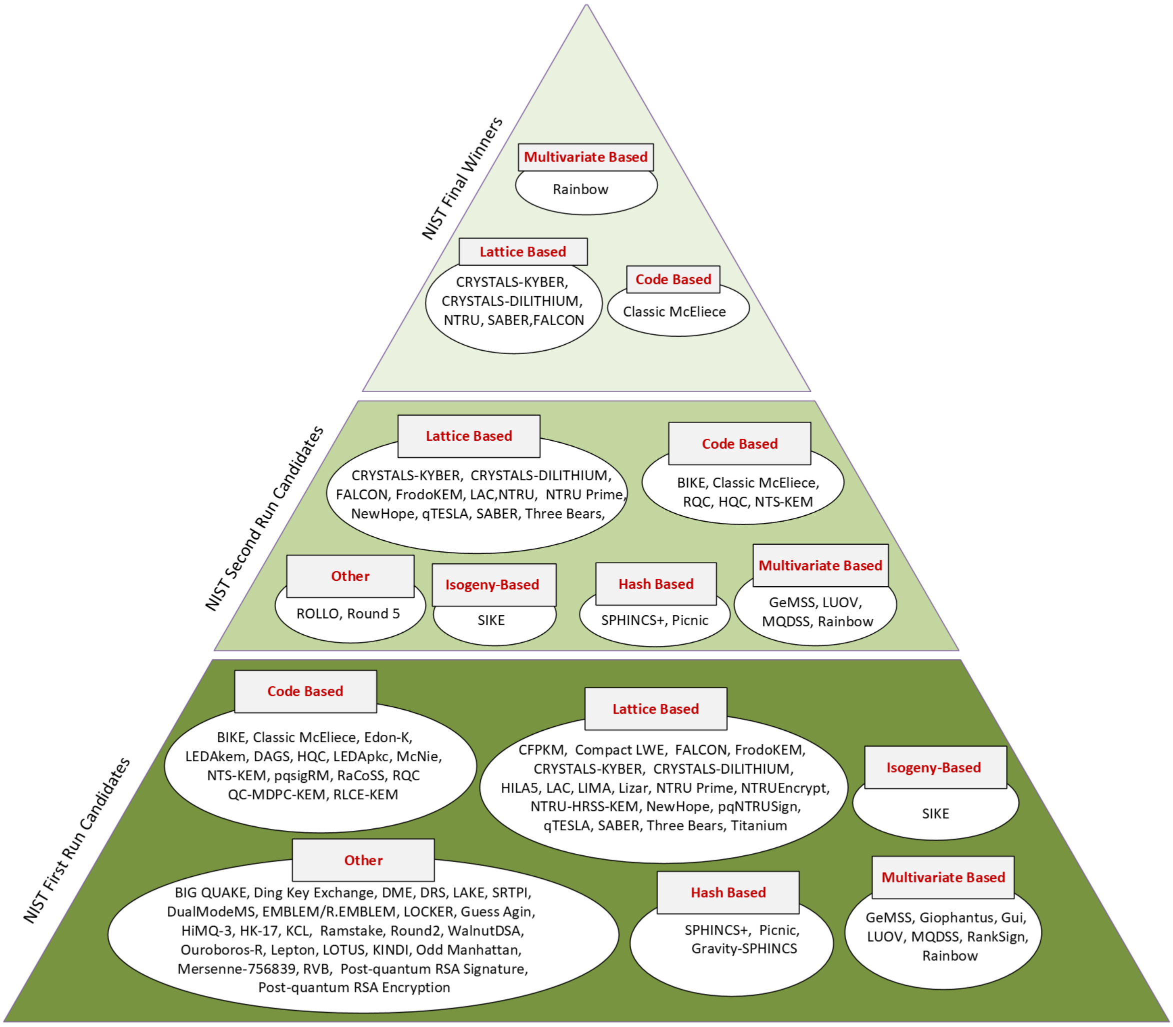
NIST Final Winners
Multivariate Based
Rainbow
Lattice Based
CRYSTALS-KYBER, CRYSTALS-DILITHIUM, NTRU, SABER,FALCON
Code Based
Classic McEliece
NIST Second Run Candidates
Lattice Based
CRYSTALS-KYBER, CRYSTALS-DILITHIUM, FALCON, FrodoKEM, LAC,NTRU, NTRU Prime, NewHope, qTESLA, SABER, Three Bears,
Code Based
BIKE, Classic McEliece, RQC, HQC, NTS-KEM
Other
ROLLO, Round 5
Isogeny-Based
SIKE
Hash Based
SPHINCS+, Picnic
Multivariate Based
GeMSS, LUOV, MQDSS, Rainbow
NIST First Run Candidates
Code Based
BIKE, Classic McEliece, Edon-K, LEDAkem, DAGS, HQC, LEDApkc, McNie, NTS-KEM, pqsigRM, RaCoSS, RQC QC-MDPC-KEM, RLCE-KEM
Lattice Based
CFPKM, Compact LWE, FALCON, FrodoKEM, CRYSTALS-KYBER, CRYSTALS-DILITHIUM, HILA5, LAC, LIMA, Lizar, NTRU Prime, NTRUEncrypt, NTRU-HRSS-KEM, NewHope, pqNTRUSign, qTESLA, SABER, Three Bears, Titanium
Isogeny-Based
SIKE
Other
BIG QUAKE, Ding Key Exchange, DME, DRS, LAKE, SRTPI, DualModeMS, EMBLEM/R.EMBLEM, LOCKER, Guess Agin, HiMQ-3, HK-17, KCL, Ramstake, Round2, WalnutDSA, Ouroboros-R, Lepton, LOTUS, KINDI, Odd Manhattan, Mersenne-756839, RVB, Post-quantum RSA Signature, Post-quantum RSA Encryption
Hash Based
SPHINCS+, Picnic, Gravity-SPHINCS
Multivariate Based
GeMSS, Giophantus, Gui, LUOV, MQDSS, RankSign, Rainbow

Figure 10. Post-quantum encryption systems in the NIST competition

6. Key Management Techniques

While cryptographic primitives, including lightweight symmetric ciphers and post-quantum algorithms, serve as the foundation of secure communication, their effectiveness in UAV systems depends significantly on the management of cryptographic keys. Key management is a critical challenge in securing UAV communication networks due to their dynamic topologies, limited resources, and susceptibility to adversarial attacks. The secure distribution, renewal, and storage of cryptographic keys directly influence the confidentiality, integrity, and availability of UAV communications. This section presents a scientific overview of key management strategies, examining the strengths and limitations of pre-deployed (static) and dynamically distributed key schemes. It also highlights recent advances involving blockchain-based trust infrastructures and Physical Unclonable Functions (PUFs), which offer promising directions for lightweight and tamper-resistant key provisioning.

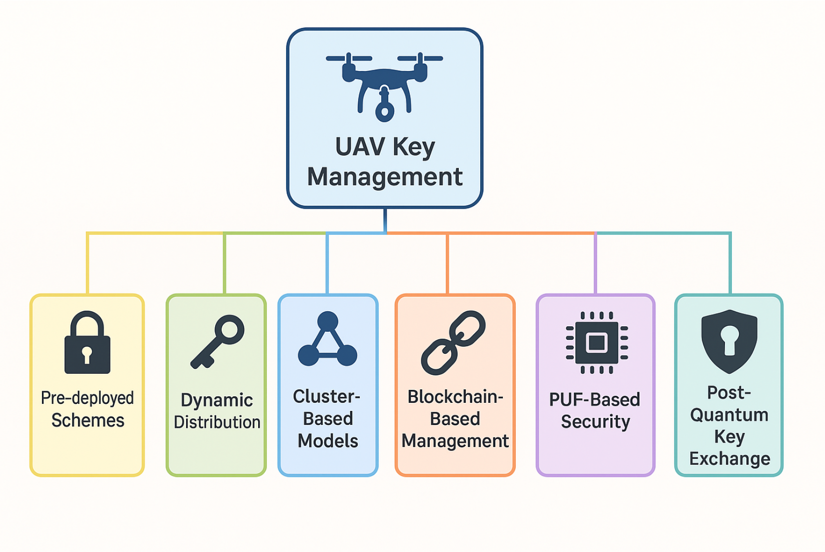

Figure 11. Overview of key management strategies in UAV networks.

6.1. Pre-Deployed vs. Dynamic Key Distribution

Pre-deployed key distribution schemes involve the assignment of cryptographic keys to UAVs prior to mission deployment. These keys may be distributed individually, hierarchically, or in clusters, and are typically stored on the UAV's onboard memory. The primary advantage of static schemes lies in their simplicity and low computational overhead, making them suitable for missions with fixed network topologies or limited resource budgets. However, static approaches exhibit significant limitations in scalability, flexibility, and resilience. If a UAV is captured or compromised, all pre-shared keys stored on the device are at risk, potentially exposing the entire network to adversarial attacks [7]. Furthermore, static keys lack forward secrecy and are particularly vulnerable to quantum computing threats, as they cannot be efficiently updated or replaced in response to evolving risks [4].

In contrast, dynamic key distribution schemes generate and negotiate cryptographic keys during mission execution. These approaches support session-based or on-demand key establishment, often leveraging protocols such as Diffie-Hellman or Elliptic Curve Diffie-Hellman for secure key exchange [138]. Dynamic schemes are inherently more adaptable to changes in network topology, enabling secure peer-to-peer communication in UAV swarms and ad hoc deployments. They also facilitate regular key refreshment, reducing the impact of key compromise and supporting forward secrecy. However, dynamic key distribution introduces additional computational and communication overhead, which may affect energy consumption and latency—critical considerations for UAV platforms with limited resources [4]. Table 7 summarizes the key attributes of pre-deployed and dynamic key distribution approaches, highlighting their relative strengths and limitations in the UAV context.

In summary, while pre-deployed key distribution remains suitable for simple, static UAV missions, dynamic schemes are better suited for flexible and scalable network environments. The ability to adapt to topological changes, support forward secrecy, and refresh keys on demand makes dynamic key distribution increasingly essential in modern UAV networks. Furthermore, the integration of post-quantum cryptographic primitives is becoming a necessary enhancement to ensure resilience against quantum-era threats. The following subsections explore advanced techniques that enhance dynamic key management, including blockchain-based decentralization, hardware-rooted security primitives, and quantum-resistant protocols.

Table 7. Qualitative Comparison of Pre-deployed and Dynamic Key Distribution Schemes in UAV Networks

Attribute	Pre-deployed (Static) Schemes	Dynamic Schemes
Scalability	Suitable for small or fixed topologies	Scales efficiently for large and dynamic UAV swarms
Security	Vulnerable to key compromise; lacks forward secrecy	Resilient to compromise; supports forward secrecy
Quantum Resistance	Not inherently resistant to quantum attacks	Supports the integration of post-quantum or QKD protocols
Energy/Latency Overhead	Low computational and communication cost	Moderate to high depending on the protocol design
Flexibility	Poor adaptability to dynamically-changing topologies	Highly adaptive to dynamic or ad hoc networks
Implementation Complexity	Low; straightforward to implement	Higher complexity due to real-time negotiation and rekeying

6.2. Cluster-Based and Hierarchical Key Management

Cluster-based and hierarchical key management strategies have gained significant traction in UAV networks due to their ability to balance scalability, efficiency, and security within dynamic and resource-constrained environments. In cluster-based approaches, UAVs are organized into logical groups or clusters, each managed by a designated cluster head responsible for key generation, distribution, and renewal within its domain [139]. This structure reduces the complexity of key management by localizing key-related operations, thereby minimizing communication overhead and confining the impact of potential node compromise to individual clusters rather than the entire network [140,141].

Hierarchical key management extends this concept by introducing multiple layers of authority and responsibility. A typical architecture involves a two-tier structure, where the lower tier consists of cell or cluster groups managed by local leaders (such as mobile backbone nodes or cluster heads), and the upper tier comprises a control group or supernodes that oversee the overall network. This hierarchical arrangement enables efficient group key management and supports secure inter-cluster communication using group key agreement protocols and implicitly certified public keys. The main advantage of this approach is its ability to restrict the effects of membership changes, such as node join or leave events, to the relevant cluster, thus enhancing scalability and reducing the frequency and scope of costly rekeying operations [142,143].

Recent advancements have incorporated unsupervised learning and clustering algorithms to further optimize cluster formation and maintenance, enabling UAV networks to dynamically adapt to changing mission requirements and network topologies [144]. For instance, agglomerative hierarchical clustering has been used to assign UAVs to clusters based on communication quality or mission objectives, ensuring that key management remains efficient even as the network evolves in real time.

Cluster-based and hierarchical schemes also facilitate the integration of advanced security features, such as distributed key agreement, resilience to node capture, and efficient lost key recovery. In denied or adversarial environments, these approaches have demonstrated the ability to maintain secure communication with minimal energy and bandwidth consumption, making them particularly suitable for large-scale UAV swarms and mission-critical applications [145].

In summary, cluster-based and hierarchical key management architectures provide a robust foundation for scalable, resilient, and efficient key distribution in UAV networks. By localizing key operations and leveraging layered control, these schemes address many of the unique challenges posed by dynamic aerial environments, supporting both intra- and inter-cluster security with reduced overhead and enhanced adaptability.

6.3. Blockchain-Based Decentralized Key Management

Blockchain-based decentralized key management has emerged as a robust paradigm for enhancing the security, transparency, and scalability of UAV networks. Traditional centralized key distribution models are prone to single points of failure and scalability limitations, particularly in dynamic and adversarial environments. In contrast, blockchain leverages a distributed, immutable ledger to enable consensus-driven management of cryptographic operations, including key generation, distribution, and revocation [9,146].

In a blockchain-enabled UAV ecosystem, each UAV or ground station may function as a participating node in a private or consortium blockchain, validating and recording security-related transactions. This decentralized architecture eliminates dependency on centralized trust authorities and enhances resilience against impersonation, data tampering, and unauthorized access [147]. Permissioned blockchain frameworks such as Hyperledger Fabric and Tendermint offer high throughput and low-latency performance, rendering them suitable for real-time UAV applications.

Several blockchain-based protocols have been proposed to address the unique constraints of UAV communication. Notably, the BETA-UAV scheme integrates smart contracts to automate mutual authentication between UAVs and ground control stations, effectively mitigating replay and spoofing attacks with minimal communication overhead [10]. Other solutions implement group key management where a private blockchain ledger is used to orchestrate secure join/leave operations, distribute group keys, and enable key recovery upon node failure [148]. These mechanisms ensure tamper-evident logging of security events and provide traceable, auditable key lifecycle management.

Beyond authentication, blockchain also supports decentralized identity frameworks. Each UAV can be assigned a unique digital identity anchored in the blockchain ledger, enabling transparent and verifiable trust relationships across multi-operator or cross-border deployments [149]. Smart contracts further enhance autonomy by orchestrating key lifecycle tasks such as renewal, revocation, and recovery without manual intervention.

Performance evaluations suggest that lightweight, permissioned blockchain configurations can achieve latency and throughput levels compatible with aerial mission timelines [9]. However, challenges persist regarding resource consumption, real-time consensus synchronization, and integration with PQC. Emerging research is exploring hybrid architectures that combine blockchain with AI/ML techniques for adaptive threat detection and self-healing key infrastructures [147].

In summary, blockchain-based decentralized key management offers a scalable, tamper-resistant solution tailored to the operational and security requirements of UAV networks. As autonomous aerial systems grow in complexity and interconnectivity, blockchain is positioned to become a foundational enabler of secure, interoperable, and self-managing UAV ecosystems.

6.4. PUF-Based Secure Key Storage and Generation

Physical Unclonable Functions (PUFs) have emerged as a foundational technology for secure key storage and generation in UAV networks, addressing limitations associated with traditional cryptographic key management systems. PUFs exploit uncontrollable physical variations in integrated circuits to produce unique device-specific responses to external challenges. These responses are reproducible under controlled conditions but nearly impossible to clone or predict, making PUFs an effective basis for lightweight and tamper-resistant security solutions in resource-constrained UAV environments [150,151].

Unlike conventional approaches that store sensitive cryptographic keys in non-volatile memory, thereby exposing them to extraction through physical attacks, PUF-based systems derive keys dynamically from the hardware at runtime. During an initial enrollment phase, a set of challenge–response pairs (CRPs) is generated from the UAV embedded PUF and stored securely at the ground station (GS). When authentication or key derivation is needed, the GS transmits a challenge to the UAV, which computes the response using its PUF circuitry. The resulting transient key is reconstructed in real time, eliminating the need for persistent key storage and reducing susceptibility to physical compromise [28,152].

This architecture enhances several core security properties. First, tamper resistance is achieved by avoiding long-term storage of static secrets, making it infeasible for adversaries to extract usable key material from a captured node. Second, PUFs support forward secrecy by generating fresh keys for each session, ensuring that the compromise of one key does not retroactively endanger past communications. Third, the lightweight computational profile of PUF-based protocols makes them ideal for UAV platforms with limited processing power and battery capacity. Studies report that authentication latencies can be reduced to 214 µs using programmable switches—roughly twice as fast as CPU-bound methods - while also consuming up to 42% less energy than AES-128 under comparable security assumptions [93,151].

Recent PUF-based schemes combine physical uniqueness with cryptographic primitives to achieve robust and scalable key management. Hybrid PUF-hash models use functions such as SHA-3 to convert raw responses into uniform and collision-resistant key material, thereby improving entropy while obscuring hardware-specific noise. Lattice-based PUF designs have also been proposed to extend these methods to post-quantum key exchange, achieving 1,024-bit quantum-resistant security at energy costs as low as 18 mJ per exchange [153,154].

A summary of PUF defenses against common UAV attack vectors is provided in Table 8. These systems resist node capture through volatile key derivation, withstand cloning due to their inherent physical randomness, and protect against eavesdropping with opaque, non-deterministic CRP mappings. Hardware tampering typically disrupts circuit behavior, rendering key generation invalid or unreliable.

Table 8. PUF-Based Security Strategies for UAV Threat Mitigation

Threat Model	PUF-Based Mitigation Strategy
Node Capture	No static key storage; responses generated dynamically on-demand
Cloning Attacks	Physical randomness prevents duplication across devices
Eavesdropping	Non-deterministic challenge-response mappings resist inference
Hardware Tampering	Altered circuit behavior degrades PUF reliability and invalidates authentication

Despite their advantages, PUF systems face challenges related to reliability and protocol design. Environmental factors—such as voltage fluctuations and temperature variations—can alter response stability. To mitigate this, error correction codes like BCH and Reed–Solomon are integrated to achieve bit error rates below 10^{-6} [154]. Additionally, early PUF schemes (e.g., PLAKE, EV-PUF) demonstrated vulnerabilities such as key leakage and response collisions. These have been addressed in more recent protocols by incorporating adaptive CRP sets and authenticated encryption using lightweight standards such as ASCON-128a [28,93].

Standardization efforts are underway to formalize PUF evaluation criteria for UAV and aerospace systems. NIST's Interagency Report 8420 aims to establish metrics to evaluate the reliability, uniqueness, and resistance of PUF to physical and logical attacks, thus supporting a greater adoption in secure UAV communication frameworks.

6.5. Post-Quantum Key Exchange Techniques

The emergence of quantum computing presents a substantial threat to classical cryptographic schemes that currently underpin UAV communication systems. Algorithms based on number-theoretic assumptions such as RSA, DSA, and Elliptic Curve Cryptography (ECC) are vulnerable to quantum attacks, particularly due to Shor's algorithm, which can solve integer factorization and discrete logarithm problems in polynomial time. Given that many UAV key management protocols rely on these primitives, their long-term security is at risk as quantum computing becomes more viable.

PQC has been proposed as a class of cryptographic algorithms that remain secure in the presence of both classical and quantum adversaries. These include lattice-based, code-based, multivariate, hash-based, and isogeny-based families. Among them, lattice-based schemes such as Kyber, NewHope, and NTRU have demonstrated promise for UAV applications due to their efficiency, strong security proofs, and ongoing standardization through NIST's Post-Quantum Cryptography project [7]. Kyber and NTRU are Key Encapsulation Mechanisms (KEMs) that rely on the hardness of problems such as Learning With Errors (LWE) and Ring-LWE, which are believed to be resistant to quantum attacks.

In UAV environments, where energy efficiency, processing speed, and communication overhead are constrained, PQC protocols must be optimized for embedded implementation. Evaluations of Kyber and NewHope have shown that key exchange can be performed with latency under 10ms and memory usage below 32KB on embedded processors, while offering 128-bit post-quantum security levels [8,133]. Despite their cryptographic strength, code-based algorithms like Classic McEliece and BIKE present challenges in terms of key size, with public keys often exceeding several hundred kilobytes [155].

To facilitate gradual migration, hybrid key exchange schemes that combine traditional algorithms (e.g., ECDH) with post-quantum primitives (e.g., Kyber) are being implemented to ensure backward compatibility and layered defense. These approaches enable resilience even if one algorithm is later broken, which is particularly useful in transitional environments like UAV networks [156]. Additionally, quantum-resilient protocols for cross-domain authentication have been developed using PUF and lattice-based key exchanges, enabling robust identity verification in drone swarms and distributed aerial systems [157].

Another area of active research involves quantum key distribution (QKD) protocols applied to UAVs. QKD enables information-theoretic security by leveraging quantum entanglement and the no-cloning theorem to generate shared secrets. Demonstrations of mobile QKD between moving aerial platforms have shown the feasibility of secure optical links under flight dynamics, though limitations remain in terms of range, environmental sensitivity, and hardware requirements [158]. As UAVs transition into more secure and autonomous roles, QKD may complement PQC in high-assurance scenarios.

Performance comparisons of post-quantum techniques indicate that lattice-based protocols offer the most practical balance for UAV networks between computational efficiency and quantum resistance. The adoption of schemes like Kyber is accelerating, driven by NIST's standardization and increasing availability of optimized embedded libraries [133,159]. Continued work in hardware acceleration, including GPU and FPGA-based implementations, further supports their real-world deployment [127].

Building on the foundational role of key distribution and maintenance in secure UAV communications, it becomes essential to address how these cryptographic mechanisms integrate across the full communication stack.

7. Multilayer Security Framework

As discussed in earlier sections, the security posture of UAV networks must span the entire OSI model, with vulnerabilities ranging from MAC-layer spoofing to application-layer control manipulation. This section introduces a defense-in-depth framework that incorporates lightweight and post-quantum cryptographic primitives, blockchain-based trust models, and hardware-anchored identity protocols. These techniques are applied systematically across multiple OSI layers to form a unified, zero-trust architecture that is resilient against both layer-specific and cross-layer attacks. The proposed framework emphasizes coordinated detection, response, and recovery mechanisms tailored for resource-constrained aerial platforms operating in adversarial environments.

7.1. Physical Layer Security

Physical Layer Security (PLS) plays a foundational role in safeguarding UAV communication systems by addressing vulnerabilities inherent to the open and broadcast nature of wireless channels. UAVs are particularly exposed due to their high mobility and reliance on line-of-sight (LoS) air-to-ground links, making them prime targets for both eavesdropping and jamming attacks. These threats can disrupt mission-critical operations by compromising confidentiality or degrading communication availability. While upper-layer cryptographic methods remain essential, they often incur computational and energy overheads unsuitable for resource-constrained UAV platforms. In contrast, PLS offers a complementary and lightweight approach by harnessing the physical properties of wireless channels to enhance secrecy and resilience.

Jamming attacks intentionally inject interference to reduce the signal-to-noise ratio (SNR) at the receiver, potentially leading to denial of service or UAV disconnection. To mitigate this, techniques such as frequency hopping, spread-spectrum communication, and cognitive radio enable UAVs to dynamically adapt transmission parameters in response to changing interference patterns [32]. Similarly, eavesdropping, which capitalizes on the broadcast nature of wireless signals, can be countered through artificial noise injection, cooperative jamming, and secure beamforming—each designed to deteriorate the adversary's reception while maintaining link quality with legitimate receivers [18,34].

UAV mobility further enhances PLS through trajectory optimization, where flight paths are adjusted to avoid proximity to eavesdroppers or to improve channel characteristics for secure communication. Multi-antenna systems, such as beamforming and MIMO (Multiple-Input Multiple-Output), allow UAVs to direct signal energy toward intended recipients and nullify transmissions in vulnerable directions [33]. Recently, reconfigurable intelligent surfaces (RIS) have emerged as a transformative technology, enabling programmable wireless environments. By reflecting signals in a controlled manner, RIS can amplify legitimate links and suppress undesired reception, thereby improving secrecy performance under both jamming and surveillance conditions [160].

The effectiveness of PLS is commonly evaluated using metrics such as secrecy capacity, secrecy outage probability, and secrecy rate. Empirical studies demonstrate that integrating PLS significantly enhances the confidentiality and robustness of UAV communications, even under complex and adversarial conditions [18]. However, the dynamic and heterogeneous nature of aerial communication channels, affected by Doppler shifts, multipath fading, and environmental obstacles, presents ongoing challenges. These call for adaptive, context-aware PLS solutions.

For comprehensive protection, PLS should be integrated with upper-layer lightweight encryption schemes, such as ASCON or Grain-128a, and dynamic key management protocols. This integration ensures a robust multilayered defense, capable of withstanding both passive and active attacks while adhering to the strict resource constraints of UAV platforms. Emerging research directions include AI-assisted mobility planning, RIS-augmented secure links, and seamless interoperability with post-quantum cryptographic frameworks. As UAV operations grow in scale and complexity, the advancement of physical layer security will remain essential for ensuring secure, resilient, and energy-efficient aerial networks.

7.2. MAC Layer: Authentication and Frame Integrity

The Medium Access Control (MAC) layer plays a central role in securing UAV communication systems by regulating access and enforcing node identity. Due to the wireless and broadcast nature of UAV networks, the MAC layer is highly susceptible to adversarial attacks such as spoofing, replay, and frame injection. These threats exploit the reliance on address-based communication, enabling malicious actors to impersonate legitimate nodes or insert falsified control messages. In UAV swarms, such vulnerabilities can lead to network partitioning, misdirection of flight paths, loss of coordination, and, in severe cases, physical collisions or emergency landings.

To mitigate these risks, researchers have proposed several lightweight security mechanisms tailored for the resource-constrained environments typical of UAV platforms. A widely adopted solution is the use of lightweight authenticated encryption with associated data (AEAD). ASCON, a cipher selected by the National Institute of Standards and Technology (NIST) as the standard for lightweight cryptography, provides both confidentiality and integrity with minimal processing overhead. It enables secure encryption and authentication of control frames in real time, thereby defending against frame injection and spoofing while maintaining energy efficiency and low latency, which are critical for UAV operations [4].

Replay attacks, in which adversaries retransmit intercepted packets to disrupt operations, are addressed through hash chain synchronization. This approach attaches a unique, time-evolving hash value to each packet, ensuring freshness and preventing reuse of old messages. Hash chain synchronization has proven effective in swarm communication, where message sequence integrity is essential to maintain formation and coordinated behavior [23].

In addition, synchronized message authentication codes are employed to verify message authenticity using shared cryptographic secrets and clock synchronization between nodes. This method allows UAVs to confirm the origin and timeliness of received data, making it more difficult for attackers to inject unauthorized messages. Such synchronized MAC verification strengthens trust across swarm participants and helps sustain uninterrupted and validated control communication [161].

Protocol-level defenses complement these cryptographic techniques. Rate-limiting policies and anomaly detection algorithms can monitor MAC-level activity, identify abnormal patterns such as excessive frame transmission, and throttle or block suspicious traffic. These strategies serve as an important second line of defense, particularly during active interference or flooding attempts [162].

Securing the MAC layer through integrated cryptographic and procedural controls is fundamental to maintaining the stability, confidentiality, and integrity of UAV networks. The combination of ASCON AEAD encryption, hash chain synchronization, and synchronized MAC validation forms a comprehensive and lightweight framework that can withstand attacks targeting low-level wireless protocols. These safeguards are essential for reliable operation in both benign and adversarial environments, contributing significantly to the broader multilayer security architecture required for resilient UAV deployments.

7.3. Network Layer: Secure Routing and Trust Models

The network layer in UAV networks is responsible for enabling reliable inter-drone and drone-to-ground station communication, but it is also a prime target for sophisticated routing-based attacks such as black hole, Sybil, and wormhole attacks. These threats can result in packet misrouting, intentional packet dropping, or the distortion of network topology, ultimately leading to the isolation or compromise of UAVs within a swarm and disruption of mission objectives [44,163]. Addressing these vulnerabilities requires a combination of cryptographic, hardware-rooted, and trust-based mechanisms tailored to the dynamic and resource-constrained environment of UAV operations [23,164].

A leading defense strategy is blockchain-based routing validation, as exemplified by protocols like BETA-UAV. Blockchain technology provides a decentralized and tamper-resistant ledger for logging and verifying routing updates. Each routing announcement or path change is cryptographically recorded and validated by network participants, making it extremely difficult for adversaries to inject forged or malicious routes without detection. The BETA-UAV protocol leverages smart contracts to automate route validation and consensus, significantly mitigating the risk of route manipulation and Sybil attacks in large-scale UAV deployments [9,10]. Performance assessments indicate that such blockchain-enabled frameworks can achieve high throughput and low latency, supporting real-time swarm operations without introducing prohibitive overhead.

In parallel, Physical Unclonable Function (PUF)-tied cryptographic certificates provide robust hardware-level identity assurance. Each UAV is equipped with a PUF module that generates a unique, tamper-resistant cryptographic identity based on intrinsic hardware characteristics. This identity is used to bind digital certificates directly to the physical device, preventing identity spoofing and ensuring that only legitimate UAVs participate in routing and network operations. PUF-based authentication protocols have demonstrated fast verification times and strong resistance to physical capture or cloning attacks, making them highly suitable for mobile and adversarial environments [28,150,151].

Decentralized trust management further strengthens network layer security by enabling UAVs to evaluate the trustworthiness of their peers based on observed behaviors such as packet forwarding consistency and historical route validity. Trust anchors and peer scoring mechanisms allow the network to dynamically adjust routing preferences, isolating or penalizing nodes that exhibit malicious or unreliable behavior [25,36]. This distributed approach to trust evaluation reduces reliance on any single point of failure and enhances resilience against coordinated attacks, including collaborative black hole and Sybil threats.

Recent research also explores the integration of artificial intelligence and anomaly detection for real-time monitoring of routing behaviors and early identification of suspicious activity. AI-driven frameworks such as Aero-LLM adaptively adjust routing policies and trust scores in response to evolving attack patterns, further improving the robustness of UAV network communications [165].

In summary, secure routing and trust at the network layer are achieved through the synergistic use of blockchain-based validation, PUF-tied cryptographic identities, and decentralized trust anchors. These mechanisms collectively provide authenticated, tamper-resistant routing, protect against identity and route spoofing, and enable dynamic adaptation to emerging threats, thereby supporting resilient and mission-assured UAV operations in contested environments.

7.4. Transport Layer: End-to-End Encryption and Quantum-Resilient Defense

The transport layer in UAV networks plays a crucial role in enabling reliable, low-latency communication between drones and ground control stations. However, this layer remains a significant target for a range of cyber threats, including session hijacking, denial-of-service (DoS), and flooding attacks. These attacks threaten not only the continuity of telemetry and command transmission but also the safety and autonomy of UAV operations. Given the real-time and mission-critical nature of aerial systems, securing the transport layer is essential for ensuring end-to-end confidentiality, integrity, and availability.

To mitigate these risks, authenticated encryption with associated data (AEAD) algorithms such as ASCON and AES-GCM are widely employed to protect data in transit. ASCON, recently selected by NIST as the standard for lightweight cryptography, offers robust message integrity and encryption with minimal computational overhead, making it particularly well-suited for resource-constrained UAVs [4]. AES-GCM, a well-established AEAD cipher, provides high throughput and efficient integrity checking, especially useful in bandwidth-sensitive telemetry channels. These encryption schemes ensure that transport-layer messages remain tamper-evident and protected from unauthorized interception or modification.

In addition to symmetric encryption, the deployment of post-quantum cryptographic protocols has become increasingly relevant as UAV systems evolve. The Kyber key encapsulation mechanism enables secure session key establishment with resistance to quantum attacks [166]. By integrating Kyber into the handshake protocols of the transport layer, UAV networks achieve forward secrecy against both classical and quantum adversaries, thereby enhancing the long-term security posture of autonomous aerial operations.

DoS and flooding attacks at this layer are addressed through intrusion detection mechanisms and traffic shaping techniques. Filters capable of identifying anomalous connection patterns, including high-frequency session requests or malformed handshake packets, are essential to maintain system responsiveness. For instance, Rugo and Wang propose lightweight filters designed to detect protocol-level anomalies that commonly precede DoS events [163]. These filters can throttle, reroute, or isolate malicious traffic sources, ensuring continuity of legitimate communication.

Complementary to detection systems, container-based architectures have been introduced to further enhance resilience. Chen et al. present a control framework that leverages containers to isolate mission-critical processes, allowing real-time control functions to remain operational even under attack

[167]. This architectural separation ensures rapid recovery and fault containment, preserving UAV control integrity in hostile environments.

Emerging research also emphasizes the importance of adaptive and context-aware transport-layer security policies. These approaches dynamically adjust session key lifetimes, cipher strengths, and detection thresholds based on environmental factors and mission profiles [133]. Such adaptability enables UAV platforms to optimize the trade-off between energy efficiency and security robustness, particularly in long-duration or swarm deployments.

In summary, securing the transport layer in UAV networks requires a layered strategy that combines lightweight AEAD algorithms (ASCON, AES-GCM), post-quantum key exchange (Kyber), intrusion detection filters, and resilient system design. Together, these elements provide a comprehensive defense capable of maintaining real-time, secure communication under both traditional and advanced cyber threats.

7.5. Application Layer: Data Integrity, Access Control, and Secure Interfaces

The application layer in UAV networks forms a critical security boundary, as it governs mission execution, software updates, data offloading, and remote service communication. With the increasing reliance on cloud infrastructure, third-party APIs, and autonomous control platforms, the attack surface at this layer has expanded significantly. This layer is particularly vulnerable to high-impact threats such as command injection, firmware tampering, unauthorized data access, and credential theft, which can result in mission failure, data breaches, or drone hijacking [25,38].

One of the most prominent attack vectors is unauthorized access to cloud-connected services. Weak authentication schemes and improper access control mechanisms can enable adversaries to intercept or manipulate mission data, access sensitive telemetry, or reroute UAVs. These risks are amplified in swarm and multi-tenant environments, where improperly scoped access rights and hardcoded credentials, such as FTP passwords or update server keys, may exist within the application code [168]. Persistent attackers can exploit these flaws to inject malicious commands or exfiltrate data, compromising operational integrity.

Software and firmware update mechanisms are a well-known vulnerability at this layer. Over-the-air (OTA) updates are essential for feature deployment and patching, yet, if not cryptographically authenticated, they offer an avenue for adversaries to upload tampered firmware or install persistent backdoors. Elliptic Curve Cryptography (ECC) based digital signatures are widely adopted to ensure software integrity. These signatures allow UAVs to verify the origin and validity of update files before execution, thereby defending against counterfeit firmware deployment [22].

Command injection threats, particularly common in logistics and delivery scenarios, are often realized through insecure application interfaces. In such attacks, adversaries may reroute drones, alter mission parameters, or hijack payloads. Role-Based Access Control (RBAC) mechanisms mitigate these risks by enforcing privilege separation. By assigning fine-grained permissions based on user roles, RBAC restricts access to critical commands, reducing the likelihood of unauthorized mission manipulation [25].

Lightweight AEAD encryption schemes, such as AES-GCM and ASCON, are increasingly implemented to secure telemetry, commands, and application-layer payloads. While AES-GCM provides strong confidentiality and integrity guarantees, its energy and memory overhead may pose challenges in UAVs with constrained resources. ASCON, in contrast, delivers comparable cryptographic strength with reduced computational complexity, making it a preferred choice for low-power aerial platforms [4].

In addition, secure API gateways and token-based authentication protocols are instrumental in protecting UAV-ground-cloud communication channels. These systems enforce real-time request validation, support logging and auditing of control events, and block unauthorized access to sensitive operations or mission data. When integrated with encrypted channels, these gateways help establish a verifiable trust perimeter around application-layer functions [22].

doi:10.20944/preprints202507.1503.v1

In summary, securing the application layer of UAV networks demands a multi-pronged strategy involving ECC-based digital signatures for firmware validation, RBAC enforcement for privilege control, lightweight encryption protocols such as ASCON for data confidentiality, and secure API gateways to manage authentication and communication flows. These components collectively defend against command injection, firmware tampering, and unauthorized access, ensuring that only verified entities and trusted data influence mission-critical operations.

7.6. Cross-Layer Security: Coordinated Defense Across the Communication Stack

Cross-layer security design in UAV networks has emerged as a critical necessity due to the interdependent nature of layered communication protocols and the complexity of modern attack vectors. Traditional siloed defenses often fail to detect or mitigate threats that propagate across multiple layers of the OSI model. In contrast, a cross-layer approach provides a unified, adaptive framework that integrates cryptographic, hardware-based, and trust-driven mechanisms across all communication layers, from the physical channel to mission-level applications.

In UAV environments, especially those involving swarms or autonomous missions, an attack targeting a single layer can cascade through the system. For instance, a jamming attack at the physical layer may disrupt MAC-level frame authentication, resulting in missed routing updates at the network layer and ultimately leading to control failures at the application layer. These coordinated threats necessitate security strategies that span layer boundaries and respond in real time.

At the lower layers, lightweight authenticated encryption algorithms such as ASCON protect against spoofing, replay, and eavesdropping while conserving battery life and processing resources. Hash chain synchronization enhances resilience by ensuring message freshness and preventing session replays. At the network layer, blockchain-based protocols such as BETA-UAV validate routing paths through decentralized consensus, while PUF-based cryptographic certificates bind identity to hardware, ensuring that only trusted nodes participate in routing [10,28]. Peer-based trust anchors add behavioral assessment, enabling the network to penalize or isolate malicious UAVs in real time [25].

Transport layer protection is achieved through a combination of AEAD ciphers like AES-GCM and post-quantum schemes such as Kyber, which ensure session confidentiality and forward secrecy against both classical and quantum threats [127]. Intrusion detection filters monitor for signs of denial-of-service (DoS), session hijacking, or malformed packet floods, enabling early threat containment [163].

The application layer is defended through ECC-based digital signatures for verifying firmware integrity, Kyber-ECIES hybrid encryption for secure payload delivery, role-based access control (RBAC) for privilege separation, and token-based secure API gateways for managing UAV-to-cloud interactions [4,22].

Cross-layer coordination is further enforced through middleware capable of executing system-wide policies such as key expiration, anomaly detection, and logging. PUF-based hardware binding ensures that identities are tied to physical devices across the entire stack, while blockchain-backed identity management allows drones to authenticate within decentralized systems. Dynamic rekeying protocols reduce key reuse risk by rotating session credentials based on time or event triggers.

Recent advances in UAV cybersecurity include the development of cross-layer convolutional attention networks for intrusion detection, which leverage temporal-spatial features across OSI layers to identify anomalies in real time [169]. Other efforts focus on satellite-UAV-ground integration, where authentication schemes span multiple communication domains, demonstrating the importance of coordinated, multi-domain trust frameworks [170]. Implementation-level practices such as disabling unused services, firmware-level cryptography integration, and dynamic whitelisting further harden the system without increasing attack surface [171].

Table 9. Threat-to-Solution Mapping Across OSI Layers in UAV Networks

OSI Layer	Section 3 Threats	Section 7 Solutions
Physical (L1)	Jamming, Eavesdropping	Frequency hopping, beamforming, trajectory optimization, RIS-based signal enhancement [32–34,160]
MAC (L2)	Spoofing, Replay, Frame Injection	ASCON AEAD encryption [4], hash chain synchronization [23], synchronized MACs [161], rate limiting and anomaly detection [162]
Network (L3)	Routing Manipulation, Sybil, Wormhole	BETA-UAV blockchain validation [10], PUF-tied certificates [28], decentralized trust anchors [25], AI-based routing anomaly detection [165]
Transport (L4)	Session Hijacking, DoS, Flooding	AES-GCM, ASCON encryption [4], Kyber key exchange [166], DoS filters [163], container-based isolation [167]
Application (L5)	Command Injection, Firmware Tampering, Credential Theft	ECC signatures for OTA validation [22], Kyber-ECIES hybrid encryption [127], RBAC policies [25], secure API gateways and token authentication [22]
Cross-Layer	Cascading Attacks, Identity Misuse	PUF-based identity binding [28], blockchain-based ID management [10], dynamic rekeying protocols [27], cross-layer intrusion detection and policy enforcement [169,171]

To illustrate the alignment between threat vectors and corresponding mitigation strategies across the communication stack, Table 9 summarizes the multilayer defense mechanisms proposed in Section 7 relative to the threats identified in Section 3.

In summary, cross-layer security represents a best-practice paradigm for UAV networks, offering unified protection against cascading, coordinated, and persistent threats. By linking cryptographic enforcement, device identity, and real-time behavioral trust across all layers, UAV systems can achieve the resilience and autonomy required for critical missions in contested environments.

8. Application Suitability

The effectiveness of any UAV security strategy depends not only on its technical soundness but also on its suitability for specific operational environments. UAVs are increasingly deployed across diverse application domains such as military surveillance, disaster response, logistics and delivery, precision agriculture, environmental monitoring, and infrastructure inspection. Each of these domains presents distinct operational requirements related to energy availability, latency tolerance, scalability, and the level of security assurance needed.

Security mechanisms must therefore be tailored to meet the constraints and objectives of each context. For example, mission-critical applications like military reconnaissance and emergency response demand high assurance of confidentiality and integrity, even under adversarial conditions or limited connectivity. On the other hand, commercial uses such as crop monitoring or package delivery may prioritize low-latency communication and energy efficiency over advanced cryptographic features. These differences underscore the importance of aligning cryptographic choices, key management schemes, and trust models with the specific mission goals and environmental constraints of each UAV deployment [1].

Figure 12 summarizes these diverse application domains, highlighting how their distinct characteristics influence security design.

doi:10.20944/preprints202507.1503.v1

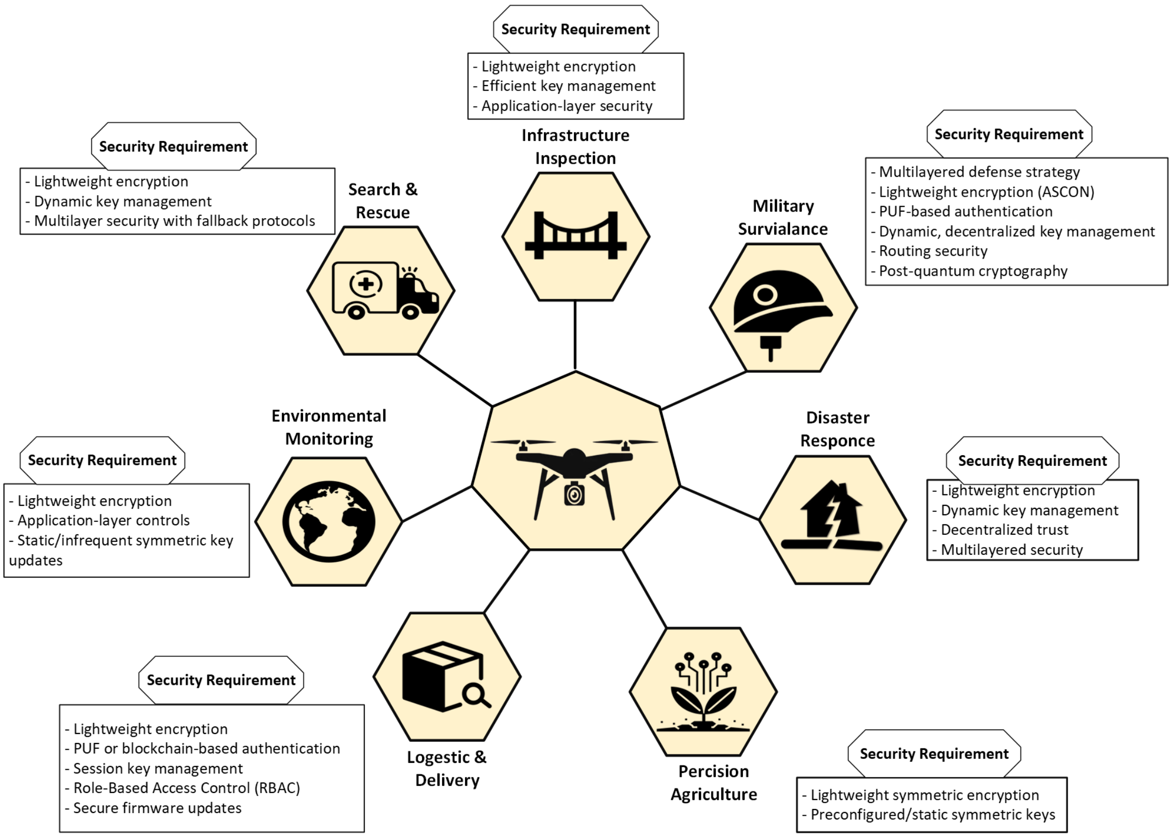
Security Requirement
- Lightweight encryption
- Efficient key management
- Application-layer security
Infrastructure Inspection
Security Requirement
- Lightweight encryption
- Dynamic key management
- Multilayer security with fallback protocols
Search & Rescue
Security Requirement
- Multilayered defense strategy
- Lightweight encryption (ASCON)
- PUF-based authentication
- Dynamic, decentralized key management
- Routing security
- Post-quantum cryptography
Military Survialance
Environmental Monitoring
Security Requirement
- Lightweight encryption
- Application-layer controls
- Static/infrequent symmetric key updates
Disaster Responce
Security Requirement
- Lightweight encryption
- Dynamic key management
- Decentralized trust
- Multilayered security
Security Requirement
- Lightweight encryption
- PUF or blockchain-based authentication
- Session key management
- Role-Based Access Control (RBAC)
- Secure firmware updates
Logestic & Delivery
Percision Agriculture
Security Requirement
- Lightweight symmetric encryption
- Preconfigured/static symmetric keys

Figure 12. UAV application domains and their distinct security requirements.

8.1. Military Surveillance

Military UAVs operate in highly contested environments where adversaries actively attempt to compromise the confidentiality, availability, and integrity of airborne communication. These attacks often include eavesdropping, GPS spoofing, jamming, Sybil, and wormhole attacks, which pose significant threats to surveillance, reconnaissance, and tactical targeting operations [44,70]. Such adversarial actions are typically persistent and coordinated, necessitating a multilayered defense strategy.

Lightweight encryption protocols such as ASCON, recently selected by NIST as the standard for lightweight authenticated encryption, support low-latency and energy-efficient communication. These algorithms are well suited for constrained military platforms and help maintain real-time telemetry and control even under resource limitations [4].

In swarm or cooperative UAV missions, identity spoofing or key compromise can lead to mission failure or drone miscoordination. Physical Unclonable Function (PUF) based authentication enables tamper-resistant, hardware-rooted identity verification, preventing cloning and impersonation of UAVs [11,28]. Dynamic and decentralized key management mechanisms, including hierarchical clustering and blockchain-based protocols such as BETA-UAV, allow for secure rekeying and session establishment during real-time operations [10].

Military UAV networks are also vulnerable to routing-based disruptions. Attacks like black hole and wormhole exploit network topologies to redirect or drop mission-critical data. Blockchain-based routing validation combined with trust scoring helps ensure authenticated route dissemination and detection of malicious behaviors [165].

With the growing risk posed by quantum computing, classical encryption is no longer sufficient for long-term security. Post-quantum encryption schemes such as Kyber and NTRU offer protection against quantum adversaries while meeting the energy and latency constraints of embedded systems [7, 127].

8.2. Precision Agriculture

UAVs used in precision agriculture typically operate in low-risk, well-controlled environments where the probability of targeted adversarial actions such as jamming, spoofing, or traffic interception is minimal [75]. The primary operational concerns in these scenarios involve maximizing battery efficiency, maintaining long-range communication, and ensuring coordinated functioning across large UAV fleets deployed for crop monitoring, irrigation assessment, or resource distribution.

Given these resource constraints, the security design emphasizes minimalism and energy efficiency. Symmetric lightweight ciphers are favored for maintaining confidentiality and data integrity without introducing computational bottlenecks or reducing flight time [95]. These ciphers are sufficient to protect telemetry data and sensor streams from passive threats while maintaining real-time responsiveness in the field [72].

For key management, agricultural UAVs often rely on preconfigured symmetric keys with occasional offline updates during refueling or recharging cycles. This approach eliminates the need for energy-intensive key exchange protocols and minimizes communication overhead in field deployments [34]. In most operational scenarios, static or infrequently rotated keys are sufficient to deter basic misuse or accidental interception, especially when transmission ranges and endpoints are well known and controlled.

Advanced security measures such as blockchain-based trust models or post-quantum key encapsulation are generally unnecessary in this context. These mechanisms are designed to mitigate high-assurance threats that are unlikely to occur in rural or industrial farming environments. Their deployment would introduce unjustified complexity and consume valuable energy without significantly improving threat resilience [31].

In summary, UAV operations in precision agriculture are best supported by lightweight, low-overhead security mechanisms that enable scalable deployment and maximize operational endurance. Security solutions must align with the domain's emphasis on autonomy, longevity, and efficient resource usage rather than comprehensive defense against sophisticated adversaries.

8.3. Disaster Response

In disaster-stricken environments, UAVs are often deployed to support real-time situational awareness, structural assessment, and victim localization. The operational landscape is typically unstable, with limited infrastructure, disrupted communication channels, and dynamic mission parameters [67]. UAVs engaged in these tasks transmit sensitive data, such as live video, environmental readings, and geolocation metrics, which may be intercepted or manipulated if left unprotected.

Disaster zones may also involve adversarial conditions, particularly in politically sensitive regions or during humanitarian conflicts. Potential threats include signal jamming, GPS spoofing, and malicious interference with control or telemetry streams [172]. These disruptions can delay response efforts, compromise safety, or distort situational intelligence.

Given these conditions, security mechanisms deployed in disaster scenarios tend to prioritize adaptability and lightweight implementation. Encryption protocols with low computational overhead are typically employed to preserve battery life while maintaining confidentiality. Dynamic key management supports rapidly changing topologies, allowing secure communication even when UAVs are introduced or removed from the network during operation.

Inter-agency coordination during disaster relief introduces the challenge of establishing trust between systems managed by different organizations. Decentralized trust models, including distributed ledgers or cross-certification schemes, can offer traceability and tamper resistance without relying on persistent centralized authority.

A multilayered security framework provides operational continuity, even when specific defenses are degraded. In such architectures, the loss or compromise of a single security layer does not result in complete system failure. This is particularly relevant in situations with intermittent ground control or delayed data synchronization.

The security profile for disaster response UAVs reflects the need for flexible and efficient protection strategies that function reliably under degraded, unpredictable, and time-sensitive conditions.

8.4. Logistics and Delivery

UAVs supporting logistics and delivery services operate in semi-structured environments where both operational efficiency and security are important. These systems typically navigate urban or suburban routes, often in autonomous or semi-autonomous modes, while transporting high-value or sensitive items [173]. Threats in this domain include unauthorized rerouting, payload interception, and manipulation of delivery authorization processes.

Preserving the integrity of predefined routes is a key requirement. Adversaries may attempt to hijack control links, spoof positional data, or redirect UAVs through compromised navigation channels. Lightweight cryptographic protocols and tightly managed session keys are commonly used to protect telemetry and navigation data [68]. These mechanisms help ensure that flight paths remain aligned with authorized delivery instructions, even under conditions of signal interference or attempted relay attacks.

Authenticating both the UAV and the recipient is important for preventing fraudulent handovers. PUF-based hardware authentication or blockchain-anchored verification systems can support this requirement by enabling device-specific identity checks and secure handoff logs [174]. These approaches also facilitate post-event audits, particularly in enterprise or regulated logistics contexts.

In addition to secure communication and hardware validation, access control policies at the application layer, such as role-based access control (RBAC), are often implemented to restrict operator privileges and prevent unauthorized command injection. Secure firmware update processes are equally important to defend against software tampering or rollback attacks.

The logistics and delivery domain emphasizes end-to-end integrity across the transport workflow, with a focus on real-time authentication, route validation, and protection of control logic from unauthorized manipulation.

8.5. Environmental Monitoring

UAVs deployed for environmental monitoring typically operate in sparsely populated or remote regions where adversarial interference is relatively unlikely [175]. These systems are primarily tasked with collecting long-term data on climate conditions, vegetation health, air quality, or water resources. In such scenarios, energy efficiency and scalability are prioritized to support large-scale or extended deployments.

Security mechanisms in this domain are often optimized for minimal computational overhead. Lightweight encryption techniques are generally adequate for maintaining confidentiality and data integrity during flight operations [176]. Static or infrequently rotated symmetric keys are often configured prior to deployment, as real-time key negotiation is typically unnecessary in isolated environments.

Although advanced trust mechanisms such as blockchain or PUF-based identity validation are less commonly applied in this setting, additional controls become relevant when UAVs transmit data to cloud-based storage or analytics platforms. Application-layer safeguards, including secure API access, data filtering, and privacy-preserving protocols, offer enhanced protection for environmental datasets and associated credentials.

As environmental monitoring applications evolve to incorporate multi-UAV coordination, real-time alerts, and third-party data sharing, there may be a need to adapt existing security architectures. Solutions that offer reliable protection while preserving low-power operation and long-range coverage are likely to remain fundamental.

8.6. Search and Rescue

Search and rescue operations require time-sensitive UAV deployments across complex and unpredictable terrains. These missions often involve continuous communication between aerial platforms and ground responders to support victim detection, guidance, and emergency triage logistics [177]. The transmitted data, which may include thermal imagery, GPS coordinates, and route information, is frequently sensitive and operationally critical.

Environmental and adversarial factors increase the likelihood of disruption. Signal loss due to terrain, jamming attempts, or targeted attacks on data streams could interfere with coordination and delay assistance [178]. Protection of control channels and situational data is therefore a core concern, particularly under resource constraints.

To address these risks, lightweight encryption protocols are commonly used to maintain data confidentiality and integrity without significant processing delay. Dynamic key management supports frequent rekeying as UAVs enter and exit the network, which helps maintain continuity in collaborative or mesh network topologies.

Multilayer security architectures enhance mission resilience by offering redundant protections. In the event of communication failure or identity spoofing, additional verification layers and autonomous fallback protocols can support partial mission continuation.

Search and rescue UAVs operate under conditions that demand responsiveness and adaptability. Security implementations must therefore align with fluctuating network configurations and intermittent access to ground infrastructure.

8.7. Infrastructure Inspection

UAVs used for infrastructure inspection operate in controlled environments and focus on visual and sensor-based evaluation of critical assets such as bridges, pipelines, and electrical lines [179]. The data they capture may expose structural vulnerabilities or operational irregularities, making confidentiality and data integrity important from both industrial and regulatory perspectives [180].

Since these UAVs often operate over extended durations and along linear infrastructures, their security protocols are designed to balance protection with endurance. Lightweight encryption helps safeguard telemetry and imaging data while minimizing energy consumption. Efficient key management practices, such as scheduled key updates or segmented encryption zones, support sustained secure operation with minimal communication overhead.

Application-layer security is critical once UAV data is integrated into backend systems. Inspection outputs are frequently shared with enterprise asset management platforms or analytics engines. As a result, secure APIs, access control policies, and data authentication mechanisms are used to maintain system-level integrity and restrict unauthorized access.

Although infrastructure inspection missions are less likely to be actively targeted during flight, the sensitivity of the data collected warrants continued attention to end-to-end security. Ensuring confidentiality during transmission, along with secure storage and controlled retrieval, supports both operational continuity and regulatory compliance.

8.8. Suitability Matrix for UAV Security Mechanisms

The effectiveness of a UAV security framework is highly dependent on the application domain in which the UAV operates. Each mission type presents distinct priorities related to latency, energy availability, interoperability, and threat level. Table 10 provides a comparative analysis of how well various security mechanisms and operational factors align with common UAV application scenarios. The matrix helps highlight which technologies are essential, optional, or less applicable across different operational contexts.

In summary, the selection and integration of security mechanisms must be closely aligned with the operational context, threat landscape, and resource constraints of each UAV application. Military and disaster response UAVs require the most comprehensive and adaptive security frameworks, while civilian applications such as agriculture and environmental monitoring can often prioritize efficiency and scalability over advanced cryptographic features [1,4,7,67,73,175,179].

Table 10. Expanded APS Matrix: Security Mechanism and Operational Requirement Suitability Across UAV Application Domains

Application Domain	LWE	KM	PQC	B/P	MLS	LS	BC	ID	TD
Military Surveillance	High	High	High	High	High	High	Medium	High	High
Precision Agriculture	Medium	Medium	Low	Low	Medium	Low	High	Low	Low
Disaster Response	High	High	Medium	Medium	High	High	Medium	High	High
Logistics & Delivery	High	High	Medium	Medium	High	Medium	Medium	Medium	Medium
Environmental Monitoring	Medium	Medium	Low	Low	Medium	Low	High	Medium	Low
Search & Rescue	High	High	Medium	Medium	High	High	Medium	High	Medium
Infrastructure Inspection	Medium	Medium	Low	Low	Medium	Medium	Medium	High	Low

LWE: Lightweight Encryption Techniques, **KM:** Key Management Schemes, **PQC:** PQC, **B/P:** Blockchain or PUF Trust Mechanisms, **MLS:** Multilayer Security Framework, **LS:** Latency Sensitivity, **BC:** Battery Constraint, **ID:** Interoperability Demand, **TD:** Trust Decentralization Need.

9. Current Limitations and Emerging Research Directions

Despite significant progress in lightweight cryptographic algorithms, decentralized trust mechanisms, and post-quantum encryption schemes, several critical challenges remain in securing UAV communication systems. These challenges arise from the operational complexity of aerial networks, which include dynamic topologies, constrained energy and computation resources, adversarial exposure, and increasing demands for interoperability. Moreover, existing solutions often lack practical validation across diverse UAV platforms and mission profiles. This section identifies key limitations in current security frameworks and highlights emerging research directions aimed at enhancing resilience, scalability, and regulatory alignment in next-generation UAV networks.

9.1. Secure Rekeying in Dynamic Swarm Topologies

Rekeying is essential to maintain forward secrecy and prevent key compromise during node mobility, departure, or failure. In UAV swarms, where topology changes are frequent and autonomous coordination is expected, rekeying protocols must adapt without inducing significant latency or computational burden. Existing solutions often suffer from scalability limitations or communication overhead, especially when the entire swarm must synchronize cryptographic material. New lightweight group key management approaches are required to support scalable and self-healing rekeying across dynamic UAV formations [138,181,182].

9.2. Defending Against Cross-Layer and Coordinated Attacks

UAV systems face security threats at every layer of the protocol stack, including physical jamming, MAC spoofing, routing manipulation, and data tampering at the application layer. Moreover, cross-layer attacks, which exploit interactions between layers, present a sophisticated threat model that is often overlooked by single-layer defense mechanisms. Integrated security frameworks that span the full communication stack and leverage anomaly detection, AI-enhanced monitoring, and protocol-aware resilience strategies are increasingly necessary [22,183].

9.3. Lack of Security Standards and Interoperability Guidelines

The absence of standardized, UAV-specific cryptographic frameworks continues to hinder secure interoperability across heterogeneous aerial systems. Although regulatory agencies such as the FAA and EASA have introduced cybersecurity requirements for UAVs, a unified guideline covering lightweight encryption protocols, decentralized trust infrastructures, and post-quantum secure key exchange mechanisms is still lacking. Ongoing standardization efforts, including those led by NIST and other international collaborative bodies, must prioritize a balance between implementation feasibility and strong cryptographic assurances that are compatible with real-time, energy-constrained UAV operations [184,185].

9.4. PQC Deployment in UAV Systems

As quantum computing advances, traditional public-key infrastructures face increasing vulnerabilities. Post-quantum cryptography, particularly lattice-based and code-based schemes such as Kyber, NTRU, and Classic McEliece, offers promising resilience against quantum threats. However, the computational complexity and memory requirements of these algorithms present significant challenges for integration into UAV systems with constrained resources. Although hybrid approaches that combine classical and quantum-resistant methods (for example, ECDH with Kyber) and hardware acceleration using FPGAs or GPUs offer potential mitigation strategies, further research is necessary to support efficient deployment and long-term compatibility within aerial communication networks [7,30,186].

9.5. Energy-Efficient Security Solutions

UAV platforms are energy-constrained by design, and cryptographic operations contribute significantly to power consumption, especially in multi-hop or high-throughput scenarios. Lightweight encryption algorithms such as ASCON and energy-aware key exchange schemes have demonstrated promise, but optimal trade-offs between security strength, computation cost, and battery life are still poorly defined. Emerging techniques, such as reinforcement learning for the adaptation of encryption strategies or context-sensitive cipher selection, require further validation through field-deployable testbeds, as discussed in recent efforts to model energy-sensitive encryption schemes for UAVs [13,31].

9.6. Physical Layer and Environmental Considerations

UAVs operating in urban landscapes or rugged terrains encounter significant physical-layer impairments, including non-line-of-sight propagation, multipath fading, Doppler shifts, and environmental interference. These effects reduce signal reliability and increase vulnerability to jamming, spoofing, and eavesdropping attacks. To mitigate these risks, future UAV systems must incorporate physical layer security (PLS) techniques such as beamforming, cooperative relaying, frequency hopping, and reconfigurable intelligent surfaces. These methods can dynamically adapt to propagation characteristics to enhance confidentiality, resilience, and spectral efficiency [34,160].

9.7. Data Privacy and Regulation Compliance

The proliferation of UAVs in civilian surveillance, logistics, and smart infrastructure raises growing concerns around user privacy and regulatory compliance. UAVs frequently capture sensitive data such as facial imagery, behavioral patterns, and geolocation histories. While encryption protects data in transit, privacy-by-design principles remain underdeveloped in UAV communication frameworks. Future protocols must incorporate techniques such as differential privacy, secure multi-party computation, homomorphic encryption, and privacy-preserving data aggregation. Furthermore, UAV systems must align with international data protection standards (e.g., GDPR, CCPA), which are not yet fully addressed in existing security architectures [22,187].

9.8. AI-Driven and Autonomous Security Management

Artificial intelligence (AI) is poised to play a transformative role in UAV cybersecurity by enabling autonomous detection, prediction, and mitigation of threats. Machine learning models can support anomaly detection, adaptive trust assessment, and context-aware encryption strategies. However, AI-driven systems also introduce new risks, such as susceptibility to adversarial inputs, model inversion, and data poisoning attacks. In safety-critical UAV deployments, explainable and robust AI architectures must be developed to ensure transparency, accountability, and fault tolerance under adversarial conditions. This area remains underexplored and requires close coordination between AI, embedded systems, and cryptographic research communities [29,188].

Table 11 summarizes the key security challenges discussed in this section, along with their corresponding research opportunities and emerging solutions tailored for UAV communication systems.

Table 11. Summary of Current Limitations and Emerging Research Directions for UAV Communication Security

Challenge Area	Problem Summary	Research Direction / Solution
Secure Rekeying in Swarms	Frequent topology changes and synchronization overhead in UAV swarms	Lightweight group key management and self-healing rekeying schemes
Cross-Layer and Coordinated Attacks	Attacks span multiple protocol layers; existing defenses are siloed	Integrated, full-stack security with anomaly detection and AI-enhanced resilience
Lack of Security Standards	Absence of UAV-specific cryptographic and interoperability guidelines	Standardization of lightweight, decentralized, and post-quantum frameworks
PQC Deployment	High computational cost of PQC algorithms on UAVs	Hybrid schemes (e.g., ECDH+Kyber), hardware acceleration, resource-aware tuning
Energy-Efficient Security	High power consumption of cryptographic operations impacts mission time	Adaptive encryption selection, reinforcement learning for energy-aware security
Physical Layer Security	Urban and rugged terrain introduces multipath, jamming, and Doppler effects	Use of beamforming, cooperative relaying, frequency hopping, and RIS
Data Privacy Compliance	UAVs collect sensitive personal data but lack privacy-preserving design	Integration of differential privacy, secure aggregation, GDPR-aligned protocols
AI-Based Security Management	AI enables autonomous threat detection but poses risks like adversarial attacks	Research into explainable, robust, and fault-tolerant AI for embedded UAV systems

9.9. Path Forward

Securing UAV communication requires interdisciplinary collaboration across cryptography, wireless systems, artificial intelligence, embedded hardware, and policy domains. Emphasis must be placed on designing lightweight, quantum-resistant cryptographic protocols; developing scalable key management schemes; establishing interoperable security standards; and ensuring privacy-preserving mechanisms for sensitive data. Future systems should incorporate adaptive, multilayer security models that can respond in real time to evolving threats. The path forward demands joint efforts from academia, industry stakeholders, and regulatory bodies to align innovation with practical deployment and compliance needs.

10. Conclusions

The rapid adoption of UAVs across diverse domains has introduced unprecedented opportunities and significant security challenges. As UAVs become more autonomous and interconnected through wireless networks, ensuring the confidentiality, integrity, authenticity, and availability of their communication systems becomes essential for mission success. This paper has provided a structured and in-depth analysis of communication security for UAVs by examining core threats, evaluating emerging countermeasures, and contextualizing these mechanisms across major UAV application scenarios.

We have explored five key technological strategies that address the growing vulnerabilities in UAV communications: lightweight encryption techniques, key management protocols, PQC, trust establishment through blockchain or PUFs, and multilayer security frameworks. Each mechanism was evaluated for its computational efficiency, scalability, and adaptability under real-world UAV constraints. Our taxonomy highlighted how the suitability of these security techniques varies depending on the operational context, from high-risk military operations to resource-constrained environmental monitoring.

By analyzing application-specific requirements such as latency sensitivity, energy availability, and interoperability demands, we developed a comprehensive suitability matrix. This matrix provides a comparative perspective across multiple UAV domains including military surveillance, precision agriculture, disaster response, logistics and delivery, environmental monitoring, search and rescue, and infrastructure inspection. The analysis revealed that no single security mechanism is universally optimal. Instead, effective UAV security design depends on selecting and tailoring mechanisms that align with both the threat landscape and operational goals of each domain.

The paper also discussed the relevance of future-proofing UAV communications using post-quantum cryptographic algorithms and the use of decentralized trust mechanisms for multi-agency collaboration. Techniques such as ASCON, Kyber, and NTRU, along with emerging implementations of blockchain-based routing validation and PUF-based device authentication, show considerable promise in advancing secure UAV deployments.

In closing, this work underscores the importance of designing UAV security frameworks that are lightweight, context-aware, and resilient. Future research should focus on optimizing cryptographic primitives for resource-constrained UAV platforms, standardizing evaluation metrics, and enabling real-time threat adaptation through integrated sensing and secure AI. As the UAV landscape evolves to support 6G connectivity, edge intelligence, and autonomous swarms, ensuring robust communication security will remain critical for operational trust, system survivability, and public safety.

Author Contributions: Conceptualization, S. Sarkar; methodology, S. Sarkar; validation, S. Sarkar, S. Shafaei, and T. S. Jones; formal analysis, S. Sarkar; investigation, S. Sarkar, S. Shafaei,T. S. Jones; resources, S. Sarkar, S. Shafaei,T. S. Jones; data curation, S. Sarkar, S. Shafaei,T. S. Jones, M. W. Totaro ; writing—original draft preparation, S. Sarkar, S. Shafaei and T. S. Jones; writing, review and editing, S. Sarkar and M. W. Totaro; visualization, S. Sarkar, S. Shafaei and T. S. Jones; supervision, M. W. Totaro; project administration, S. Sarkar. All authors have read and agreed to the published version of the manuscript.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflicts of interest

References

1. Telli, K.; Kraa, O.; Himeur, Y.; Ouamane, A.; Boumehraz, M.; Atalla, S.; Mansoor, W. A comprehensive review of recent research trends on unmanned aerial vehicles (uavs). *Systems* **2023**, *11*, 400.
2. Abro, G.E.M.; Zulkifli, S.A.B.; Masood, R.J.; Asirvadam, V.S.; Laouiti, A. Comprehensive review of UAV detection, security, and communication advancements to prevent threats. *Drones* **2022**, *6*, 284.
3. Yang, Z.; Xu, W.; Shikh-Bahaei, M. Energy efficient UAV communication with energy harvesting. *IEEE Transactions on Vehicular Technology* **2019**, *69*, 1913–1927.
4. Patel, A.; Cherukuri, A.K. Analysis of Light-Weight Cryptography Algorithms for UAV-Networks. *arXiv preprint arXiv:2504.04063* **2025**.
5. Meer, I.A.; Besser, K.L.; Ozger, M.; Schupke, D.; Poor, H.V.; Cavdar, C. Hierarchical Multi-Agent DRL Based Dynamic Cluster Reconfiguration for UAV Mobility Management. *arXiv preprint arXiv:2412.16167* **2024**.
6. Lei, Y.; Zeng, L.; Li, Y.X.; Wang, M.X.; Qin, H. A lightweight authentication protocol for UAV networks based on security and computational resource optimization. *IEEE Access* **2021**, *9*, 53769–53785.
7. Khan, M.A.; Javaid, S.; Mohsan, S.A.H.; Tanveer, M.; Ullah, I. Future-proofing security for UAVs with post-quantum cryptography: A review. *IEEE Open Journal of the Communications Society* **2024**.
8. Xia, T.; Wang, M.; He, J.; Yang, G.; Fan, L.; Wei, G. A Quantum-Resistant Identity Authentication and Key Agreement Scheme for UAV Networks Based on Kyber Algorithm. *Drones* **2024**, *8*, 359.
9. Hossain, M.I.; Tahtali, M.; Turhan, U.; Biswas, K. Blockchain Integration in UAV Networks: Performance Metrics and Analysis. *Sensors* **2024**, *24*, 7813.
10. Hafeez, S.; Shawky, M.A.; Al-Quraan, M.; Mohjazi, L.; Imran, M.A.; Sun, Y. Beta-UAV: blockchain-based efficient authentication for secure UAV communication. *arXiv preprint arXiv:2402.15817* **2024**.

11. Ranjitha, K.; Pathak, D.; Tammana, P.; Alladi, T.; et al. Accelerating PUF-based UAV authentication protocols using programmable switch. In Proceedings of the 2022 14th International Conference on COMmunication Systems & NETworkS (COMSNETS). IEEE, 2022, pp. 309–313.
12. Avery, J.; Fraelich, B.; Duran, W.; Lee, A.; Sullivan, A.; Mechalke, Z.; Birrer, M.; Dick, S.; Cochran, J. Analysis of practical application of lightweight cryptographic algorithm ascon. *Computer Security Resource Center* **2022**.
13. Li, T.; Zhang, J.; Obaidat, M.S.; Lin, C.; Lin, Y.; Shen, Y.; Ma, J. Energy-efficient and secure communication toward UAV networks. *IEEE Internet of Things Journal* **2021**, *9*, 10061–10076.
14. Federal Aviation Administration. Equipment, Systems, and Network Information Security Protection (2120-AL94): Notice of Proposed Rulemaking. https://www.regulations.gov/docket/FAA-2024-1398, 2024. Docket No. FAA-2024-1398.
15. European Union Aviation Safety Agency. Easy Access Rules for Unmanned Aircraft Systems: Regulations (EU) 2019/947 and 2019/945. Technical report, EASA, 2024. Consolidated version with amendments and guidance material.
16. Pandey, G.K.; Gurjar, D.S.; Nguyen, H.H.; Yadav, S. Security threats and mitigation techniques in UAV communications: A comprehensive survey. *IEEE Access* **2022**, *10*, 112858–112897.
17. Rupasinghe, N.; Yapici, Y.; Guvenc, I.; Dai, H.; Bhuyan, A. Physical layer security for UAV communications. *UAV Communications for 5G and Beyond* **2020**, pp. 373–397.
18. Wang, J.; Wang, X.; Gao, R.; Lei, C.; Feng, W.; Ge, N.; Jin, S.; Quek, T.Q. Physical layer security for UAV communications: A comprehensive survey. *China Communications* **2022**, *19*, 77–115.
19. Xiaoning, Z. Analysis of military application of UAV swarm technology. In Proceedings of the 2020 3rd International Conference on Unmanned Systems (ICUS). IEEE, 2020, pp. 1200–1204.
20. Jin, H.; Zhou, Y.; Jin, X.; Zhang, S. Energy-efficient UAV communication: A NOMA scheme with resource allocation and trajectory optimization. *Plos one* **2024**, *19*, e0301819.
21. Abdullayeva, F.; Valikhanli, O. A survey on UAVs security issues: attack modeling, security aspects, countermeasures, open issues. *Control and Cybernetics* **2023**, *52*, 405–439.
22. Mekdad, Y.; Aris, A.; Babun, L.; El Fergougui, A.; Conti, M.; Lazzeretti, R.; Uluagac, A.S. A survey on security and privacy issues of UAVs. *Computer networks* **2023**, *224*, 109626.
23. Felix, O.O. Securing the skies: A comprehensive survey on internet of drones security challenges and solutions. *architecture* **2023**, *45*, 46.
24. Rugo, A.; Ardagna, C.A.; Ioini, N.E. A security review in the UAVNet era: Threats, countermeasures, and gap analysis. *ACM Computing Surveys (CSUR)* **2022**, *55*, 1–35.
25. Tang, A.C. A review on cybersecurity vulnerabilities for urban air mobility. In Proceedings of the Aiaa scitech 2021 forum, 2021, p. 0773.
26. Patel, T.; Salot, N.; Parikh, V. A systematic literature review on Security of Unmanned Aerial Vehicle Systems. *arXiv preprint arXiv:2212.05028* **2022**.
27. Niyonsaba, S.; Konate, K.; Soidridine, M.M. A Survey on Cybersecurity in Unmanned Aerial Vehicles: Cyberattacks, Defense Techniques and Future Research Directions. *International Journal of Computer Networks and Applications* **2023**, *10*, 688.
28. Choi, J.; Son, S.; Kwon, D.; Park, Y. A PUF-Based Secure Authentication and Key Agreement Scheme for the Internet of Drones. *Sensors* **2025**, *25*, 982.
29. Tlili, F.; Ayed, S.; Fourati, L.C. Advancing UAV security with artificial intelligence: A comprehensive survey of techniques and future directions. *Internet of Things* **2024**, p. 101281.
30. Aissaoui, R.; Deneuville, J.C.; Guerber, C.; Pirovano, A. Evaluating Post-Quantum Key Exchange Mechanisms for UAV Communication Security. In Proceedings of the 2024 AIAA DATC/IEEE 43rd Digital Avionics Systems Conference (DASC). IEEE, 2024, pp. 1–10.
31. Gu, X.; Zhang, G.; Wang, M.; Duan, W.; Wen, M.; Ho, P.H. UAV-aided energy-efficient edge computing networks: Security offloading optimization. *IEEE Internet of Things Journal* **2021**, *9*, 4245–4258.
32. Sun, X.; Ng, D.W.K.; Ding, Z.; Xu, Y.; Zhong, Z. Physical layer security in UAV systems: Challenges and opportunities. *IEEE Wireless Communications* **2019**, *26*, 40–47.
33. Wu, Q.; Mei, W.; Zhang, R. Safeguarding wireless network with UAVs: A physical layer security perspective. *IEEE Wireless Communications* **2019**, *26*, 12–18.
34. Xu, F.; Ahmad, S.; Ahmed, M.; Raza, S.; Khan, F.; Ma, Y.; Khan, W.U.; et al. Beyond encryption: Exploring the potential of physical layer security in UAV networks. *Journal of King Saud University-Computer and Information Sciences* **2023**, *35*, 101717.

35. Lu, H.; Zhang, H.; Dai, H.; Wu, W.; Wang, B. Proactive eavesdropping in UAV-aided suspicious communication systems. *IEEE Transactions on Vehicular Technology* **2018**, *68*, 1993–1997.
36. Ceviz, O.; Sen, S.; Sadioglu, P. A survey of security in uavs and fanets: Issues, threats, analysis of attacks, and solutions. *IEEE Communications Surveys & Tutorials* **2024**.
37. Tsao, K.Y.; Girdler, T.; Vassilakis, V.G. A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks. *Ad Hoc Networks* **2022**, *133*, 102894.
38. Wang, Z.; Li, Y.; Wu, S.; Zhou, Y.; Yang, L.; Xu, Y.; Zhang, T.; Pan, Q. A survey on cybersecurity attacks and defenses for unmanned aerial systems. *Journal of Systems Architecture* **2023**, *138*, 102870.
39. Emani, R. Cybersecurity Analysis and Defense of the MAVLink UAS Protocol **2024**.
40. Koubâa, A.; Allouch, A.; Alajlan, M.; Javed, Y.; Belghith, A.; Khalgui, M. Micro air vehicle link (mavlink) in a nutshell: A survey. *IEEE Access* **2019**, *7*, 87658–87680.
41. Baek, H.; Lim, J. Design of future UAV-relay tactical data link for reliable UAV control and situational awareness. *IEEE Communications Magazine* **2018**, *56*, 144–150.
42. Thakur, A.; Sharma, S.K.; Bhogey, R.K.; et al. EVALUATING AD-HOC NETWORK PERFORMANCE AGAINST BLACK HOLE, SYBIL, AND DDOS ATTACKS. *Machine Intelligence Research* **2024**, *18*, 161–173.
43. Younas, S.; Rehman, F.; Maqsood, T.; Mustafa, S.; Akhunzada, A.; Gani, A. Collaborative detection of black hole and gray hole attacks for secure data communication in VANETs. *Applied Sciences* **2022**, *12*, 12448.
44. Wang, X.; Zhao, Z.; Yi, L.; Ning, Z.; Guo, L.; Yu, F.R.; Guo, S. A Survey on Security of UAV Swarm Networks: Attacks and Countermeasures. *ACM Computing Surveys* **2024**, *57*, 1–37.
45. Khan, N.A.; Jhanjhi, N.; Brohi, S.N.; Almazroi, A.A.; Almazroi, A.A. A secure communication protocol for unmanned aerial vehicles. *CMC-Computers Materials & Continua* **2022**, *70*, 601–618.
46. Choe, H.; Kang, D. ECC based Authentication Protocol for Military Internet of Drone (IoD): A Holistic Security Framework. *IEEE Access* **2025**.
47. Catuogno, L.; Galdi, C. Secure Firmware Update: Challenges and Solutions. *Cryptography* **2023**, *7*, 30.
48. Ficco, M.; Esposito, C.; Aloi, G.; Palmieri, F. MAVLink Protocol for Unmanned Aerial Vehicle: Vulnerabilities Analysis. In Proceedings of the 2022 IEEE International Conference on Dependable, Autonomic and Secure Computing, International Conference on Pervasive Intelligence and Computing, International Conference on Cloud and Big Data Computing, International Conference on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech). IEEE, 2022, pp. 453–460. https://doi.org/10.1109/DASC/PiCom/CBDCom/CyberSciTech56310.2022.00080.
49. Pathak, D.; Ranjitha, K.; Tammana, P.; Alladi, T. Accelerating PUF-Based Authentication Protocols Using Programmable Switch. In Proceedings of the NOMS 2023–2023 IEEE/IFIP Network Operations and Management Symposium. IEEE, 2023, pp. 1–6. https://doi.org/10.1109/NOMS56928.2023.10154451.
50. Mouha, N. The design space of lightweight cryptography. *Cryptology ePrint Archive* **2015**.
51. Buchanan, W.J.; Li, S.; Asif, R. Lightweight cryptography methods. *Journal of Cyber Security Technology* **2017**, *1*, 187–201.
52. Aljaedi, A.; Alharbi, A.R.; Aljuhni, A.; Alghuson, M.K.; Alassmi, S.; Shafique, A. A lightweight encryption algorithm for resource-constrained IoT devices using quantum and chaotic techniques with metaheuristic optimization. *Scientific Reports* **2025**, *15*, 14050.
53. Hatzivasilis, G.; Fysarakis, K.; Papaefstathiou, I.; Manifavas, C. A review of lightweight block ciphers. *Journal of cryptographic Engineering* **2018**, *8*, 141–184.
54. Salama, D.; Kader, H.A.; Hadhoud, M. Studying the effects of most common encryption algorithms. *International Arab Journal of e-technology* **2011**, *2*, 1–10.
55. Alizadeh, M.; Salleh, M.; Zamani, M.; Shayan, J.; Karamizadeh, S. Security and performance evaluation of lightweight cryptographic algorithms in RFID. *Kos Island, Greece* **2012**, pp. 45–50.
56. Prakasam, P.; Madheswaran, M.; Sujith, K.; Sayeed, M.S. Low latency, area and optimal power hybrid lightweight cryptography authentication scheme for internet of things applications. *Wireless Personal Communications* **2022**, *126*, 351–365.
57. Bogdanov, A.; Knudsen, L.R.; Leander, G.; Paar, C.; Poschmann, A.; Robshaw, M.J.; Seurin, Y.; Vikkelsoe, C. PRESENT: An ultra-lightweight block cipher. In Proceedings of the Cryptographic Hardware and Embedded Systems-CHES 2007: 9th International Workshop, Vienna, Austria, September 10-13, 2007. Proceedings 9. Springer, 2007, pp. 450–466.
58. Abed, F.; List, E.; Lucks, S.; Wenzel, J. Cryptanalysis of the speck family of block ciphers. *Cryptology ePrint Archive* **2013**.

59. Beaulieu, R.; Shors, D.; Smith, J.; Treatman-Clark, S.; Weeks, B.; Wingers, L. The SIMON and SPECK lightweight block ciphers. In Proceedings of the Proceedings of the 52nd annual design automation conference, 2015, pp. 1–6.
60. De Canniere, C.; Preneel, B. Trivium. In *New Stream Cipher Designs: The eSTREAM Finalists*; Springer, 2008; pp. 244–266.
61. Hell, M.; Johansson, T.; Meier, W. Grain: a stream cipher for constrained environments. *International journal of wireless and mobile computing* **2007**, *2*, 86–93.
62. Miller, V.S. Use of elliptic curves in cryptography. In Proceedings of the Conference on the theory and application of cryptographic techniques. Springer, 1985, pp. 417–426.
63. Koblitz, N. Elliptic curve cryptosystems. *Mathematics of computation* **1987**, *48*, 203–209.
64. Lara-Nino, C.A.; Diaz-Perez, A.; Morales-Sandoval, M. Elliptic curve lightweight cryptography: A survey. *Ieee Access* **2018**, *6*, 72514–72550.
65. Semsch, E.; Jakob, M.; Pavlicek, D.; Pechoucek, M. Autonomous UAV surveillance in complex urban environments. In Proceedings of the 2009 IEEE/WIC/ACM International Joint Conference on Web Intelligence and Intelligent Agent Technology. IEEE, 2009, Vol. 2, pp. 82–85.
66. Asadzadeh, S.; de Oliveira, W.J.; de Souza Filho, C.R. UAV-based remote sensing for the petroleum industry and environmental monitoring: State-of-the-art and perspectives. *Journal of Petroleum Science and Engineering* **2022**, *208*, 109633.
67. Hildmann, H.; Kovacs, E. Using unmanned aerial vehicles (UAVs) as mobile sensing platforms (MSPs) for disaster response, civil security and public safety. *Drones* **2019**, *3*, 59.
68. Dorling, K.; Heinrichs, J.; Messier, G.G.; Magierowski, S. Vehicle routing problems for drone delivery. *IEEE Transactions on Systems, Man, and Cybernetics: Systems* **2016**, *47*, 70–85.
69. Chiang, W.C.; Li, Y.; Shang, J.; Urban, T.L. Impact of drone delivery on sustainability and cost: Realizing the UAV potential through vehicle routing optimization. *Applied energy* **2019**, *242*, 1164–1175.
70. Roberge, V.; Tarbouchi, M.; Labonté, G. Fast genetic algorithm path planner for fixed-wing military UAV using GPU. *IEEE Transactions on Aerospace and Electronic Systems* **2018**, *54*, 2105–2117.
71. Outay, F.; Mengash, H.A.; Adnan, M. Applications of unmanned aerial vehicle (UAV) in road safety, traffic and highway infrastructure management: Recent advances and challenges. *Transportation research part A: policy and practice* **2020**, *141*, 116–129.
72. Tsouros, D.C.; Bibi, S.; Sarigiannidis, P.G. A review on UAV-based applications for precision agriculture. *Information* **2019**, *10*, 349.
73. Scherer, J.; Rinner, B. Multi-UAV surveillance with minimum information idleness and latency constraints. *IEEE Robotics and Automation Letters* **2020**, *5*, 4812–4819.
74. Motlagh, N.H.; Bagaa, M.; Taleb, T. UAV-based IoT platform: A crowd surveillance use case. *IEEE Communications Magazine* **2017**, *55*, 128–134.
75. Maddikunta, P.K.R.; Hakak, S.; Alazab, M.; Bhattacharya, S.; Gadekallu, T.R.; Khan, W.Z.; Pham, Q.V. Unmanned aerial vehicles in smart agriculture: Applications, requirements, and challenges. *IEEE sensors journal* **2021**, *21*, 17608–17619.
76. Betti Sorbelli, F. UAV-based delivery systems: A systematic review, current trends, and research challenges. *Journal on Autonomous Transportation Systems* **2024**, *1*, 1–40.
77. Noorwali, A.; Javed, M.A.; Khan, M.Z. Efficient UAV Communications: Recent Trends and Challenges. *Computers, Materials & Continua* **2021**, *67*.
78. Vandersteegen, M.; Van Beeck, K.; Goedemé, T. Super accurate low latency object detection on a surveillance UAV. In Proceedings of the 2019 16th International Conference on Machine Vision Applications (MVA). IEEE, 2019, pp. 1–6.
79. Jin, H.; Jin, X.; Zhou, Y.; Guo, P.; Ren, J.; Yao, J.; Zhang, S. A survey of energy efficient methods for UAV communication. *Vehicular Communications* **2023**, *41*, 100594.
80. Abubakar, A.I.; Ahmad, I.; Omeke, K.G.; Ozturk, M.; Ozturk, C.; Abdel-Salam, A.M.; Mollel, M.S.; Abbasi, Q.H.; Hussain, S.; Imran, M.A. A survey on energy optimization techniques in UAV-based cellular networks: from conventional to machine learning approaches. *Drones* **2023**, *7*, 214.
81. Kumar, N. Energy efficient communication methods for unmanned ariel vehicles (UAVs): last five years' study. *Unmanned Aerial Vehicles for Internet of Things (IoT) Concepts, Techniques, and Applications* **2021**, pp. 73–88.
82. Nawaz, H.; Ali, H.M.; Laghari, A.A. UAV communication networks issues: A review. *Archives of Computational Methods in Engineering* **2021**, *28*, 1349–1369.

83. Di, H.; Zhu, X.; Liu, Z.; Tu, X. Joint blocklength and trajectory optimizations for urllc-enabled uav relay system. *IEEE Communications Letters* **2023**, *28*, 118–122.
84. Huang, Y.; Cui, M.; Zhang, G.; Chen, W. Bandwidth, power and trajectory optimization for UAV base station networks with backhaul and user QoS constraints. *IEEE Access* **2020**, *8*, 67625–67634.
85. Saleab, M.; Sax, F.; Schumann, J.; Holzapfel, F. Low-level memory and timing analysis of flight code for unmanned aerial systems. *Aerospace Systems* **2024**, *7*, 209–225.
86. Iacovelli, G.; Boccadoro, P.; Grieco, L.A. On the interplay between energy and memory constraints in optimized uav communications. *IEEE Networking Letters* **2020**, *2*, 203–206.
87. Thammawichai, M.; Baliyarasimhuni, S.P.; Kerrigan, E.C.; Sousa, J.B. Optimizing communication and computation for multi-UAV information gathering applications. *IEEE Transactions on Aerospace and Electronic Systems* **2017**, *54*, 601–615.
88. Khalid, R.; Shah, Z.; Naeem, M.; Ali, A.; Al-Fuqaha, A.; Ejaz, W. Computational efficiency maximization for UAV-assisted MEC networks with energy harvesting in disaster scenarios. *IEEE Internet of Things Journal* **2023**, *11*, 9004–9018.
89. Jouhari, M.; Al-Ali, A.K.; Baccour, E.; Mohamed, A.; Erbad, A.; Guizani, M.; Hamdi, M. Distributed CNN inference on resource-constrained UAVs for surveillance systems: Design and optimization. *IEEE Internet of Things Journal* **2021**, *9*, 1227–1242.
90. Mohd, B.J.; Hayajneh, T.; Vasilakos, A.V. A survey on lightweight block ciphers for low-resource devices: Comparative study and open issues. *Journal of Network and Computer Applications* **2015**, *58*, 73–93.
91. McKay, K.; Bassham, L.; Sönmez Turan, M.; Mouha, N. Report on lightweight cryptography. Technical report, National Institute of Standards and Technology, 2016.
92. Al-Yousfi, E.A.; Alkhawlani, M. Comprehensive Survey of Lightweight Ciphers for Resource-Constrained IoT Devices. *University of Science and Technology Journal for Engineering and Technology* **2025**, *3*, 77–115.
93. Son, S.; Kwon, D.; Lee, S.; Jeon, Y.; Das, A.K.; Park, Y. Design of secure and lightweight authentication scheme for UAV-enabled intelligent transportation systems using blockchain and PUF. *IEEE Access* **2023**, *11*, 60240–60253.
94. Nikooghadam, M.; Amintoosi, H.; Islam, S.H.; Moghadam, M.F. A provably secure and lightweight authentication scheme for Internet of Drones for smart city surveillance. *Journal of Systems Architecture* **2021**, *115*, 101955.
95. Zhang, J.; Gu, P.; Wang, Z.; Zou, J.; Liu, G. A Low-Complexity Security Scheme for Drone Communication Based on PUF and LDPC. *Drones* **2024**, *8*, 472.
96. Thakor, V.A.; Razzaque, M.A.; Khandaker, M.R. Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities. *IEEE Access* **2021**, *9*, 28177–28193.
97. Okello, W.J.; Liu, Q.; Siddiqui, F.A.; Zhang, C. A survey of the current state of lightweight cryptography for the Internet of things. In Proceedings of the 2017 International Conference on Computer, Information and Telecommunication Systems (CITS). IEEE, 2017, pp. 292–296.
98. Pu, C.; Wall, A.; Choo, K.K.R.; Ahmed, I.; Lim, S. A lightweight and privacy-preserving mutual authentication and key agreement protocol for Internet of Drones environment. *IEEE Internet of Things Journal* **2022**, *9*, 9918–9933.
99. Ning, L.; Ali, Y.; Ke, H.; Nazir, S.; Huanli, Z. A hybrid MCDM approach of selecting lightweight cryptographic cipher based on ISO and NIST lightweight cryptography security requirements for internet of health things. *IEEE Access* **2020**, *8*, 220165–220187.
100. De Canniere, C.; Dunkelman, O.; Knežević, M. KATAN and KTANTAN—a family of small and efficient hardware-oriented block ciphers. In Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems. Springer, 2009, pp. 272–288.
101. Fadhil, K.; Batan, A.B. Advancing Lightweight Cryptographic Techniques for Encrypted Drone Data in Cooperative Smart Grid Transportation. *Open Journal of Robotics, Autonomous Decision-Making, and Human-Machine Interaction* **2024**, *9*, 10–17.
102. Dhanda, S.S.; Singh, B.; Jindal, P. Lightweight cryptography: a solution to secure IoT. *Wireless Personal Communications* **2020**, *112*, 1947–1980.
103. Singh, S.; Sharma, P.K.; Moon, S.Y.; Park, J.H. Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions. *Journal of Ambient Intelligence and Humanized Computing* **2024**, pp. 1–18.
104. Stallings, W. *Cryptography and network security, 4/E*; Pearson Education India, 2006.
105. Bansod, G.; Raval, N.; Pisharoty, N. Implementation of a new lightweight encryption design for embedded security. *IEEE Transactions on Information Forensics and Security* **2014**, *10*, 142–151.

106. Alshamsi, R.; Naouss, M. Communication Security for UAV in military **2025**.
107. Eisenbarth, T.; Gong, Z.; Güneysu, T.; Heyse, S.; Indesteege, S.; Kerckhof, S.; Koeune, F.; Nad, T.; Plos, T.; Regazzoni, F.; et al. Compact implementation and performance evaluation of block ciphers in ATtiny devices. In Proceedings of the Progress in Cryptology-AFRICACRYPT 2012: 5th International Conference on Cryptology in Africa, Ifrance, Morocco, July 10-12, 2012. Proceedings 5. Springer, 2012, pp. 172–187.
108. Jassim, S.A.; Farhan, A.K. A survey on stream ciphers for constrained environments. In Proceedings of the 2021 1st Babylon International Conference on Information Technology and Science (BICITS). IEEE, 2021, pp. 228–233.
109. Manifavas, C.; Hatzivasilis, G.; Fysarakis, K.; Papaefstathiou, Y. A survey of lightweight stream ciphers for embedded systems. *Security and Communication Networks* **2016**, *9*, 1226–1246.
110. Robshaw, M.; Billet, O. *New stream cipher designs: the eSTREAM finalists*; Vol. 4986, Springer, 2008.
111. Bernstein, D.J. The Salsa20 family of stream ciphers. In *New stream cipher designs: the eSTREAM finalists*; Springer, 2008; pp. 84–97.
112. Bernstein, D.J.; et al. ChaCha, a variant of Salsa20. In Proceedings of the Workshop record of SASC. Lausanne, Switzerland, 2008, Vol. 8, pp. 3–5.
113. Hasan, H.; Ali, G.; Elmedany, W.; Balakrishna, C. Lightweight encryption algorithms for internet of things: a review on security and performance aspects. In Proceedings of the 2022 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT). IEEE, 2022, pp. 239–244.
114. Van Tilborg, H.C.; Jajodia, S. *Encyclopedia of cryptography and security*; Springer Science & Business Media, 2014.
115. Liu, Z.; Weng, J.; Hu, Z.; Seo, H. Efficient elliptic curve cryptography for embedded devices. *ACM Transactions on Embedded Computing Systems (TECS)* **2016**, *16*, 1–18.
116. Boneh, D.; Franklin, M. Identity-based encryption from the Weil pairing. In Proceedings of the Annual international cryptology conference. Springer, 2001, pp. 213–229.
117. Tan, C.C.; Wang, H.; Zhong, S.; Li, Q. IBE-Lite: A lightweight identity-based cryptography for body sensor networks. *IEEE Transactions on Information Technology in Biomedicine* **2009**, *13*, 926–932.
118. Jordan, S.P.; Liu, Y.K. Quantum cryptanalysis: shor, grover, and beyond. *IEEE Security & Privacy* **2018**, *16*, 14–21.
119. Kumar, A.; Bhatia, S.; Kaushik, K.; Gandhi, S.M.; Devi, S.G.; Pacheco, D.A.D.J.; Mashat, A. Survey of promising technologies for quantum drones and networks. *Ieee Access* **2021**, *9*, 125868–125911.
120. Alagic, G.; Alagic, G.; Apon, D.; Cooper, D.; Dang, Q.; Dang, T.; Kelsey, J.; Lichtinger, J.; Liu, Y.K.; Miller, C.; et al. Status report on the third round of the NIST post-quantum cryptography standardization process **2022**.
121. Fernández-Caramés, T.M. From pre-quantum to post-quantum IoT security: A survey on quantum-resistant cryptosystems for the Internet of Things. *IEEE Internet of Things Journal* **2019**, *7*, 6457–6480.
122. Bernstein, D.J.; Lange, T. Post-quantum cryptography. *Nature* **2017**, *549*, 188–194.
123. Halak, B.; Gibson, T.; Henley, M.; Botea, C.B.; Heath, B.; Khan, S. Evaluation of performance, energy, and computation costs of quantum-attack resilient encryption algorithms for embedded devices. *IEEE Access* **2024**, *12*, 8791–8805.
124. McEliece, R.J. A public-key cryptosystem based on algebraic. *Coding Thv* **1978**, *4244*, 114–116.
125. Berlekamp, E. Goppa codes. *IEEE Transactions on Information Theory* **2003**, *19*, 590–592.
126. Kumar, M. Post-quantum cryptography Algorithm's standardization and performance analysis. *Array* **2022**, *15*, 100242.
127. Sandanamudi, P.K.; Agrawal, N.; Tripathi, N.; BN, P.K. Securing UAV Communications: A Comparative Performance Analysis of Post-Quantum Cryptographic Techniques. In Proceedings of the 2025 17th International Conference on COMmunication Systems and NETworks (COMSNETS). IEEE, 2025, pp. 1096–1101.
128. Pradhan, P.K.; Rakshit, S.; Datta, S. Lattice based cryptography: Its applications, areas of interest & future scope. In Proceedings of the 2019 3rd international conference on computing methodologies and communication (ICCMC). IEEE, 2019, pp. 988–993.
129. Hoffstein, J.; Pipher, J.; Silverman, J.H. NTRU: A ring-based public key cryptosystem. In Proceedings of the International algorithmic number theory symposium. Springer, 1998, pp. 267–288.
130. Alkim, E.; Ducas, L.; Pöppelmann, T.; Schwabe, P. Post-quantum key {Exchange—A} new hope. In Proceedings of the 25th USENIX Security Symposium (USENIX Security 16), 2016, pp. 327–343.
131. Lamport, L. Constructing digital signatures from a one way function **1979**.

132. Merkle, R.C. A digital signature based on a conventional encryption function. In Proceedings of the Conference on the theory and application of cryptographic techniques. Springer, 1987, pp. 369–378.
133. Aissaoui, R. Assessment and optimization of post-quantum cryptographic protocols for civil UAV communications. PhD thesis, Ecole Nationale Aviation Civile, 2024.
134. Courtois, N.T. The security of hidden field equations (HFE). In Proceedings of the Topics in cryptology—CT-RSA 2001: the cryptographers' track at RSA conference 2001 San Francisco, CA, USA, April 8–12, 2001 proceedings. Springer, 2001, pp. 266–281.
135. Rostovtsev, A.; Stolbunov, A. Public-key cryptosystem based on isogenies. *Cryptology ePrint Archive* **2006**.
136. Childs, A.; Jao, D.; Soukharev, V. Constructing elliptic curve isogenies in quantum subexponential time. *Journal of Mathematical Cryptology* **2014**, *8*, 1–29.
137. Costello, C.; Longa, P.; Naehrig, M. Efficient algorithms for supersingular isogeny Diffie-Hellman. In Proceedings of the Advances in Cryptology–CRYPTO 2016: 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part I 36. Springer, 2016, pp. 572–601.
138. Ouadah, M.; Merazka, F. Securing UAV communication: Authentication and integrity. In Proceedings of the 2024 11th International Conference on Wireless Networks and Mobile Communications (WINCOM). IEEE, 2024, pp. 1–7.
139. Abdulhae, O.T.; Mandeep, J.S.; Islam, M. Cluster-based routing protocols for flying ad hoc networks (FANETs). *IEEE access* **2022**, *10*, 32981–33004.
140. Liu, J.; Yuan, L. Key management technology analysis based on UAV cluster communication security. In Proceedings of the International Conference on Network Communication and Information Security (ICNCIS 2021). SPIE, 2022, Vol. 12175, pp. 127–132.
141. Mehmood, A.; Iqbal, Z.; Shah, A.A.; Maple, C.; Lloret, J. An intelligent cluster-based communication system for multi-unmanned aerial vehicles for searching and rescuing. *Electronics* **2023**, *12*, 607.
142. Zhang, X.; Wang, Y.L.; Byun, H. Divisive hierarchical clustering for energy saving and latency reduction in UAV-assisted WSANs. *EURASIP Journal on Wireless Communications and Networking* **2025**, *2025*, 2.
143. Tummala, V.M.R.; Hazra, A.; Kalita, A.; Gurusamy, M. Cluster Based Pseudo Hierarchical Decentralized Federated Learning in UAV Networks. In Proceedings of the 2024 IEEE 100th Vehicular Technology Conference (VTC2024-Fall). IEEE, 2024, pp. 1–5.
144. Tran, T.N.; Nguyen, T.L.; Hoang, V.T.; Voznak, M. Sensor clustering using a K-means algorithm in combination with optimized unmanned aerial vehicle trajectory in wireless sensor networks. *Sensors* **2023**, *23*, 2345.
145. Yuan, L.; Feng, Z.; Zhang, C.; Ji, H. Cross-platform UAV swarm key management in denied environments. *Applied Sciences* **2023**, *13*, 8918.
146. Lv, Z.; Qiao, L.; Hossain, M.S.; Choi, B.J. Analysis of using blockchain to protect the privacy of drone big data. *IEEE network* **2021**, *35*, 44–49.
147. Hafeez, S. Blockchain-based secure Unmanned Aerial Vehicles (UAV) in network design and optimization. PhD thesis, University of Glasgow, 2024.
148. Harbi, Y.; Medani, K.; Gherbi, C.; Senouci, O.; Aliouat, Z.; Harous, S. A systematic literature review of blockchain technology for Internet of Drones security. *Arabian Journal for Science and Engineering* **2023**, *48*, 1053–1074.
149. Decent Cybersecurity. Decentralized Drone Identity Management: Securing the Skies with Blockchain Technology. https://decentcybersecurity.eu/decentralized-drone-identity-management-securing-the-skies-with-blockchain-technology/, 2024. Accessed: 2025-06-10.
150. Lee, S.W.; Safkhani, M.; Le, Q.; Ahmed, O.H.; Hosseinzadeh, M.; Rahmani, A.M.; Bagheri, N. Designing secure PUF-based authentication protocols for constrained environments. *Scientific Reports* **2023**, *13*, 21702.
151. Zhang, L.; Xu, J.; Obaidat, M.S.; Li, X.; Vijayakumar, P. A PUF-based lightweight authentication and key agreement protocol for smart UAV networks. *IET Communications* **2022**, *16*, 1142–1159.
152. Karmakar, R.; Kaddoum, G.; Akhrif, O. A PUF and fuzzy extractor-based UAV-ground station and UAV-UAV authentication mechanism with intelligent adaptation of secure sessions. *IEEE Transactions on Mobile Computing* **2023**, *23*, 3858–3875.
153. Irshad, A.; Alzahrani, B.A.; Albeshri, A.; Alsubhi, K.; Nayyar, A.; Chaudhry, S.A. SPAKE-DC: A secure PUF enabled authenticated key exchange for 5G-based drone communications. *IEEE Transactions on Vehicular Technology* **2023**, *73*, 5770–5780.
154. Wang, D.; Cao, Y.; Lam, K.Y.; Hu, Y.; Kaiwartya, O. Authentication and key agreement based on three factors and PUF for UAVs-assisted post-disaster emergency communication. *IEEE Internet of Things Journal* **2024**.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 17 July 2025 doi:10.20944/preprints202507.1503.v1

155. Kuznetsov, O.; Kandiy, S.; Frontoni, E.; Smirnov, O. Trade-offs in Post-Quantum Cryptography: A Comparative Assessment of BIKE, HQC, and Classic McEliece. In Proceedings of the CQPC, 2023, pp. 1–11.
156. Turnip, T.N.; Andersen, B.; Vargas-Rosales, C. Towards 6G Authentication and Key Agreement Protocol: A Survey on Hybrid Post Quantum Cryptography. *IEEE Communications Surveys & Tutorials* **2025**.
157. Nair, A.S.; Thampi, S.M.; Jafeel, V. A post-quantum secure PUF based cross-domain authentication mechanism for Internet of drones. *Vehicular Communications* **2024**, *47*, 100780.
158. Conrad, A.; Cochran, R.; Sanchez-Rosales, D.; Isaac, S.; Javid, T.; Rezaei, T.; Schroeder, A.; Golba, G.; Gutha, A.; Wilens, B.; et al. Drone-and Vehicle-Based Quantum Key Distribution. *arXiv preprint arXiv:2505.17587* **2025**.
159. National Institute of Standards and Technology (NIST). Post-Quantum Cryptography Standardization. https://csrc.nist.gov/projects/post-quantum-cryptography, 2025. Accessed June 10, 2025.
160. Khan, W.U.; Lagunas, E.; Ali, Z.; Javed, M.A.; Ahmed, M.; Chatzinotas, S.; Ottersten, B.; Popovski, P. Opportunities for physical layer security in UAV communication enhanced with intelligent reflective surfaces. *IEEE Wireless Communications* **2022**, *29*, 22–28.
161. Abduljabbar, Z.A.; Nyangaresi, V.O.; Ma, J.; Al Sibahee, M.A.; Khalefa, M.S.; Honi, D.G. MAC-based symmetric key protocol for secure traffic forwarding in drones. In Proceedings of the International Conference on Future Access Enablers of Ubiquitous and Intelligent Infrastructures. Springer, 2022, pp. 16–36.
162. Swinney, C.J.; Woods, J.C. A review of security incidents and defence techniques relating to the malicious use of small unmanned aerial systems. *IEEE Aerospace and Electronic Systems Magazine* **2022**, *37*, 14–28.
163. Rugo, A.; Ardagna, C.A.; Ioini, N.E. A Security Review in the UAVNet Era: Threats, Countermeasures, and Gap Analysis. *ACM Computing Surveys (CSUR)* **2022**, *55*, 1–35. https://doi.org/10.1145/3487057.
164. Abdulrazak, C. Cybersecurity Threat Analysis and Attack Simulations for Unmanned Aerial Vehicle Networks. *arXiv preprint arXiv:2404.16842* **2024**.
165. Dharmalingam, B.; Mukherjee, R.; Piggott, B.; Feng, G.; Liu, A. Aero-LLM: A Distributed Framework for Secure UAV Communication and Intelligent Decision-Making. *arXiv preprint arXiv:2502.05220* **2025**.
166. Gandhi, M.; Mulay, C.; Durai, K.; Murali, G.; Masood, J.A.I.S.; Vijayarajan, V.; Gautam, K.; Chakravarthy, N.K.; Kumar, S.S.; Agarwal, S.; et al. Quantum blockchain: Trends, technologies, and future directions. *IET Quantum Communication* **2024**, *5*, 516–542.
167. Chen, J.; Feng, Z.; Wen, J.Y.; Liu, B.; Sha, L. A container-based DoS attack-resilient control framework for real-time UAV systems. In Proceedings of the 2019 Design, Automation & Test in Europe Conference & Exhibition (DATE). IEEE, 2019, pp. 1222–1227.
168. Alhawi, O.M.; Mustafa, M.A.; Cordiro, L.C. Finding security vulnerabilities in unmanned aerial vehicles using software verification. In Proceedings of the 2019 International Workshop on Secure Internet of Things (SIOT). IEEE, 2019, pp. 1–9.
169. Aldossary, M.; Alzamil, I.; Almutairi, J. Enhanced Intrusion Detection in Drone Networks: A Cross-Layer Convolutional Attention Approach for Drone-to-Drone and Drone-to-Base Station Communications. *Drones* **2025**, *9*, 46.
170. Li, S.; Cao, J.; Shi, X.; Li, H. Enabling Space-Air integration: A Satellite-UAV networking authentication scheme. *Security and Safety* **2024**, *3*, 2023030.
171. Malik, N.; Sinha, H.; Dahiya, M. Security in UAV ecosystem: An implementation perspective. *Sigma Journal of Engineering and Natural Sciences* **2024**, *42*, 1986–1994.
172. Khalid, R.; Shah, Z.; Naeem, M.; Ali, A.; Al-Fuqaha, A.; Ejaz, W. Computational efficiency maximization for UAV-assisted MEC networks with energy harvesting in disaster scenarios. *IEEE Internet of Things Journal* **2023**, *11*, 9004–9018.
173. Tan, X.; Zuo, Z.; Su, S.; Guo, X.; Sun, X. Research of security routing protocol for UAV communication network based on AODV. *Electronics* **2020**, *9*, 1185.
174. Betti Sorbelli, F. UAV-based delivery systems: A systematic review, current trends, and research challenges. *Journal on Autonomous Transportation Systems* **2024**, *1*, 1–40.
175. Asadzadeh, S.; de Oliveira, W.J.; de Souza Filho, C.R. UAV-based remote sensing for the petroleum industry and environmental monitoring: State-of-the-art and perspectives. *Journal of Petroleum Science and Engineering* **2022**, *208*, 109633.
176. Nawaz, H.; Ali, H.M.; Laghari, A.A. UAV communication networks issues: A review. *Archives of Computational Methods in Engineering* **2021**, *28*, 1349–1369.
177. Scherer, J.; Rinner, B. Multi-UAV surveillance with minimum information idleness and latency constraints. *IEEE Robotics and Automation Letters* **2020**, *5*, 4812–4819.

178. Mehmood, A.; Iqbal, Z.; Shah, A.A.; Maple, C.; Lloret, J. An intelligent cluster-based communication system for multi-unmanned aerial vehicles for searching and rescuing. *Electronics* **2023**, *12*, 607.
179. Outay, F.; Mengash, H.A.; Adnan, M. Applications of unmanned aerial vehicle (UAV) in road safety, traffic and highway infrastructure management: Recent advances and challenges. *Transportation research part A: policy and practice* **2020**, *141*, 116–129.
180. Saleab, M.; Sax, F.; Schumann, J.; Holzapfel, F. Low-level memory and timing analysis of flight code for unmanned aerial systems. *Aerospace Systems* **2024**, *7*, 209–225.
181. Banerjee, B.; Neogy, S. Study and Analysis of the Recent Trends for Security Mechanisms in Mobile Adhoc Network. In Proceedings of the International Conference on Security, Surveillance and Artificial Intelligence (ICSSAI-2023). CRC Press, 2024, pp. 23–32.
182. Park, M.; Lee, S.; Lee, S. Dynamic topology reconstruction protocol for uav swarm networking. *Symmetry* **2020**, *12*, 1111.
183. Shah, S.F.A.; Mazhar, T.; Al Shloul, T.; Shahzad, T.; Hu, Y.C.; Mallek, F.; Hamam, H. Applications, challenges, and solutions of unmanned aerial vehicles in smart city using blockchain. *PeerJ Computer Science* **2024**, *10*, e1776.
184. Chittoor, P.K.; Chokkalingam, B.; Mihet-Popa, L. A review on UAV wireless charging: Fundamentals, applications, charging techniques and standards. *IEEE access* **2021**, *9*, 69235–69266.
185. Mohsan, S.A.H.; Othman, N.Q.H.; Li, Y.; Alsharif, M.H.; Khan, M.A. Unmanned aerial vehicles (UAVs): Practical aspects, applications, open challenges, security issues, and future trends. *Intelligent service robotics* **2023**, *16*, 109–137.
186. Abbood, A.A.; AL-Shammri, F.K.; Alzamili, Z.M.; Al-Shareeda, M.A.; Almaiah, M.A.; AlAli, R. Investigating quantum-resilient security mechanisms for flying ad-hoc networks (fanets). *Journal of Robotics and Control (JRC)* **2025**, *6*, 456–469.
187. Al Farsi, A.S.; Khan, A.; Mughal, M.R.; Bait-Suwailam, M. Privacy and Security Challenges in Federated Learning for UAV Systems: A Comprehensive Review. *SECURITY AND PRIVACY* **2024**.
188. Zolfaghari, B.; Abbasmollaei, M.; Hajizadeh, F.; Yanai, N.; Bibak, K. Secure UAV (drone) and the great promise of AI. *ACM Computing Surveys* **2024**, *56*, 1–37.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.