Afro-Asian Journal of Scientific Research (AAJSR)
المجلة الأفروآسيوية للبحث العلمي
E-ISSN: 2959-6505
Volume 3, Issue 4, 2025
Page No: 207-216
Website: https://aajsr.com/index.php/aajsr/index

SJIFactor 2024: 5.028 ISI 2025: 0.915 معامل التأثير العربي (AIF) 2025: 0.76

Secure Communication Protocols for UAV-Assisted Wireless Networks: Designing Encryption, Authentication, and Anti-Jamming Systems

Mohamed Ahmed Elhabeb[1*], Bilgasem Omer Mohammed Esmaeel[2], Elhabeb Abdu Allah Elhabeb[3], Tahher Ahmed Elhabeb[4]
[1]Department of Computer Technologies, Faculty of Science and Technology, Al-Zawiya Al-Shati, Libya
[2]Department of Electrical and Electronic Engineering, Higher Institute Faculty of Science and Technology, Tamzawa Al-shati, Libya
[3]Department of Information Technologies, Faculty of Technical Sciences, Al-shati, Libya
[4]The Libyan Academy for Post Graduate Studies, Tripoli, Libya

بروتوكولات الاتصال الآمن للشبكات اللاسلكية المدعومة بالطائرات بدون طيار: تصميم أنظمة التشفير والمصادقة ومكافحة التشويش

محمد احمد الحبيب[1*]، بلقاسم عمر محمد اسماعيل[2]، الحبيب عبدالله الحبيب[3]، طاهر احمد الحبيب[4]
[1]قسم تقنيات الحاسوب، كلية العلوم والتقنية، الزوية الشاطئ، ليبيا
[2]قسم الكهربائية والالكترونية، المعهد العالي للعلوم والتقنية، تامزاوة الشاطئ، ليبيا
[3]قسم تقنية المعلومات، كلية العلوم والتقنية، الشاطئ، ليبيا
[4]الاكاديمية الليبيا للدراسات العليا، طرابلس، ليبيا

*Corresponding author: Mohamedelhabeb670@gmail.com

Received: October 06, 2025	Accepted: December 21, 2025	Published: December 29, 2025

Abstract:

Unmanned Aerial Vehicles (UAVs) have emerged as critical components in modern wireless communication systems due to their flexibility, rapid deployment, and broad coverage. However, their integration introduces serious security concerns. This paper presents a comprehensive study on the design and implementation of secure communication protocols for UAV-assisted wireless networks. Focusing on three major aspects, encryption, authentication, and anti-jamming, we explore the challenges, technologies, and design strategies essential for protecting UAV-based communications against evolving threats. The paper concludes by identifying key research gaps and proposing future directions for resilient and secure UAV communication systems.

Keywords: UAV, drone communication, encryption, authentication, anti-jamming.

الملخص:

لقد برزت المركبات الجوية غير المأهولة (UAVs) كمكونات أساسية في أنظمة الاتصالات اللاسلكية الحديثة نظرًا لمرونتها، وسرعة نشرها، وقدرتها على تغطية نطاق واسع. ومع ذلك، فإن دمجها يطرح مخاوف أمنية خطيرة. يقدم هذا البحث دراسة شاملة حول تصميم وتنفيذ بروتوكولات الاتصال الآمن في الشبكات اللاسلكية المدعومة بالطائرات بدون طيار. ومن خلال التركيز على ثلاثة جوانب رئيسية، التشفير، والمصادقة، ومكافحة التشويش، نستعرض التحديات والتقنيات واستراتيجيات التصميم الضرورية لحماية الاتصالات المعتمدة على الطائرات بدون طيار من التهديدات المتطورة. ويختتم البحث بتحديد الفجوات البحثية الرئيسية واقتراح اتجاهات مستقبلية لبناء أنظمة اتصالات آمنة ومرنة للطائرات بدون طيار.

الكلمات المفتاحية: الطائرات بدون طيار، اتصالات الطائرات بدون طيار، التشفير، المصادقة، مكافحة التشويش.

Introduction:

UAVs, commonly known as drones, are increasingly utilized in wireless networks for applications ranging from disaster recovery to surveillance and cargo delivery [1]. Their ability to form ad hoc airborne networks makes them invaluable in scenarios lacking infrastructure. However, their reliance on open-air communication channels renders them highly susceptible to eavesdropping, spoofing, and jamming attacks [2]. To ensure the reliability and safety of data transmission, robust security mechanisms must be integrated into UAV communication protocols [3].

Unmanned Aerial Vehicles (UAVs), or drones, have become integral to the future of wireless communications due to their unique capabilities such as rapid deployment, high mobility, and line-of-sight communication [4]. Unlike terrestrial communication systems that require fixed infrastructure, UAVs can dynamically form aerial networks to provide temporary or supplemental wireless coverage in hard-to-reach or infrastructure-less areas. This makes them invaluable for a range of applications including disaster response, military operations, environmental monitoring, precision agriculture, and delivery services [5].

Despite these advantages, UAVs also introduce a new set of vulnerabilities to wireless communication systems [6]. Because UAVs operate in open and often hostile environments, the communication links they rely on are exposed to interception, interference, and spoofing. Furthermore, UAVs often communicate over public frequency bands, making them prime targets for jamming and other signal disruption techniques [7]. The wireless nature of these communications inherently expands the attack surface, exposing both the UAVs and their ground control stations to a wide array of cyber and physical threats [8].

Moreover, the increasing autonomy and intelligence of UAV systems mean that a successful breach could have catastrophic consequences, from mission failure to public safety risks [9]. Given the potential sensitivity of the data transmitted, such as live video feeds, location coordinates, and mission-critical instructions, ensuring secure communication becomes not just a technical requirement but a foundational necessity [10].

Consider a UAV-aided relaying system as depicted in Figure. 1, in which a terrestrial BS S communicates with an on-ground mobile user D, in the presence of an eavesdropper E on the ground [11]. We assume that the direct link between S and D is not available, e.g., due to blockages and/or long distance. For that, the communications and security of the transmission from S to D are assisted by a swarm of U UAVs that functions as a relay and friendly jammers [12]. Let Ru denote the u-th UAV where u ∈Φu = {1, 2, ..., U}. Due to their limited energy, we assume that UAVs are only equipped with a single antenna, operate in the half-duplex AF mode, and can wirelessly harvest power from S [13].

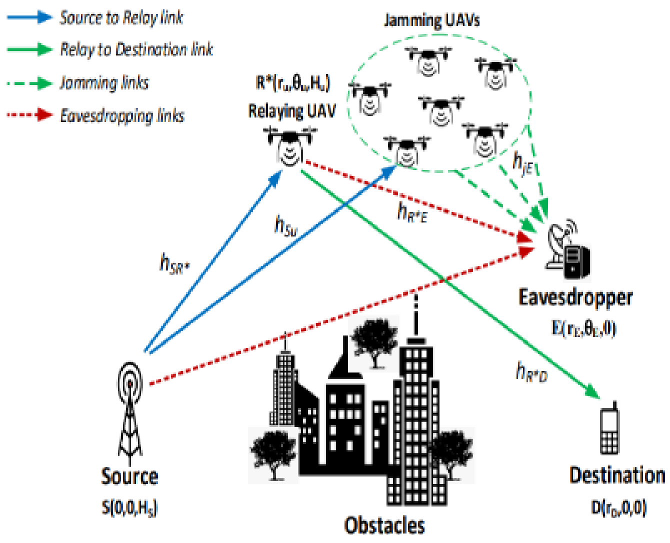

Figure (1): System model of UAV-assisted relaying network.

To counteract these threats, the design of secure communication protocols for UAV-assisted wireless networks must incorporate multiple layers of protection. These include robust encryption techniques to maintain data confidentiality and integrity, strong authentication mechanisms to verify the identity of users and devices, and resilient anti-jamming strategies to ensure continuous and reliable communication under adversarial conditions. This paper provides a focused exploration of these three pillars, offering insights into current technologies, best practices, and emerging research directions [14].

Security Challenges in UAV-Assisted Networks:

UAV-based communication systems face several unique threats:

- **Eavesdropping:** Attackers can intercept unencrypted signals.
- **Spoofing:** Adversaries may impersonate legitimate UAVs or ground stations.
- **Jamming:** Intentional interference disrupts signal transmission.
- **Man-in-the-middle attacks:** Unauthorized interception and alteration of messages.

Such threats can compromise mission objectives, leak sensitive data, or endanger human lives [15]. Addressing these issues requires a multilayered approach to security.

Table (1): Description of Security Challenges

Security Challenge	Description
Eavesdropping	UAVs frequently use open wireless channels that can be intercepted by unauthorized parties, risking sensitive data exposure.
Spoofing Attacks	Attackers impersonate legitimate UAVs or controllers, potentially taking control or injecting malicious commands.
Jamming Attacks	Intentional RF interference can disrupt communication, causing mission failure or emergency responses.
MITM Attacks	Adversaries secretly intercept and alter communications between UAVs and their controllers.
Replay Attacks	Previously captured valid data is resent to trick UAV systems into executing outdated commands.
Physical Tampering	Captured UAVs may be reverse-engineered or altered to extract data or compromise future missions.
Denial-of-Service	Attacks that overload communication or computing resources, rendering UAVs inoperable.
Resource Constraints	Limited energy and processing power restrict the use of heavy-duty security mechanisms.

UAV-based communication systems face several unique and multifaceted threats that differ from those encountered in conventional terrestrial networks. These threats stem from the operational characteristics of UAVs, including their mobility, altitude, line-of-sight dependence, and exposure to hostile environments [16].

Below are the primary security challenges:

- **Eavesdropping:** UAVs frequently communicate over wireless channels that are inherently vulnerable to interception. Malicious actors equipped with appropriate radio hardware can intercept unencrypted data, leading to the exposure of sensitive information such as surveillance footage, positional data, and control commands.
- **Spoofing Attacks:** In a spoofing attack, an adversary attempts to impersonate a legitimate UAV or ground control station. This deception can allow attackers to take over control, redirect flight paths, or inject false data into the system. GPS spoofing, in particular, poses a significant risk by providing UAVs with incorrect location data, potentially leading to crashes or hijacked missions.
- **Jamming Attacks:** UAV communication systems often rely on specific radio frequency bands, which can be deliberately disrupted using jamming devices. These attacks can cause the UAV to lose contact with its control station, triggering fail-safe behaviors like emergency landing or return-to-home, which may be exploited to disrupt operations.
- **Man-in-the-Middle (MITM) Attacks:** In these attacks, an adversary intercepts communication between the UAV and its control unit, often without detection. The attacker can alter messages, delay commands, or inject malicious data, compromising the integrity of the mission.
- **Replay Attacks:** By capturing and replaying previously transmitted valid data packets, attackers can trick UAV systems into executing outdated or unauthorized actions. This is particularly dangerous in UAV swarms where synchronized operations are required.
- **Physical Capture and Tampering:** UAVs deployed in unsecured or remote environments are at risk of being physically captured. Once in possession, attackers can reverse-engineer the hardware, extract cryptographic keys, or install malicious firmware.
- **Denial-of-Service (DoS):** Targeting the UAV's communication or processing resources, DoS attacks can render a UAV inoperative by overwhelming it with unnecessary traffic or computation.

- **Resource Constraints:** Unlike ground-based systems, UAVs are limited by power, weight, and processing capacity. These limitations make it challenging to implement traditional security mechanisms without significantly impacting flight performance or mission duration.

Addressing these challenges requires a holistic and adaptive approach to security that goes beyond conventional IT security models [17]. Protocols must be lightweight yet robust, capable of withstanding adversarial conditions while ensuring low latency, high reliability, and minimal power consumption. This lays the groundwork for the design considerations and defense mechanisms discussed in the following sections.

Encryption Mechanisms:

Encryption ensures confidentiality and integrity in UAV communications. Two major types of encryption are used:

- **Symmetric Encryption:** AES (Advanced Encryption Standard) is widely adopted due to its efficiency. UAVs with pre-shared keys can securely exchange data with minimal latency.
- **Asymmetric Encryption:** Public-key schemes like RSA and ECC (Elliptic Curve Cryptography) provide better key management, especially in large-scale deployments.

Recent advancements include lightweight encryption algorithms tailored for UAVs with constrained resources. Implementing hybrid cryptographic systems can balance security and computational load.

Table (2): Use of Encryption Method Characteristics

Encryption Method	Characteristics	Use in UAV Systems
Symmetric Encryption	Fast, energy-efficient, but requires key sharing. Algorithms like AES are widely used.	Data transmission with pre-shared keys
Asymmetric Encryption	Public/private key pairs; better key management but more computationally intense. ECC is common.	Secure key exchange
Lightweight Encryption	Custom-designed for low power devices; e.g., SPECK, SIMON.	Real-time UAV communications
Hybrid Encryption	Combines symmetric and asymmetric for best of both.	Session key establishment and data transmission
Post-Quantum Cryptography	Resistant to quantum attacks; e.g., lattice-based schemes.	Future-proofing UAV security

Encryption plays a critical role in safeguarding the confidentiality and integrity of information exchanged within UAV networks. Due to their resource-constrained nature, UAVs require encryption methods that are not only secure but also computationally efficient. Here, we explore key encryption approaches and recent innovations:

- **Symmetric Encryption:** Symmetric-key algorithms like AES (Advanced Encryption Standard) are widely used for their speed and efficiency. In UAV systems, symmetric encryption is typically implemented using pre-shared keys between UAVs and ground control stations. However, key management becomes a challenge in large or dynamic networks.
- **Asymmetric Encryption:** Public-key cryptographic schemes such as RSA and Elliptic Curve Cryptography (ECC) offer improved scalability and secure key exchange mechanisms. ECC, in particular, is favored for UAV applications due to its high security per bit and reduced computational overhead compared to RSA.
- **Lightweight Cryptography:** Given the strict energy and processing constraints of UAVs, researchers are developing lightweight encryption algorithms such as PRESENT, SPECK, and SIMON. These algorithms are optimized for constrained devices while maintaining reasonable security margins.
- **Hybrid Cryptographic Systems:** Many UAV systems now employ hybrid models that combine symmetric and asymmetric encryption. For example, asymmetric cryptography may be used to establish a session key, after which symmetric encryption is used for ongoing data transfer. This approach balances the efficiency of symmetric encryption with the flexible key management of asymmetric methods.
- **Secure Key Distribution:** Ensuring secure and scalable key distribution is essential in UAV networks. Approaches like Diffie-Hellman key exchange, identity-based encryption, and certificate-less cryptography are being explored to simplify key management without compromising security.
- **Post-Quantum Cryptography:** As quantum computing becomes a realistic threat, there is increasing interest in quantum-resistant encryption algorithms such as lattice-based, hash-based,

and multivariate polynomial cryptographic schemes. These offer future-proof solutions for securing UAV communications.

Effective encryption is foundational for defending UAV systems against eavesdropping, data tampering, and unauthorized access. However, its implementation must be carefully tailored to the constraints and requirements of UAV platforms. The next section delves into complementary authentication mechanisms that further enhance security [18,19].

Authentication Protocols:

ensures that communication between UAVs, ground stations, and other devices is established only with trusted entities. Given the susceptibility of UAVs to impersonation and spoofing, designing lightweight yet secure authentication protocols are paramount.

Table (3): Authentication Protocols

Authentication Type	Description	Pros	Cons
Password-Based	Uses shared secrets between nodes.	Simple implementation	Vulnerable to brute-force and replay attacks
Token-Based	Authentication via temporary tokens (e.g., OAuth-like systems).	Scalable	Token theft risks
Biometric-Based	Utilizes human operator's traits like fingerprints or voice.	High assurance	Needs biometric sensors, not always feasible
Certificate-Based	Uses digital certificates from a Certificate Authority (CA).	Strong identity proof	Requires PKI infrastructure
Challenge-Response	One party issues a challenge, the other responds with a cryptographically derived answer.	Strong against replay attacks	More processing required

Authentication verifies the legitimacy of communicating parties. For UAVs, this prevents unauthorized access and control [20].

- **Mutual Authentication:** Ensures both UAVs and ground stations verify each other's identity.
- **Digital Certificates and PKI:** Certificates issued by a trusted authority can validate identities.
- **Blockchain-Based Authentication:** Decentralized ledgers provide tamper-proof authentication records.

Additionally, biometric and behavioral authentication mechanisms are being explored for operator identity verification [21].

Anti-Jamming Techniques:

In UAV-assisted wireless networks, jamming attacks pose a significant threat to the reliability and availability of communication links. UAVs rely heavily on wireless signals for command and control (C2), navigation, telemetry, and data transmission. Any disruption caused by intentional or unintentional jamming can lead to mission failure, data loss, or even UAV crashes. Therefore, robust anti-jamming techniques are essential components in the design of secure UAV communication protocols.

Types of Jamming Attacks:

Jamming can be categorized based on how it interferes with communication signals. One of the most prevalent types is constant jamming, where a jammer persistently emits radio signals to overwhelm legitimate transmissions. This brute-force method is easy to detect but effective if not countered. Another form is deceptive jamming, which involves transmitting fake signals that confuse the UAV's receiver, making it difficult to distinguish between legitimate and malicious inputs.

Reactive jamming activates only when a valid signal is detected, conserving energy and reducing the chances of being identified. Finally, random jamming operates intermittently, introducing unpredictability that complicates detection and mitigation strategies. These types of jamming attacks exploit different vulnerabilities in the wireless communication medium, necessitating diverse and adaptive countermeasures for effective defense.

Spread Spectrum Techniques:

Spread spectrum methods increase the robustness of UAV communication against interference by spreading the signal across a wider bandwidth.

Frequency Hopping Spread Spectrum (FHSS):

- The transmitter and receiver hop between multiple frequencies in a synchronized manner.

- Reduces the chance of successful jamming because the jammer cannot predict the next frequency.

Direct Sequence Spread Spectrum (DSSS):

- The data signal is multiplied by a high-frequency pseudo-random noise (PN) code.
- Makes the signal appear like noise to unintended receivers, increasing resistance to jamming [22].

Figure2. illustrates two scenarios involving the UAV, the receiver, and jammer. In the first scenario, the receiver is a stationary RSU, while, in the second scenario, the receiver is a moving vehicle. Our paper focuses on the analysis and discussion of these two distinct scenarios. The positions of the receivers and the jammer are measured using Cartesian coordinates, which can be denoted by $C'R$=[$c'xR$,$c'yR$] and $C'J$=[$c'xJ$,$c'yJ$], respectively. In terms of the moving UAV, let CU=[cxU,cyU,czU] denote its position. While the jammer persistently emits jamming signals towards the UAV, the UAV simultaneously transmits messages to the receiver. At the beginning of each time slot, the UAV selects the communication center frequency fcU, and initiates the transmission of a signal to the receiver. Subsequently, the jammer, upon sensing the UAV's selected frequency fcU, chooses the center frequency fcJ for its jamming signal [23].

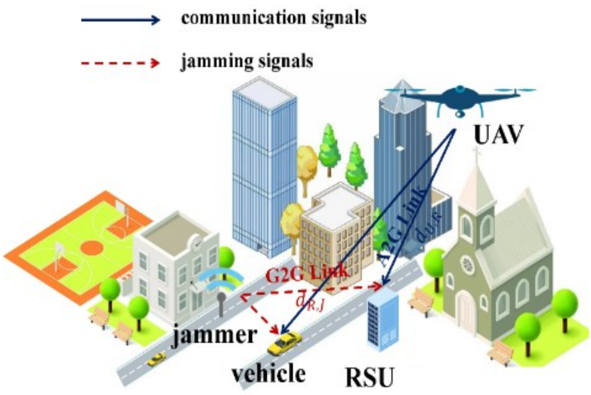

Figure (2): An A2G network in the presence of a jammer.

Adaptive Transmission Power Control

Dynamic adjustment of the transmission power can mitigate jamming without significantly draining battery life:

- **Low-power Transmission:** Reduces the likelihood of detection by adversarial jammers.
- **High-power Burst Mode:** Used temporarily when jamming is detected to overcome signal interference.

Power control algorithms are implemented to balance energy efficiency and robustness against jamming threats.

Directional Antennas and Beamforming:

- **Directional antennas** focus signal energy in a specific direction, limiting the jammer's ability to intercept or disrupt the signal.
- **Beamforming techniques** can steer communication beams toward legitimate receivers while nullifying interference from jammers.

This is particularly useful in swarm UAV deployments or when line-of-sight communication with ground control is critical [24].

Cognitive Radio and Spectrum Sensing:

Cognitive radio enables UAVs to dynamically sense and adapt to their spectrum environment:

- **Spectrum sensing** detects unused frequencies and identifies jamming activity.
- UAVs can **switch channels** in real-time to avoid congested or jammed bands.
- Machine learning models can predict jamming patterns and pre-emptively adjust the communication strategy.

Multi-Path and Multi-Hop Communication:

- **Multi-path routing** involves sending duplicate data packets across different paths to increase the likelihood of successful delivery.
- **Multi-hop networks** allow UAVs to relay data through intermediate nodes, bypassing jammed areas.

These methods increase redundancy and reliability in environments prone to interference.

Jamming Detection Algorithms:

Effective jamming countermeasures begin with timely detection. Techniques include:

- **Signal-to-Noise Ratio (SNR) Monitoring:** A sudden drop in SNR indicates possible jamming.
- **Packet Delivery Ratio (PDR) Analysis:** Low PDRs can be indicative of persistent jamming.
- **Entropy-Based Methods:** Analyzing signal randomness to distinguish between natural and malicious interference.

UAV Mobility and Evasion Tactics

UAVs can physically reposition themselves to escape jamming zones:

- **Geo-fencing:** Maps known jamming areas and reroutes UAVs accordingly.
- **Flight Path Optimization:** Integrates jamming awareness into route planning to maintain secure links.

Protocol Design Considerations:

Designing secure communication protocols for UAV-assisted wireless networks requires careful attention to several key considerations, including resource limitations, dynamic topology, latency sensitivity, and threat diversity. As UAVs are often deployed in rapidly changing environments with varying mission profiles, the communication protocols must be robust, lightweight, adaptable, and interoperable across multiple platforms [25].

Lightweight and Energy-Efficient Protocols:

UAVs are typically constrained by size, weight, and power (SWaP) limitations, which restrict computational resources and energy availability. Security mechanisms such as encryption, authentication, and anti-jamming measures must therefore be optimized to minimize computational overhead:

- **Use of Symmetric Cryptography:** Lightweight symmetric encryption algorithms (e.g., AES-128, PRESENT) are preferred over computationally intensive public-key algorithms.
- **Energy-Aware Protocols:** Protocols must minimize retransmissions and idle listening to conserve battery life.
- **Hardware Acceleration:** Utilization of specialized hardware for cryptographic operations can enhance speed and reduce energy usage.

Scalability and Dynamic Network Topologies:

UAV networks often experience high mobility and frequent changes in topology. The protocol must adapt to varying node densities and topological changes without compromising performance or security:

- **Cluster-Based Communication:** Nodes may be grouped into clusters with designated cluster heads to manage communication and reduce overhead.
- **Self-Healing Mechanisms:** The protocol should support route repair and dynamic reconfiguration in case of node failures or disconnections.
- **Topology-Aware Security Policies:** Security policies should be updated in real-time as the network structure evolves.

Real-Time Communication and Low Latency:

Applications such as surveillance, reconnaissance, and real-time video streaming demand low-latency communication. Security mechanisms must not introduce significant delays:

- **Fast Authentication Mechanisms:** Use of lightweight challenge-response protocols or one-time passwords (OTP) to reduce handshake time.
- **Prioritized Traffic Scheduling:** Time-critical data should be prioritized in routing and transmission.
- **Delay-Tolerant Security:** Where immediate authentication is not feasible, deferred authentication methods may be temporarily employed.

Interoperability and Standardization:

UAV-assisted networks often need to interact with terrestrial and satellite networks, requiring standardized communication and security protocols:

- **Compliance with Existing Standards:** Integration with protocols such as IEEE 802.11s, 5G NR, and IPsec enhances compatibility.
- **Modular Security Architecture:** The protocol design should be modular to allow updates or integration with future technologies.
- **Cross-Layer Coordination:** Security features should be implemented across the network stack, from the physical to the application layer.

Resilience Against Diverse Threats:

Given the diverse threat landscape—including jamming, spoofing, and man-in-the-middle attacks—the protocol must incorporate multi-layered defenses:

- **Redundancy and Failover:** Redundant paths and automatic failover mechanisms can ensure communication continuity.
- **Intrusion Detection Systems (IDS):** Onboard IDS can monitor for anomalies and trigger security responses.

- **Security Policy Adaptability:** Policies should dynamically adjust based on threat detection and mission-criticality.

Quality of Service (QoS) Assurance:

Security mechanisms must coexist with QoS requirements, ensuring that adding encryption or authentication does not compromise throughput or reliability:

- **QoS-Aware Encryption:** Protocols should support selective encryption based on data priority.
- **Adaptive Bandwidth Allocation:** Resources should be dynamically allocated based on mission phase and network condition [26,27].

Future Directions:

As UAV-assisted wireless networks continue to evolve, so must the secure communication protocols that support them. Looking ahead, several promising avenues for future research and development emerge:

AI-Driven Security Adaptation:

Integrating artificial intelligence and machine learning into UAV protocols offers dynamic threat detection, adaptive encryption, and predictive analytics for network behavior. AI models can be trained to detect abnormal communication patterns, proactively reconfigure networks, and optimize routing based on both performance and security metrics.

Quantum-Resistant Cryptography:

With the rise of quantum computing, traditional cryptographic schemes may become vulnerable. The development and integration of quantum-resistant algorithms like lattice-based, hash-based, or multivariate polynomial cryptography are critical for long-term security in UAV communications.

Blockchain for Trust Management:

Blockchain can decentralize trust in UAV networks, providing immutable logs of communication, mission data, and security events. This helps establish transparency, accountability, and secure multi-UAV coordination without relying on a central authority.

6G and Beyond Integration:

Future generations of wireless technology will bring ultra-low latency, higher bandwidth, and enhanced connectivity. Secure protocol designs must align with upcoming 6G capabilities, such as integrated satellite-terrestrial links, AI-native infrastructure, and dynamic spectrum access, to ensure seamless and secure UAV operations.

Biometric and Behavioral Authentication:

Instead of relying solely on traditional keys or certificates, future UAV systems may use biometric indicators or pilot behavior analytics for identity verification and access control. This would enhance resistance to spoofing and insider attacks.

Swarm Security Protocols:

As UAV swarm systems gain popularity, developing secure group communication and coordination protocols will be essential. These must ensure confidentiality, mutual authentication, synchronized operations, and robustness to node failure or compromise.

In summary, future advances in secure communication protocols for UAV-assisted networks will rely heavily on interdisciplinary innovations that blend cryptography, AI, quantum resilience, and distributed systems. By anticipating emerging threats and embracing forward-looking technologies, researchers and engineers can ensure UAVs continue to operate safely and securely in increasingly complex airspace environments [28].

Conclusion:

The development of secure communication protocols for UAV-assisted wireless networks is a multifaceted challenge, shaped by the unique characteristics of UAV platforms, such as their mobility, limited energy resources, and exposure to hostile environments. This paper has outlined key protocol design considerations that are vital to ensuring robust, efficient, and secure communication in such settings. From implementing lightweight encryption mechanisms and designing scalable, latency-aware protocols to enhancing interoperability and resisting sophisticated attacks, each strategy plays a crucial role in the overall system resilience.

Moreover, the exploration of future directions highlights the transformative potential of emerging technologies such as artificial intelligence, blockchain, and quantum-resistant cryptography. These innovations promise not only to strengthen the security architecture of UAV systems but also to enable adaptive, intelligent, and trustworthy network behavior that meets the demands of evolving threats and applications. In conclusion, secure protocol design for UAV-assisted networks demands a holistic, forward-thinking approach. By integrating interdisciplinary solutions and anticipating future challenges, researchers and engineers can pave the way for UAVs to fulfill their growing roles in civil, military, and commercial domains while maintaining the highest standards of security, reliability, and performance.

References:

1. M. Emimi, M. Khaleel, and A. Alkrash, “The Current Opportunities and Challenges in Drone Technology ”, *IJEES*, vol. 1, no. 3, pp. 74–89, Jul. 2023.
2. W. Wang, X. Li, M. Zhang, K. Cumanan, D. W. Kwan Ng, G. Zhang, J. Tang, and O. A. Dobre, “Energy-constrained UAV-assisted secure communications with position optimization and cooperative jamming,” IEEE Transactions on Communications, vol. 68, no. 7, pp. 4476–4489, July 2020.
3. Y. Wu, W. Yang, X. Guan, and Q. Wu, “Energy-efficient trajectory design for UAV-enabled communication under malicious jamming,” IEEE Wireless Communications Letters, vol. 10, no. 2, pp. 206–210, February 2021.
4. R. Ma, W. Yang, Y. Zhang, J. Liu, and H. Shi, “Secure mmWave communication using UAV-enabled relay and cooperative jammer,” IEEE Access, vol. 7, pp. 119 729–119 741, 2019.
5. M. Tatar Mamaghani and Y. Hong, “On the performance of low-altitude UAV-enabled secure AF relaying with cooperative jamming and SWIPT,” IEEE Access, vol. 7, pp. 153 060–153 073, 2019.
6. J. Miao and Z. Zheng, “Cooperative jamming for secure UAV-enabled mobile relay system,” IEEE Access, vol. 8, pp. 48 943–48 957, 2020. 30
7. Y. Sun, D. Xu, D. W. K. Ng, L. Dai, and R. Schober, “Optimal 3D-trajectory design and resource allocation for solarpowered UAV communication systems,” IEEE Transactions on Communications, vol. 67, no. 6, pp. 4281–4298, June 2019.
8. D. N. K. Jayakody, T. D. P. Perera, A. Ghrayeb, and M. O. Hasna, “Self-energized UAV-assisted scheme for cooperative wireless relay networks,” IEEE Transactions on Vehicular Technology, vol. 69, no. 1, pp. 578–592, January 2020.
9. P. K. Chittoor, B. Chokkalingam, and L. Mihet-Popa, “A review on UAV wireless charging: fundamentals, applications, charging techniques and standards,” IEEE Access, vol. 9, pp. 69 235–69 266, 2021.
10. H. Yan, Y. Chen, and S.-H. Yang, “UAV-enabled wireless power transfer with base station charging and UAV power consumption,” IEEE Transactions on Vehicular Technology, vol. 69, no. 11, pp. 12 883–12 896, November 2020.
11. Rong Huang and Yuancheng Li. 2023. Adversarial Attack Mitigation Strategy for Machine Learning-Based Network Attack Detection Model in Power System. IEEE Transactions on Smart Grid 14, 3 (2023), 2367ś2376. DOI:http: //dx.doi.org/10.1109/TSG.2022.3217060.
12. Jingjing Guo, Haiyang Li, Feiran Huang, Zhiquan Liu, Yanguo Peng, Xinghua Li, Jianfeng Ma, Varun G Menon, and Konstantin Kostromitin Igorevich. 2022. ADFL: A poisoning attack defense framework for horizontal federated learning. IEEE Transactions on Industrial Informatics 18, 10 (2022), 6526ś6536.
13. Boyu Hou, Jiqiang Gao, Xiaojie Guo, Thar Baker, Ying Zhang, Yanlong Wen, and Zheli Liu. 2022. Mitigating the Backdoor Attack by Federated Filters for Industrial IoT Applications. IEEE Transactions on Industrial Informatics 18, 5 (2022), 3562ś3571. DOI:http: //dx.doi.org/10.1109/TII.2021.3112100
14. Thien Duc Nguyen, Phillip Rieger, Huili Chen, Hossein Yalame, Helen Möllering, Hossein Fereidooni, Samuel Marchal, Markus Miettinen, Azalia Mirhoseini, Shaza Zeitouni, Farinaz Koushanfar, Ahmad-Reza Sadeghi, and Thomas Schneider. 2022. FLAME: Taming Backdoors in Federated Learning. In Proc. USENIX Security Symposium. 1415ś1432. https://www.usenix.org/conference/usenixsecurity22/ presentation/Nguyen
15. Zheyi Chen, Pu Tian, Weixian Liao, and Wei Yu. 2020. Zero knowledge clustering based adversarial mitigation in heterogeneous federated learning. IEEE Transactions on Network Science and Engineering 8, 2 (2020), 1070ś1083.
16. Yong Li, Yipeng Zhou, Alireza Jolfaei, Dongjin Yu, Gaochao Xu, and Xi Zheng. 2021. Privacy-Preserving Federated Learning Framework Based on Chained Secure Multiparty Computing. IEEE Internet of Things Journal 8, 8 (2021), 6178ś6186.
17. Xiangwang Hou, Jingjing Wang, Chunxiao Jiang, Xudong Zhang, Yong Ren, and Mérouane Debbah. 2023. UAV-Enabled Covert Federated Learning. IEEE Transactions on Wireless Communications 22, 10 (2023), 6793ś6809.
18. Chaosheng Feng, Bin Liu, Keping Yu, Sotirios K. Goudos, and Shaohua Wan. 2022. Blockchain-Empowered Decentralized Horizontal Federated Learning for 5G-Enabled UAVs. IEEE Transactions on Industrial Informatics 18, 5 (2022), 3582ś3592.
19. Pathum Chamikara Mahawaga Arachchige, Peter Bertok, Ibrahim Khalil, Dongxi Liu, Seyit Camtepe, and Mohammed Atiquzzaman. 2020. A Trustworthy Privacy Preserving Framework for Machine Learning in Industrial IoT Systems. IEEE Transactions on Industrial Informatics 16, 9 (2020), 6092ś6102.

20. Xiaoqiang He, Qianbin Chen, Lun Tang, Weili Wang, and Tong Liu. 2022. CGAN-Based Collaborative Intrusion Detection for UAV Networks: A Blockchain-Empowered Distributed Federated Learning Approach. IEEE Internet of Things Journal 10, 1 (2022), 120ś132. [173] Pankaj K Sharma and Dong In Kim. 2019. Random 3D mobile UAV networks: Mobility modeling and coverage probability. IEEE Transactions on Wireless Communications 18, 5 (2019), 2527ś2538.
21. Pankaj K Sharma and Dong In Kim. 2020. Secure 3D mobile UAV relaying for hybrid satellite-terrestrial networks. IEEE Transactions on Wireless Communications 19, 4 (2020), 2770ś2784.
22. M. Carrick, J. H. Reed, and V. Marojevic, "Method for jointly adapting an OFDM waveform and the demodulator for interference mitigation and harsh channels," Feb. 5, 2019, US Patent No. US 10,200,138 B2.
23. F. Pan, Z. Pang, M. Luvisotto, X. Jiang, R. N. Jansson, M. Xiao, and H. Wen, "Authentication based on channel state information for industrial wireless communications," in IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society, Oct 2018, pp. 4125–4130.
24. A. Eldosouky, A. Ferdowsi, and W. Saad, "Drones in distress: A gametheoretic countermeasure for protecting UAVs against GPS spoofing," https://arxiv.org/abs/1904.11568, November 2019.
25. T. Yu, J. Zhao, and Y. Gong, "UAV-aided localization algorithm with relay for train-mounted mobile terminals," Physical Communication, vol. 34, pp. 227 – 234, 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1874490718305913
26. K. Jansen, M. Schfer, D. Moser, V. Lenders, C. Ppper, and J. Schmitt, "Crowd-GPS-Sec: Leveraging crowdsourcing to detect and localize GPS spoofing attacks," in 2018 IEEE Symposium on Security and Privacy (SP), May 2018, pp. 1018–1031.
27. A. Al-Hourani, S. Kandeepan, and S. Lardner, "Optimal LAP altitude for maximum coverage," IEEE Wireless Communications Letters, vol. 3, no. 6, pp. 569–572, Dec 2014.
28. C. Del-Valle-Soto, L. J. Valdivia, and J. C. Rosas-Caro, "Novel detection methods for securing wireless sensor network performance under intrusion jamming," in 2019 Int. Conf. Electronics, Communications and Computers (CONIELECOMP), Feb 2019, pp. 1–8.