ISSN: 2424-8460(O)
2251-2608(P)

Original Research Article

Security risk analysis and countermeasure technologies for unmanned aerial vehicles

Yishi Xue*
Department of Computer Information and Network Security, Jiangsu Police Institute, Nanjing, Jiangsu, 210012, China

Abstract: The expanding deployment of unmanned aerial vehicles (UAVs) across logistics, agriculture, infrastructure inspection, and emergency response has generated corresponding growth in security incidents. This paper presents a systematic survey of UAV security threats and their associated countermeasure technologies. A three-layer risk taxonomy is proposed that classifies threats into physical layer risks, communication layer risks, and data and privacy risks. The cross-layer cascade propagation mechanisms through which localized anomalies escalate into systemic failures are also analyzed. For each risk category, state-of-the-art countermeasures are reviewed, including multi-modal sensor fusion detection, graduated-response counter-UAV systems, network security hardening, digital-twin-enabled airspace governance, and AI-augmented intelligent management. The analysis reveals that effective UAV security governance requires a cross-layer defense-in-depth architecture coordinating detection, prevention, response, and regulatory enforcement.
Keywords: unmanned aerial vehicle; security risk; management and countermeasure

1. Introduction

Unmanned aerial vehicles (UAVs) have transitioned from military platforms into widely deployed civilian tools. Market forecasts suggest the global UAV industry will exceed 41 billion US dollars by 2026, where China accounting for a substantial share of both production volume and operational diversity [1]. UAVs perform tasks ranging from parcel delivery and precision crop spraying to high-voltage transmission line inspection and disaster area reconnaissance.

The expansion of the registered UAV has proportionally widened the attack surface accessible to malicious actors. Chinese civil aviation authorities documented over 20,000 unauthorized flight events in 2024, including multiple incursions into controlled airport zones that forced commercial flight diversions [2]. GPS spoofing experiments have demonstrated that an adversary counterfeit satellite signals can override legitimate navigation inputs and assume control of a target aircraft [3]. Command-channel eavesdropping, firmware-level exploits, and supply-chain backdoors further widen the vulnerability envelope [4,5]. Meanwhile, high-resolution imagery, geolocation logs, and operator records generated during routine missions generate an expanding volume of sensitive data, the unauthorized disclosure of which entails both legal and ethical ramifications [6].

While existing studies have yielded valuable findings, these contributions remain fragmented and siloed across individual threat domains. Deep-learning architectures for GPS anomaly detection have been proposed [3]; privacy-preserving remote identification schemes have been designed [6]; and counter-UAV technology taxonomies have been organized [7]. However, relatively few studies have examined the causal relationship from threat identification through defense selection to governance implementation within a unified analytical framework.

This paper addresses the issue by constructing a three-layer risk taxonomy capturing physical, communication, and data-privacy threats together with their cross-layer propagation dynamics, mapping each risk category to corresponding detection, prevention, and response technologies.

2. Security risk analysis

UAV security threats are coupled through functional dependencies, whereby a disruption originating at one layer may propagate upward to induce failures at adjacent or higher layers. **Figure 1** illustrates the three-layer taxonomy and the cascade propagation paths.

ISSN: 2424-8460(O)
2251-2608(P)

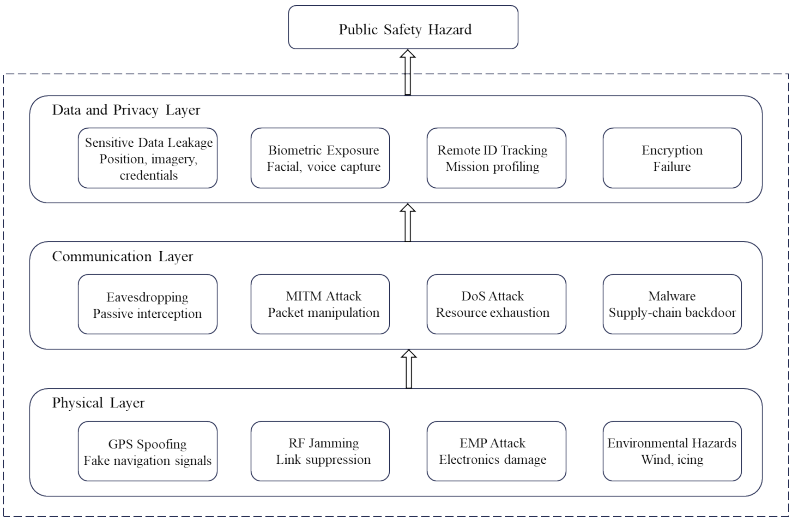

Figure 1. Three-layer UAV security risk taxonomy with cross-layer cascade propagation.

2.1. Physical layer risks

GPS spoofing has emerged as the most extensively investigated physical-layer threat. By transmitting counterfeit ranging signals at power levels exceeding authentic satellite broadcasts, an adversary can induce the target receiver to derive erroneous position, velocity, and timing estimates, potentially commanding the aircraft to deviate from its planned route or enter restricted airspace. Conventional signal processing defences, such as carrier-to-noise ratio monitoring and Doppler shift consistency verification, have proven susceptible to sophisticated spoofing strategies that gradually escalate transmission power to evade detection thresholds. Radio-frequency jamming disrupts command and telemetry links by overwhelming receiver ends, severing operator-UAV connectivity within seconds. Electromagnetic pulse attacks are capable of inflicting irreversible damage to onboard avionics. Environmental factors, such as crosswind and airframe icing, constitute a physical risk that compounds adversarial threats.

2.2. Communication layer risks

The wireless channels employed for UAV command and data transmission possess an inherently broadcast, rendering them fundamentally susceptible to interception and tampering. Passive eavesdropping enables adversaries to silently harvest critical mission data streams, including encrypted flight plans, payload telemetry, and authentication credentials. Moreover, man-in-the-middle (MITM) attacks transcend passive collection by allowing the interceptor to inject, modify, or suppress command packets in real time, introducing unauthorized control inputs with potentially severe flight-safety consequences. Denial-of-service (DoS) campaigns exploit protocol-level or volumetric resource exhaustion to saturate communication links and servers. This vulnerability is further compounded in multi-UAV cooperative formations, where decentralized controllers rely on continuous updates exchanged among neighbouring nodes. A data-injection attack targeting a single aircraft can disseminate corrupted state estimates throughout the inter-vehicle communication topology to destabilize the entire formation geometry.

2.3. Data and privacy risks

Standard UAV operations generate substantial quantities of sensitive information assets, including centimeter-accuracy position trajectories, high-resolution optical imagery, flight-plan metadata, and regulatory remote identification broadcasts. The privacy implications of such data collection are particularly pronounced during surveillance and inspection missions, where onboard sensors may inadvertently record biometric identifiers, such as facial features, voice patterns, and license plate information of individuals who are not aware of such capture. The Remote Identification (Remote ID) regulatory framework introduces a paradoxical tension. Periodic broadcast of aircraft identification and real-time position data is essential for airspace accountability and regulatory compliance.

2.4. Cross-layer cascade propagation

The three risk categories proposed above are tightly coupled through functional dependency chains that can amplify localized anomalies into systemic failures. For instance, A GPS spoofing incident at the physical layer may corrupt the onboard navigation solution, which consequently invalidates the mobility predictions on which

ISSN: 2424-8460(O)
2251-2608(P)

communication-layer routing protocols depend. As routing performance degrades, data-layer confidentiality and integrity mechanisms are undermined due to encrypted packets can no longer be guaranteed reliable delivery to their intended recipients. In the most severe scenario, the compounded failure sequence results in an uncontrolled aircraft operating constituting a direct public-safety hazard. This cascade dynamics is especially pronounced in dense swarm configurations, where tightly coupled inter-vehicle feedback loops ensure that a single-node compromise undergoes rapid diffusion across the entire UAV swarm.

3. Management and countermeasure technologies

3.1. Multi-modal detection and surveillance

Multiple sensor modalities cooperatively can provide comprehensive UAV detection under all conditions. Radar achieves long-range tracking but struggles against small, low-altitude targets with minimal radar cross-sections. Radio-direction sensors passively intercept control signals but suffer localization errors in multipath environments. Electro-optical and infrared cameras offer detailed visual identification while it may be degraded under fog, rain, or low illumination. Acoustic sensors detect characteristic rotor signatures at low cost but are susceptible to urban background noise. Considering these complementary trade-offs, the multi-modal sensor fusion becomes the preferred approach. By performing spatio-temporal alignment across radar, optical, RF, and acoustic channels, fused systems deliver highly reliable detection performance particularly as commercial UAV platforms decrease in size and altitude.

3.2. Counter-UAV systems

Counter-UAV operations follow a sequential workflow of detect, identify, track, and defeat. Defeat measures fall into two categories. Soft-kill methods, such as RF jamming and navigation spoofing, disrupt command links or inject false GPS signals to force the target into failsafe return-to-home or controlled-landing behavior. Hard-kill methods, including net-gun interception, high-energy laser ablation, and directed electromagnetic weapons, physically destroy or incapacitate the target which are generally restricted to military or high-value asset protection. Modern counter-UAV systems implement a graduated-response paradigm: multi-sensor fusion classifies the intruder, the threat assessment engine evaluates its trajectory and payload, and the system selects the least disruptive countermeasure consistent with the threat level. This proportional engagement model balances operational effectiveness and legal accountability.

3.3. Network security hardening

Protecting UAV communication links requires a combination of encryption, intrusion detection, and distributed trust mechanisms. End-to-end encryption forms the fundamental defense. However, standard ciphers such as AES-256 impose computational demands that exceed the processing capacity of many resource-constrained onboard processors, driving active research into lightweight cryptographic primitives. Network-based intrusion detection systems have adopted deep-learning architectures supporting both rule-based recognition of known attack signatures and unsupervised detection of zero-day anomalies. For distributed multi-UAV deployments, blockchain technology contributes an additional solution of security by enabling decentralized node authentication, tamper-evident data logging, and automated trust scoring through smart contracts.

3.4. Digital-twin-enabled airspace governance

Airspace management provides the structural framework in which detection, response, and prevention capabilities are coordinated. The digital air traffic management model transforms physical airspace into a computable resource, allowing conflict detection and aircraft separation. Digital-twin technology builds upon this foundation by constructing and continuously updating a high-fidelity virtual replica of the operational environment, including real-time UAV states, obstacle geometry, and communication conditions. Risk assessment, conflict simulation, and scheduling optimization are first conducted in the virtual domain before validated directives are issued to physical assets. Consequently, airspace governance is shifted from reactive incident handling to anticipatory pre-emptive management [8].

3.5. AI-augmented intelligent governance

Artificial intelligence is increasingly significant to UAV security operations. Deep-learning models are capable of jointly processing communication traffic features, onboard sensor readings, and flight-parameter telemetry. It has achieved low-latency, unified detection of GPS spoofing, command hijacking, and data-injection attacks. For autonomous flight control, model predictive control has demonstrated strong performance in multi-

ISSN: 2424-8460(O)
2251-2608(P)

objective constrained scenarios such as precision landing and dynamic obstacle avoidance [9]. Reinforcement learning has shown potential for adaptive trajectory tracking in partially observable and time-varying environments. However, there are still challenges that need to be faced, such as adversarial robustness of AI models, interpretability of automated decisions, and generalization across heterogeneous operational domains.

Table 1 delineates the mapping of various UAV security countermeasures to their respective risk categories and outlines the key constraints of each approach.

Table 1. Summary of UAV security countermeasure technologies mapped to risk categories and associated limitations.

Risk layer	Representative threats	Countermeasure technologies	Key limitations
Physical	GPS spoofing, RF jamming	ML-based spoofing detection, anti-jam frequency hopping	Evasive spoofers circumvent signal-level detection
Communication	Eavesdropping, MITM, DoS, malware	End-to-end encryption, lightweight cryptography, deep-learning IDS, blockchain trust management	Computational constraints on UAV processors; zero-day exploits evade signature-based IDS
Data and privacy	Data leakage, biometric capture, remote ID tracking	Differential privacy for remote ID, data minimization, encrypted storage	Privacy-utility trade-off; regulatory fragmentation across jurisdictions
Cross-layer	Cascade propagation, swarm destabilization	Multi-modal sensor fusion, digital-twin governance, AI-augmented control	Sensor fusion deployment cost; AI explainability and adversarial robustness

4. Conclusion

This paper has provided a systematic review of security risks and countermeasure technologies for UAVs. A three-layer risk taxonomy has been established, classifying risks at the physical, communication, and data-privacy levels. The cross-layer cascade propagation mechanisms are also analyzed. Countermeasure technologies are examined in accordance with their respective risk categories. Findings reveal that an integrated defense-in-depth architecture is required where detection, prevention, response, and regulatory enforcement are coordinated across all operational layers.

Fundings

This work is supported by General Project of Natural Science Research in Jiangsu Universities, Grant No. 22KJB510017 and General Project of Philosophy and Social Science Research in Jiangsu Universities, Grant No. 2023SJSZ0189.

About the author

*corresponding author:Yishi Xue.

References

[1] Drone Industry Insights. The drone market report 2025–2030[R/OL]. https://www.droneii.com/drone-market-report.

[2] Pu F, Chen Z J, Liu Y, et al. Air traffic management technologies for digital low-altitude integrated operations [J]. Acta Aeronautica et Astronautica Sinica, 2025, 46(11): 531331.

[3] Al-Sabbagh, A., El-Bokhary, A., El-Koussa, S., et al. Enhancing UAV security against GPS spoofing attacks through a genetic algorithm-driven deep learning framework[J]. Information, 2025, 16(2): 115.

[4] Bai N, Hu X, Wang S. A survey on unmanned aerial systems cybersecurity[J]. Journal of Systems Architecture, 2024, 156: 103282.

[5] Kumar N., Chaudhary A. Surveying cybersecurity vulnerabilities and countermeasures for enhancing UAV security[J]. Computer Networks, 2024, 252: 110695.

[6] Cordill B, Fang D, Xu S, et al. A comprehensive survey of security and privacy in UAV systems[J]. IEEE Access, 2025, 13: 12987-13015.

[7] Development review of counter-UAV technologies at home and abroad[EB/OL]. Secrss, 2025. https://www.secrss.com/articles/76379.

[8] Yu P, Tan C, Li W J, et al. Digital twin driven autonomous management and control architecture and key technologies for low-altitude intelligent networks[J]. Sci Sin Inform, 2025, 55: 2449–2470.

[9] Panjavarnam, K, Ismail, Z H, Tang C H H, et al. Model predictive control for autonomous UAV landings: A comprehensive review of strategies, applications and challenges[J]. The Journal of Engineering, 2025.