SCIENCE CHINA
Information Sciences

• REVIEW •

April 2026, Vol. 69, Iss. 4, 141202:1–141202:25
https://doi.org/10.1007/s11432-025-4811-2

Securing the low-altitude economy: a survey

Minrui YAN[1], Ruiqi DONG[1], Qing-Long HAN[1*], Zehang DENG[1], Wanlun MA[1], Xiaogang ZHU[1,2], Wei ZHOU[1], Sheng WEN[1] & Yang XIANG[1]

[1]*School of Science, Computing and Emerging Technologies, Swinburne University of Technology, Melbourne 3122, Australia*
[2]*School of Computer Science and Information Technology, The University of Adelaide, Adelaide 5005, Australia*

Received 29 July 2025/Revised 20 October 2025/Accepted 4 December 2025/Published online 25 March 2026

Abstract The rapid growth of the low-altitude economy, including unmanned aerial vehicles (UAVs) and urban air mobility (UAM), is reshaping industries from transportation to emergency response. Powered by advances in fifth-generation (5G) and 5G-advanced (5.5G) connectivity, artificial intelligence (AI), and new energy systems, these platforms are becoming increasingly autonomous and capable. However, their growing software complexity introduces critical cybersecurity risks. Vulnerabilities in communication protocols, onboard firmware, and AI systems can be exploited to hijack UAVs, disrupt operations, or leak sensitive data. While research has addressed isolated aspects, a unified security perspective is still lacking. This work presents a systematic review of software-level security challenges and defenses in low-altitude UAV/UAM systems. We first categorize major attack surfaces across communication, firmware, and AI layers. Furthermore, we survey defense mechanisms suited to real-time, resource-constrained aerial platforms. Finally, we propose future directions, including quantum-resistant communication protocols, hardware-software cosecurity, and edge-AI-driven architectures. Our work aims to inform researchers, practitioners, and regulators in developing integrated, resilient security strategies for the evolving low-altitude ecosystem.

Keywords unmanned aerial vehicles, urban air mobility, attack surface analysis, network protocol, communication network

Citation Yan M R, Dong R Q, Han Q-L, et al. Securing the low-altitude economy: a survey. Sci China Inf Sci, 2026, 69(4): 141202, https://doi.org/10.1007/s11432-025-4811-2

1 Introduction

The low-altitude economy represents a rapidly emerging sector centered on aviation activities occurring at lower airspace levels and is poised to revolutionize a variety of industries [1]. Enabled by key technological pillars such as unmanned aerial vehicles (UAVs) [2], urban air mobility (UAM) [3], and real-time UAV control systems [4], this new economic domain is gaining global momentum.

It broadly refers to manned and unmanned aviation activities in airspace below about 1000 m. These technologies promise to alleviate urban congestion, expedite last-mile deliveries, and enhance disaster response capabilities. In China alone, the "low-altitude economy" is forecast to expand more than five-fold from roughly USD 93 billion in 2024 to USD 483 billion by 2035 [5], illustrating the global momentum in this domain. Several converging innovations are driving this progress. (1) Advanced connectivity: Next-generation 5G networks (and emerging 5.5G standards) [6] now provide the multi-gigabit speeds and ultra-low latency needed for real-time UAV control. For example, a recent 5G trial linked an autonomous vehicle over 1000 km away with end-to-end latency under 0.2 s. (2) Artificial intelligence (AI): Onboard AI algorithms handle tasks like navigation [7], obstacle avoidance [8], and target recognition [9], enabling high levels of autonomy [10, 11] in UAV operations. (3) New energy technologies: Improvements in batteries and the advent of hydrogen fuel cells are dramatically extending flight endurance. For instance, a prototype hydrogen-powered UAV achieved a 14-hour flight (5800-mile range) with a payload of 10 kg, aided by 5G/LTE links for remote control [12]. Together, these trends are turning concepts such as UAV delivery networks and autonomous eVTOL passenger taxis into a practical reality.

However, the increasing software dependence of the low-altitude economy raises serious security challenges that threaten to undermine safety and public trust. Modern UAVs rely on complex software stacks, including wireless communication protocols, flight control firmware, and AI-based decision systems, and vulnerabilities at any of these layers could lead to catastrophic failures or malicious exploits [13–15]. Indeed, security researchers have demonstrated that unprotected command links can be intercepted via man-in-the-middle attacks, allowing hijackers

* Corresponding author (email: qhan@swin.edu.au)

© The Author(s) 2026. This article is published with open access at link.springer.com.

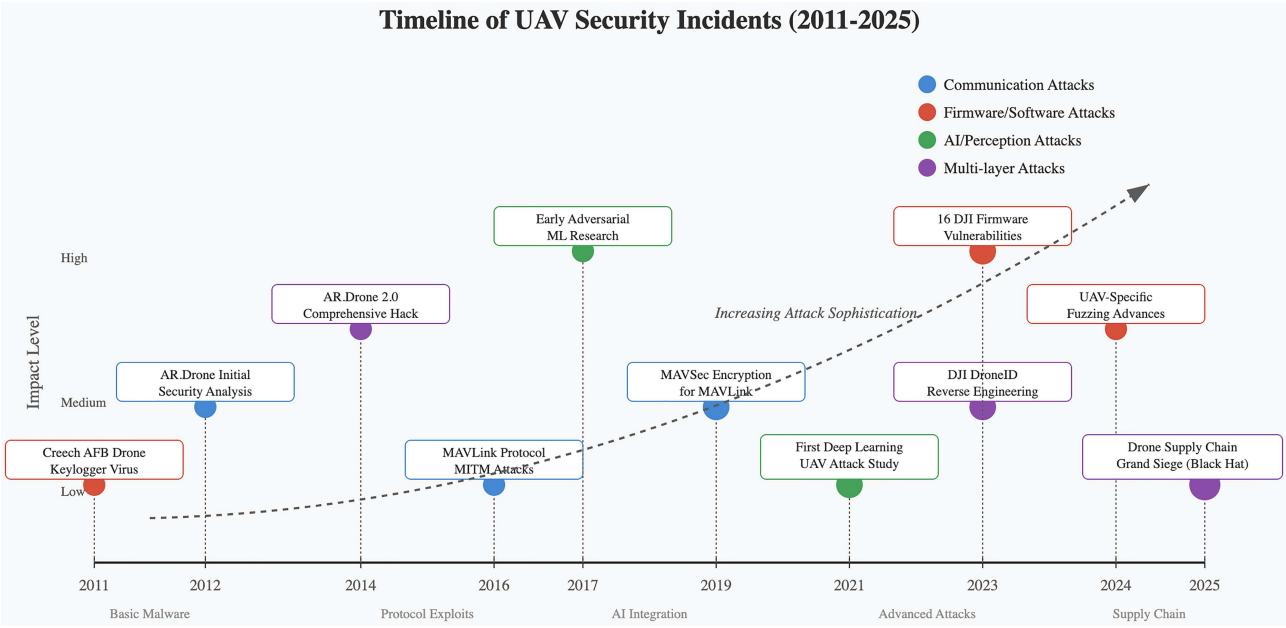

Figure 1 (Color online) Timeline of documented UAV security incidents from 2011 to 2025, illustrating the evolution of attack sophistication and diversity. Events are categorized by primary attack vector: communication attacks (blue circles) targeting wireless protocols and network services; firmware/software attacks (red circles) exploiting code vulnerabilities and update mechanisms; AI/perception attacks (green circles) manipulating machine learning models and sensor inputs; and multi-layer attacks (purple circles) combining multiple exploitation techniques. The upward trend demonstrates increasing attack complexity, with notable milestones including the first military UAV malware infection at Creech AFB in 2011 [21], and comprehensive AR.Drone 2.0 security analysis in 2014 [22], MAVLink encryption development in 2019 [13], emergence of deep learning adversarial attacks in 2021 [23], and supply chain compromises in 2025 [24]. Circle size indicates relative impact severity, with larger circles representing attacks affecting broader systems or introducing novel threat paradigms.

to seize control of a UAV without the operator's knowledge [16–18]. Likewise, UAVs with deep learning models onboard can be fooled by adversarial inputs such as specially crafted camouflage or perturbations, causing the AI navigation or vision system to misbehave [19]. Such incidents could result in UAVs crashing, veering off course, or leaking sensitive data [20]. These threats underscore an urgent need for robust cybersecurity frameworks tailored to the low-altitude economy to ensure that a major security incident does not derail the sector's rapid expansion.

The historical progression of UAV security incidents, as illustrated in Figure 1 [13, 21–24], reveals a clear evolution from opportunistic malware infections to sophisticated multi-layer attacks. Earlier communication-focused surveys [25–27] primarily addressed protocol-level vulnerabilities but offered limited AI security coverage. More recent security or AI-focused surveys [28, 29] broadened the scope to multi-layer analysis, yet none systematically integrated firmware, AI, and regulatory dimensions as undertaken in this work. The timeline begins with the 2011 Creech Air Force Base incident, where a keylogger virus infected ground control stations used to pilot military UAVs over Afghanistan and other conflict zones [21]. This event marked the first publicly acknowledged malware infection in military UAV operations, though the virus was later determined to be credential-stealing malware rather than a targeted attack on UAV systems.

The period from 2012 to 2014 witnessed foundational security research on consumer UAVs, particularly focusing on the Parrot AR.Drone platform. Initial investigations revealed fundamental vulnerabilities in WiFi-based control systems and exposed network services [30]. By 2014, comprehensive security analyses demonstrated complete system compromise possibilities, including unauthorized control takeover and data exfiltration through exposed services such as Telnet and FTP [22]. These early studies established the methodological framework for subsequent UAV security research.

The 2016–2019 timeframe marked a transition toward protocol-level security enhancements. Researchers demonstrated practical man-in-the-middle attacks against the unencrypted MAVLink protocol, the de facto standard for UAV-ground station communication [31]. This vulnerability prompted the development of MAVSec in 2019, which integrated lightweight encryption algorithms, including ChaCha20, into the MAVLink protocol while maintaining compatibility with resource-constrained UAV platforms [13]. The successful implementation demonstrated that security enhancements cannot compromise operational performance.

In recent years, from 2020 to 2025, we have witnessed the emergence of AI-targeted attacks against UAVs because machine learning techniques have been increasingly integrated into UAVs' systems. The first comprehensive

Table 1 Comparison with previous UAV/UAM survey papers.

Survey	Scope (UAV/UAM)	Software layers	AI security coverage	Policy/standards link	Quantitative synthesis
Earlier communication-focused surveys					
Pandey et al. [25]	UAV comms	Comm.	Limited	Limited	–
Sharma & Mehra [26]	UAV IoT	Comm.	–	–	–
Fotouhi et al. [27]	UAV cellular	Comm./Std.	–	Moderate	–
Security or AI-focused UAV surveys					
Kumar & Chaudhary [28]	UAV security	Multi-layer	–	–	–
Tlili et al. [29]	UAV+AI	Multi-layer	Perception	–	–
This review (2025)	UAV+UAM	Comm., Firmware, AI	Perception, decision poisoning, and model extraction	ICAO/FAA/EU mapping	Highlights + gaps

study about AI-targeted attacks was published in 2021, demonstrating that carefully crafted perturbations could cause navigation failures and collision risks [23]. The 2023 disclosure of DJI DroneID vulnerabilities represented a watershed moment, with researchers documenting 16 security flaws affecting multiple UAV models and revealing that the proprietary tracking protocol transmitted unencrypted location data of both UAVs and pilots [32]. Most recently, the scheduled presentation at Black Hat Asia 2025 on supply chain attacks highlights the evolution toward systemic threats that compromise entire UAV ecosystems through development and distribution channels [24].

This temporal analysis reveals three distinct phases in UAV security evolution. The initial phase (2011–2014) focused on discovering basic vulnerabilities in consumer platforms through manual testing and reverse engineering. The intermediate phase (2015–2020) emphasized protocol security and the development of defensive mechanisms. The current phase (2021–present) addresses emergent threats from AI integration and supply chain complexity. Each phase has built upon previous discoveries while introducing novel attack vectors that reflect technological advances in UAV capabilities and deployment scenarios.

While some efforts have begun addressing these issues, comprehensive analyses of software security in this emerging domain are still lacking. Existing research tends to focus on isolated aspects of the problem. For example, in the area of communications, the UAV protocol MAVLink, which is widely used for UAV-ground station communication [13], has been retrofitted with encryption schemes to prevent eavesdropping and command injection. In parallel, hardware-assisted approaches like UAV authentication based on physical unclonable functions (PUFs) [33] have been explored to secure devices against impersonation or physical capture. Likewise, the robustness of UAV AI systems is being studied. Recent work [20] proposes ensemble deep-learning defenses to harden UAV vision models against adversarial attacks, within the latency and weight constraints of onboard electronics. Each of these initiatives offers pieces of the solution, yet we lack a unifying perspective that ties them together. In other words, so far, there are no surveys that have systematically examined the full range of software security challenges in the low-altitude economy, spanning communications, firmware, and AI, or assessed how emerging solutions in one area might complement others.

The gap of lacking systematic knowledge motivates our work: by consolidating scattered research insights and real-world case studies, we aim to provide a holistic understanding of where the security pain points lie and how they can be mitigated in tandem. Such an overview is crucial for researchers, industry practitioners, and regulators to prioritize efforts and devise integrated protection strategies for next-generation aerial platforms. The comparison with existing surveys is shown in Table 1. In this paper, we present a systematic review of cybersecurity challenges and defenses in the low-altitude economy. Our contributions are threefold.

• **Attack surfaces.** We identify and categorize the major software-level attack surfaces in low-altitude economy, including vulnerabilities in wireless links (communication protocols and networking), onboard software & firmware (flight controllers, operating systems, and update mechanisms), and AI components (autonomy algorithms and sensor data processing). This taxonomy clarifies where and how UAVs and UAM vehicles are exposed to digital threats.

• **Defense methods.** We survey and synthesize existing defense mechanisms addressing these vulnerabilities. This includes secure communication protocols (encryption and authentication techniques for command-and-control links), software and firmware protections (secure boot, integrity attestation, and malware detection tailored to UAVs), and AI robustness enhancements (methods to detect or withstand sensor spoofing and adversarial inputs). We highlight the state of the art in each category and discuss how these solutions meet the unique constraints of the platform of the low-altitude economy (e.g., real-time operation and limited computing resources).

• **Future directions.** Based on the gaps identified, we outline open research challenges and promising future directions for the security of the low-altitude economy. Current countermeasures remain insufficient to completely eliminate risks. We discuss potential approaches such as quantum-resistant communication protocols for UAV networks, AI-driven security architectures at the edge, and cross-domain collaborations (borrowing techniques from IoT and automotive security). These forward-looking perspectives are designed to assist researchers and stakeholders in advancing the security posture of the low-altitude ecosystem going forward.

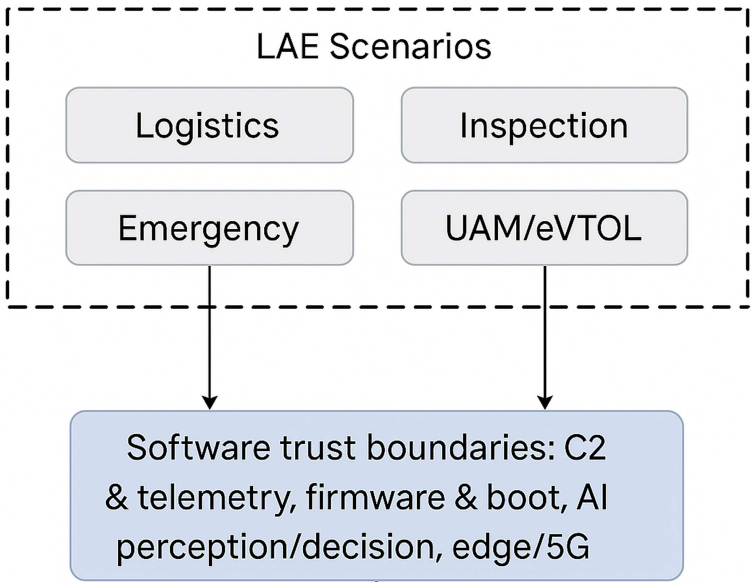

Figure 2 (Color online) LAE application scenarios.

The remainder of this paper is organized as follows. Section 2 provides an overview of software architectures in the low-altitude economy, establishing context for the subsequent discussion. Section 3 analyzes the key security threats and attack vectors in these systems, as identified from literature and incident reports. Section 4 reviews existing mitigation techniques and defense solutions corresponding to the threats. In Section 5, we discuss emerging approaches and propose future research directions to address the security challenges that are not yet fully resolved. Section 6 concludes the paper with a summary of key insights.

2 Overview of low-altitude economy

2.1 The system of low-altitude economy

A system of low-altitude economy is a framework that integrates infrastructure, regulations, and technologies to enable safe and efficient operations of aerial vehicles (e.g., UAVs, eVTOLs) within the airspace below 1000 m [29]. It addresses challenges such as air traffic management, real-time monitoring, and collision avoidance in complex urban or rural environments. Key components include communication networks, autonomous flight algorithms, and regulatory compliance mechanisms. Low-altitude security (LAS) supports applications like logistics, infrastructure inspection, and emergency response, forming the foundation for the emerging low-altitude economy. This section provides the context for understanding the software architecture required to realize such systems. The low-altitude ecosystem (LAE) application is shown in Figure 2.

2.2 Integration with 5G/5.5G for secure LAE operations

As shown in Table 2, 5G/5.5G capabilities strengthen LAE security and safety when engineered as part of the software stack.

- **URLLC** reduces command/telemetry latency, improving resilience to DoS-induced queueing and enabling timely failsafes.
- **Network slicing** isolates safety-critical flows (C2, Remote ID) from payload video, constraining blast radius under attacks.
- **MEC/edge** hosts key services (attestation, anomaly detection) close to UAVs for rapid response and privacy-preserving analytics.
- **RedCap/NTN** extend coverage and energy efficiency for LAE fleets; **sidelink** supports resilient peer-to-peer swarms.
- **Security primitives** (e.g., SIM-based identity, cipher agility) complement PUF-based device authentication.

Table 2 5G/5.5G features and their corresponding security capabilities for LAE.

5G/5.5G feature	What it enables	Security/safety impact
URLLC	Low-latency, high-reliability C2	Faster control loops; mitigates DoS backpressure; supports timely evasive action
Network slicing	Dedicated logical networks per service type	Limits lateral movement; enforces QoS/priority isolation for safety-critical traffic
MEC/edge computing	On-path computation near base stations	Enables onboard–offboard cooperative detection, trusted attestation, and privacy-preserving analytics
Sidelink (PC5)	Direct UAV–UAV or UAV–vehicle communication	Builds resilient swarms and fallback connectivity when infrastructure is degraded or jammed
RedCap / NTN	Reduced-capability and non-terrestrial network access	Extends secure service envelope to remote areas; reduces reconnect churn; improves continuity
Crypto agility	Algorithm update and negotiation flexibility	Enables rapid mitigation of broken ciphers; supports migration toward post-quantum cryptography

Figure 3 (Color online) The software architecture of the system of low-altitude economy.

2.3 Software architecture of low-altitude economy

As shown in Figure 3, the software architecture for low-altitude economy employs a three-tiered hierarchical structure augmented by cross-layer modules, designed to unify hardware control, autonomous intelligence, and regulatory interoperability. At its core, the hardware abstraction layer (HAL) abstracts heterogeneous sensors and propulsion systems into standardized interfaces, while the autonomous decision layer (ADL) synthesizes real-time perception and decision-making through hybrid AI and rule-based paradigms. The Service Orchestration Layer exposes mission-critical capabilities via domain-specific APIs and human-machine interfaces. Vertically spanning these tiers, the Security & Compliance Fabric embeds cryptographic controls and airspace regulation logic directly into the architecture's core, ensuring adherence to International Civil Aviation Organization (ICAO) Unmanned Aircraft Systems (UAS) standards [34]. This layered yet integrated approach enables deterministic sub-50-ms actuation cycles, modular subsystem upgrades, and seamless integration with existing aviation infrastructure.

2.3.1 *Architectural frameworks*

(1) Hardware abstraction layer for the system of low-altitude economy is an intermediary layer between hardware components (sensors, motors, communication modules) and upper-layer software (flight control, navigation). Its core purpose is to mask hardware-specific details by providing standardized interfaces (e.g., data acquisition, control commands), allowing developers to bypass direct hardware driver manipulation (e.g., IMU drivers, ESC

PWM protocols, CAN bus communication) and focus on application logic across platforms (e.g., STM32/Pixhawk compatibility). Typical implementations include sensor drivers (ROS drivers packages), communication protocols (MAVLink), RTOS interfaces (FreeRTOS task abstraction), and support for mainstream frameworks (PX4 [34], ROS 2 [35], DJI SDK [36]), ensuring code reusability and cross-platform robustness.

(2) Service orchestration layer is a middleware framework designed to automate and coordinate complex workflows across distributed systems, applications, and microservices. Abstracting infrastructure dependencies, it enables seamless integration, dynamic resource allocation, and policy-driven management of heterogeneous services. Core components include declarative APIs, event-driven task schedulers, and a policy engine for enforcing governance, scalability, and fault tolerance. This layer ensures optimal service delivery in cloud-native environments, IoT ecosystems, and hybrid architectures, while simplifying cross-platform interoperability and lifecycle management. Key advantages include reduced operational overhead, real-time adaptability to changing workloads, and unified visibility into end-to-end service performance.

(3) Autonomous decision layer (ADL) for the aerial vehicles of low-altitude economy bridges perception (sensors, LiDAR) and execution (flight control), translating environmental data and mission goals into real-time actions via standardized interfaces. It abstracts sensor fusion (e.g., SLAM, Kalman filters), decision engines (reinforcement learning, behavior trees), and path planning (e.g., A Star and Rapidly-exploring Random Tree Star), enabling obstacle avoidance, task optimization, and dynamic replanning. Developers bypass raw perception processing, focusing on high-level logic (e.g., mission priorities, safety constraints). ADL integrates fault tolerance (e.g., fallback states, redundancy) and human-AI collaboration (e.g., natural language commands, override protocols), ensuring adaptability across different scenarios such as delivery and inspection.

2.3.2 *Key software components*

The system of low-altitude economy relies on a suite of specialized software components to achieve autonomous operation. These components bridge hardware capabilities with mission requirements through real-time processing, sensor fusion, and adaptive control.

(1) Sensor drivers and data fusion modules. Sensor drivers serve as the foundational layer for environmental perception, translating raw hardware signals from heterogeneous sensors—LiDAR, inertial measurement units (IMUs), and multispectral cameras—into structured data streams. They enforce precise temporal synchronization across devices through protocols such as IEEE 1588 Precision Time Protocol (PTP) [37], aligning sensor measurements to microsecond accuracy. Data fusion algorithms integrate these multimodal inputs into cohesive spatial representations, employing techniques like extended Kalman filters (EKF) to reconcile GPS coordinates with inertial data for robust localization. Spatial calibration routines further refine sensor alignment, utilizing nonlinear optimization frameworks to minimize extrinsic errors between LiDAR and camera frames.

(2) Coordination middleware. Coordination middleware enables collaborative autonomy by orchestrating communication, task allocation, and formation control across distributed agents. Protocol stacks prioritize low-latency telemetry exchange and fault-tolerant consensus mechanisms, often utilizing lightweight binary encodings (e.g., MAVLink [13]) to minimize bandwidth overhead. Decentralized decision-making frameworks employ auction-based algorithms or gradient descent optimization to allocate targets dynamically, balancing workload and energy constraints. Such systems inherently manage topological changes, such as node failures or network partitions, through heartbeat monitoring and redundant routing paths. Applications range from synchronized light shows to industrial inventory management, where fleets coordinate to survey large-scale infrastructure.

(3) Flight vontrollers. Flight control systems govern platform stability and motion execution, converting navigation directives into actuator commands. These systems operate through layered architectures: low-level firmware manages real-time pulse-width modulation (PWM) signals for motor control, while high-level algorithms execute adaptive PID loops to track attitude and trajectory references. Open-source platforms like PX4[1)] and ArduPilot[2)] extend this paradigm with modular design, enabling customization for diverse airframe configurations. Dynamic disturbance observers within these controllers compensate for environmental perturbations, such as wind gusts, by adjusting rotor thrust vectors in real time. The ArduPilot ecosystem, for instance, dynamically reroutes flight paths when proximity sensors detect obstacles, illustrating the integration of reactive control into mission workflows.

(4) Edge AI inference engines. Onboard AI engines enable autonomous UAVs to perceive, reason, and adapt by executing optimized machine learning models at the edge. These systems transform raw sensor data into actionable insights: convolutional neural networks (CNNs) analyze 4K camera feeds to detect sub-centimeter

1) https://px4.io/.
2) https://ardupilot.org/.

Table 3 Mapping taxonomy elements to standards and certification levers (illustrative).

Taxonomy element	ICAO UAS (global)	FAA part 107/UTM (US)	EU U-Space (EU)
A1 protocol exploits	Secure C2/ATS links; communication integrity requirements	Remote ID; C2 reliability constraints	U1–U3 service tiers; network ID and geo-awareness
A2 service exposure	Software assurance for exposed services	Ground control cyber hygiene practices	Service provider security obligations
A3 denial of service (DoS)	Resilience and contingency procedures	Lost-link procedures; operational limits	Strategic deconfliction and fallback modes
B1 firmware tampering	Airworthiness software integrity; trusted updates	Maintenance and update traceability	SORA evidence requirements; change control protocols
B4 supply chain	Configuration management; provenance tracking	Supplier control and SBOM requirements	Notified body audit and certification trails
C1–C4 AI threats	Safety assessments and assurance frameworks	Waivers for operations over people or critical infrastructure	Specific category risk mitigations and AI safety requirements

obstacles like power lines, while reinforcement learning policies dynamically adjust flight paths to balance mission objectives (e.g., inspection accuracy vs. battery life). During sensor failures or environmental extremes, AI arbitrates between conflicting inputs—for example, fusing thermal imagery with inertial data for navigation in darkness, or switching to visual-inertial odometry (VIO) when GPS signals degrade. Hardware-software co-design is critical: NVIDIA Jetson's tensor cores accelerate multi-sensor inference, while model compression techniques (e.g., pruning, quantization) reduce compute loads by 60% [38], sustaining real-time performance under 15 W power budgets.

2.4 China's low-altitude security practices

We summarize China-specific practices relevant to LAE security: (i) a real-name registration regime for UAV operators and platforms; (ii) cloud-based supervision and UTM-like platforms (e.g., municipal deployments such as SILAS) supporting geo-awareness, flight authorization, and incident tracing; and (iii) BeiDou (BDS) integration for resilient PNT, including anti-spoofing and differential services that improve navigation integrity. These practices complement the standards landscape discussed in Table 3.

3 Security challenges in software system

The modern systems of low-altitude economy confront increasingly security threats characterized by multi-layered vulnerabilities. As conceptualized in Figure 4, research reveals three interdependent threat domains. The detailed taxonomy is listed in Table 4 [13,21–23,25–28,30–32,39–79], which synthesizes findings from communication security studies [13, 22, 25–27, 30, 31, 40–45, 48, 53–56, 64–69], firmware and software security research [21, 32, 46, 47, 50, 57–63, 70–79], and AI security investigations [23, 29, 39, 49, 51, 52]. (A) **Communication security** challenges emerge from fundamental protocol design vulnerabilities and interception techniques that exploit wireless transmission characteristics. (B) **Software and firmware security** arises from code exploitation methodologies and increasingly complex supply chain compromises that introduce vulnerabilities at multiple stages of development. (C) **AI security** threats represent an emerging frontier where adversarial learning techniques target perception and decision pipelines with carefully crafted perturbations designed to cause system failures.

3.1 (A) Communication security

Communication security serves as the fundamental pillar of UAV defense systems [80, 81], establishing the first line of defense against unauthorized access and control. The wireless nature of UAV communications introduces inherent vulnerabilities that traditional wired systems do not face [26]. Signal propagation through open air enables adversaries to intercept transmissions from considerable distances without physical access to the system [40]. The primary objective extends beyond simple data confidentiality to encompass comprehensive protection against eavesdropping, message tampering, and complete command hijacking scenarios [41].

Achieving robust communication security in resource-constrained aerial platforms necessitates a carefully orchestrated multi-layered strategy. This approach must balance computational efficiency with security strength, incorporating lightweight cryptographic mechanisms specifically designed for embedded systems [27]. The integration of rigorous authentication protocols ensures that only authorized entities can establish communication channels, while resilient protocol designs provide defense-in-depth against various attack vectors [42]. Physical-layer security mechanisms add an additional dimension of protection by exploiting channel characteristics unique to legitimate communication pairs [82].

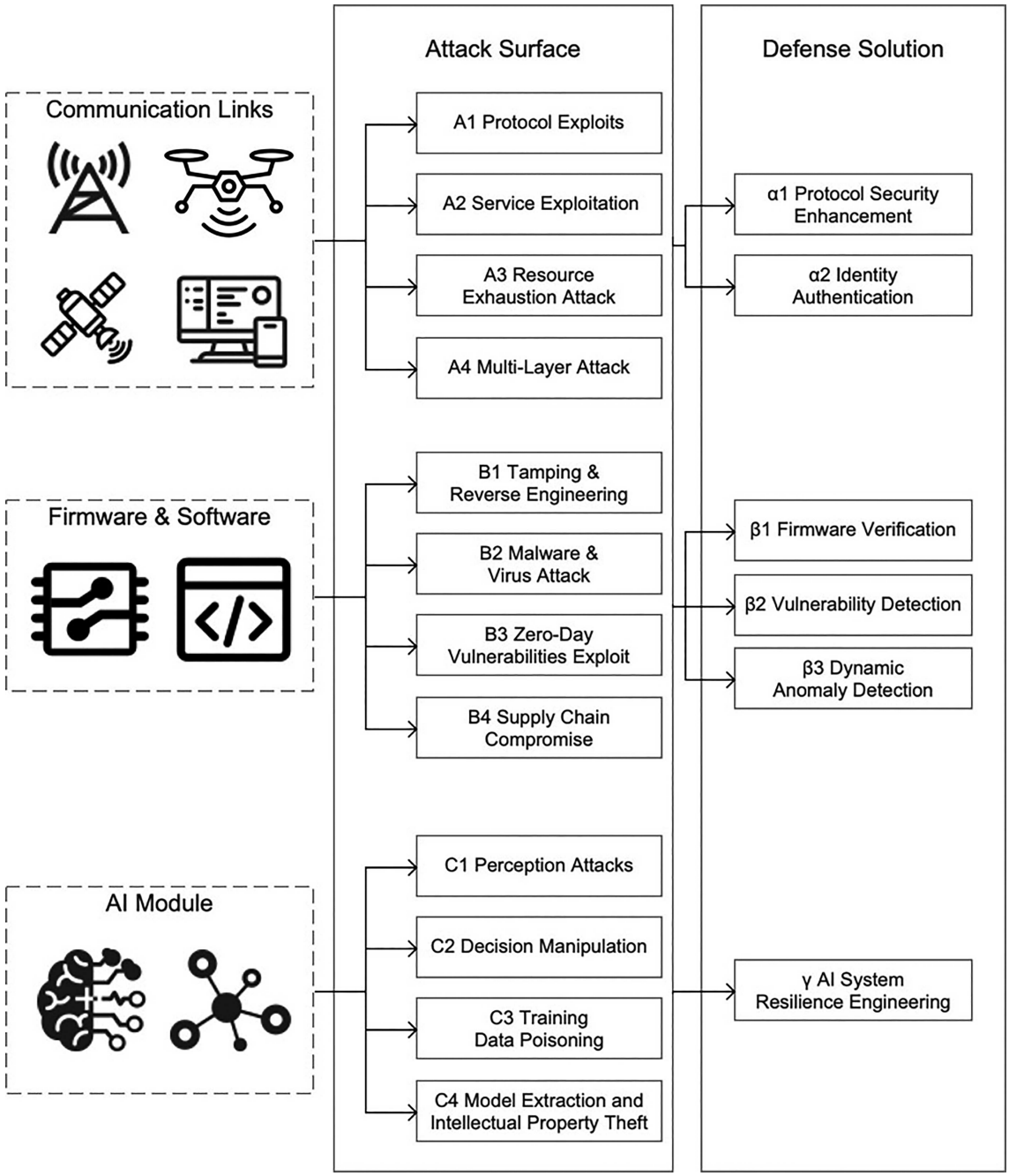

Figure 4 Security challenges and defense solutions in the software system of low-altitude economy, highlighting interdependencies between communication, firmware, and AI module layers.

3.1.1 *(A1) Protocol exploits*

Protocol-level vulnerabilities represent the most fundamental attack surface in UAV communication systems. These vulnerabilities stem from inherent design flaws or implementation errors that create exploitable weaknesses throughout the communication stack. The transmission of sensitive operational data in plaintext format remains surprisingly common in legacy UAV systems [25]. This includes critical flight commands, telemetry data streams, and authentication credentials that traverse wireless channels without any cryptographic protection. The absence of proper encryption transforms every communication session into a potential intelligence-gathering opportunity for adversaries. Experimental evaluations demonstrate the severity of these vulnerabilities: unencrypted MAVLink communications can be intercepted with >95% packet capture rate at distances up to 1 km using commodity hardware [31]. Man-in-the-middle attacks against WiFi-based control systems achieve command injection success rates of 87%–92% within 3–5 s of initial positioning [22, 44].

Table 4 Systematic taxonomy of UAV security research: classification of attack and defense vectors (A, α: communication, B, β: firmware/software, C, γ: AI, detailed in Sections 3 and 4), and technical attributes. In Type, S: survey, C: case study, R: report, M: proposed method.

Study	Type	Challenge	Defense	Attack entity	Defense strategy
[25]	S	A1–A4, B1–B3	α1	–	–
[32]	C	A1, B1	–	Firmware, UAVID protocol	–
[39]	M	C2	γ	Wireless transmissions	Higher SINR thresholds
[26]	S	A1, A2	α1, α2	–	–
[40]	C	A1	–	WiFi	–
[41]	S	A1, A2	α1, α2	–	–
[27]	S	A1	α1	–	–
[42]	S	A1	α1	–	–
[43]	S	A1	–	–	–
[31]	C	A1	–	Open-source software	–
[44]	C	A1, A2	–	GPS, DJI-SDK	–
[22]	C	A2, A4, B1	α2	WiFi, GNU/Linux OS	Coupling with iptables
[45]	C	A3, B3	–	WiFi, ARDiscovery	–
[30]	C	A4, B3	α1, α2, β1	Unencrypted WLAN, UDP	Encrypted WLAN
[46]	S	B1, B3	–	–	–
[21]	R	B2	–	Host-based security system	–
[47]	M	B1	β1	Firmware	Reverse engineering & patching
[48]	C	A1, A2, B3	α2	FTP, RF	Hash-based message authentication code
[23]	M	C1	γ	UAV cyber-physical systems	Adversarial training & defensive distillation
[49]	M	C1	–	UAV trackers	–
[50]	R	B2, B4	–	TTPs, toolsets	–
[51]	M	C1	γ	AI models in UAV	Adversarial training
[52]	M	C1	–	Object detection with UAVs	–
[53]	M	A1	α1	PHY-layer security mechanisms	Two-factor authentication mechanism
[54]	M	A1	α1	Explicit storage of a private key	PUF-based dynamic secret-key strategy
[55]	M	A1	α1	Authorization in UAV networks	PUFs within the flying ad-hoc network
[13]	M	A1	α1	Security vulnerabilities of the MAVLink	New security-integrated mechanism
[56]	M	A1	α1	Stored secret keys for authentication	New lightweight and secure authentication
[57]	M	–	β3	Anomalous behaviour in aircraft	LSTM feep learning autoencoder
[58]	S	–	β3	–	–
[59]	M	–	β3	Data anomaly	New online subspace tracking
[60]	M	–	β3	Data anomaly	S3VM classification
[61]	M	–	β3	Anomaly detection	A Dataset for fault detection
[62]	S	–	β3	–	–
[63]	M	–	β3	Anomaly detection	New LSTM correlation analysis
[64]	C	A1	α1, α2	Authentication strategies	Security-specific operation in protocol
[65]	M	A1	α2	Traditional authentication mechanism	New lightweight authentication method
[66]	M	A1	α2	Authentication scheme	New SM2 authentication method
[67]	M	A1	α2	Authentication mechanism	New public-key based authentication
[68]	M	A1	α2	Authentication mechanism	PUFs for authentication
[69]	M	A1	α2	Automatic UAV identification	Behavior-based intelligent identification
[70]	M	B1	β1	Firmware update	Block-chain based firmware update
[71]	M	B1, B2	β1, β2	Malicious behavior of the firmware	New malicious behavior detection method
[72]	M	B1	β1	Tampering the firmware	New blockchain-based verification method
[73]	M	–	β2	Rigorous safety standards	New fuzzing framework
[74]	S	A1, B3	β2	–	–
[75]	M	–	β2, β3	Misconfigured parameters	New fuzzing framework
[76]	S	B1	β2	–	–
[77]	M	B1	β2	Known vulnerabilities	New vulnerability search methods
[78]	S	B1, B4	β2	–	–
[79]	M	B1	β2	Searching bug in firmware	New vulnerability detection methods
[29]	S	A1–A4, B1–B3	–	–	–

Message authentication mechanisms in many UAV protocols suffer from critical deficiencies that enable forgery attacks. Insufficient source verification allows attackers to craft messages that appear to originate from legitimate control stations [32]. Similarly, inadequate integrity protection mechanisms fail to detect message modifications during transmission, enabling attackers to alter command parameters or telemetry values without detection [43]. The lack of mutual authentication between communicating parties creates asymmetric trust relationships where UAVs accept commands from any entity capable of formatting valid protocol messages. Replay attack vulnerabilities persist due to insufficient temporal validation mechanisms in protocol designs. Without proper sequence numbering or timestamp verification, adversaries can capture legitimate command sequences and retransmit them at opportune moments [31]. This enables attacks ranging from simple trajectory manipulation to complex multi-stage exploitation chains. The combination of these vulnerabilities creates a cascading effect where successful exploitation of one weakness facilitates more attacks.

Man-in-the-middle attacks represent the culmination of protocol-level vulnerabilities, enabling adversaries to position themselves as invisible intermediaries in the communication path. Initial positioning often exploits lower-layer protocol weaknesses such as address resolution protocol spoofing in WiFi networks or deauthentication frame injection [44]. Once positioned, attackers leverage application-layer protocol deficiencies to conduct real-time message interception and modification. The absence of end-to-end encryption in protocols like unencrypted MAVLink transforms these attacks from theoretical possibilities into practical exploitation techniques demonstrated in real-world scenarios.

3.1.2 *(A2) Service exploitation*

The exposure of network services on UAV platforms creates additional attack vectors beyond protocol-level vulnerabilities. Many commercial and hobbyist UAVs inadvertently expose standard network services through their wireless interfaces, often with minimal security hardening [22]. These services, including Telnet for remote administration, FTP for file transfer, and HTTP for web-based configuration interfaces, frequently retain default configurations that prioritize ease of use over security.

Beyond authentication weaknesses, service implementations often contain exploitable vulnerabilities such as buffer overflows in input parsing routines or injection flaws in command processors. These vulnerabilities grant attackers the ability to execute arbitrary code within the UAV's operating system context. Once system-level access is achieved, adversaries can exfiltrate sensitive operational data, including flight logs, captured imagery, and stored authentication tokens. The compromise extends beyond data theft to include persistent backdoor installation and real-time flight control manipulation.

3.1.3 *(A3) Resource exhaustion attacks (denial-of-service)*

Resource exhaustion attacks exploit the fundamental asymmetry between attack cost and defense overhead in resource-constrained UAV systems. These attacks aim to degrade or completely halt UAV operations by overwhelming finite computational resources, including processor cycles, memory allocation, and network bandwidth [45]. The limited resources available in embedded UAV platforms make them particularly susceptible to carefully crafted denial-of-service attacks that would be ineffective against more powerful ground-based systems. Network-layer flooding attacks generate high volumes of malformed or computationally expensive packets targeting specific protocol handlers. The lack of robust rate-limiting mechanisms in many UAV communication stacks allows attackers to saturate processing queues with minimal effort. Application-layer attacks focus on resource-intensive operations such as cryptographic verification or complex state machine transitions. By triggering these operations repeatedly, attackers force the UAV to allocate disproportionate resources to attack traffic rather than legitimate control commands.

The impact of successful resource exhaustion extends beyond temporary service disruption to create safety-critical scenarios. Delays in command processing can cause UAVs to miss crucial navigation updates or collision avoidance maneuvers. Complete system unresponsiveness may trigger fail-safe mechanisms such as return-to-home procedures, effectively accomplishing the attacker's goal of mission disruption. The cascading effects of resource exhaustion in interconnected UAV swarms amplify individual attacks into system-wide failures.

3.1.4 *(A4) Multi-layer attacks*

Adversaries increasingly employ multi-layer attack strategies that combine vulnerabilities across different system components to achieve persistent compromise. These attacks demonstrate an advanced understanding of UAV system architectures and the interdependencies between communication, firmware, and application layers [30].

Initial compromise often begins with relatively simple attacks against exposed services or protocol weaknesses, establishing a foothold from which to launch more complex exploitation chains.

The attack progression typically follows a systematic escalation pattern designed to maximize persistence while minimizing detection probability. Initial access through communication-layer vulnerabilities provides limited privileges sufficient for reconnaissance and lateral movement [22]. Attackers then identify and exploit firmware or operating system vulnerabilities to escalate privileges and disable security mechanisms. The installation of rootkits or firmware modifications ensures persistence across system reboots and security updates.

3.2 (B) Firmware & software security

Firmware and software security represent the foundational trust layer in the systems of the low-altitude economy, where any compromise can cascade into complete system failure. The embedded nature of UAV firmware creates unique security challenges distinct from traditional computing platforms [47]. Limited computational resources restrict the deployment of conventional security mechanisms, while real-time operational requirements prevent the use of computationally intensive protection schemes. The attack surface encompasses not only the flight control firmware but also extends through the entire software stack, including bootloaders, device drivers, communication middleware, and application-level services. The heterogeneous nature of UAV software ecosystems compounds security challenges through integration complexity. Modern UAVs incorporate components from multiple vendors, each potentially introducing vulnerabilities through inadequate security practices or insufficient integration testing [46]. The lack of standardized security frameworks across the industry results in inconsistent protection levels where the weakest component determines overall system security. Supply chain risks further complicate the security landscape as malicious actors target upstream dependencies to compromise multiple downstream systems simultaneously.

3.2.1 *(B1) Tampering & reverse engineering*

Firmware tampering attacks exploit both physical and logical access vectors to modify critical system components and bypass security controls. Physical attacks against UAV hardware involve direct manipulation of memory chips, debug interfaces, and communication buses [47]. Attackers employ specialized hardware tools such as logic analyzers and chip programmers to extract firmware images directly from flash memory. Once extracted, reverse engineering techniques, including static disassembly and dynamic analysis reveal implementation details, cryptographic keys, and exploitable vulnerabilities.

The manipulation of sensor data streams represents a particularly insidious form of tampering that undermines the integrity of autonomous decision-making. Attackers inject false readings into sensor communication channels by exploiting unprotected inter-chip communication protocols [46]. For instance, forging inter-integrated circuit or serial peripheral interface signals allows adversaries to corrupt inertial measurement unit data, causing navigation errors or triggering emergency landing procedures. The absence of cryptographic authentication on internal buses enables these attacks to proceed undetected by higher-level software components.

Advanced reverse engineering campaigns target proprietary communication protocols and control algorithms that manufacturers attempt to protect through obscurity. Systematic protocol analysis reveals message formats, command structures, and state machine implementations. This knowledge enables the construction of rogue control stations capable of issuing unauthorized commands indistinguishable from legitimate control inputs. The extraction of hardcoded cryptographic keys through differential power analysis or fault injection attacks permanently compromises the security of affected systems, as these keys often cannot be updated in fielded devices.

3.2.2 *(B2) Malware & virus attacks*

The increasing complexity and connectivity of UAV systems create fertile ground for malware proliferation previously confined to traditional computing platforms. Modern UAVs run operating systems derived from embedded Linux distributions, inheriting both the flexibility and vulnerability of these platforms [21]. The integration of third-party libraries, network services, and application frameworks introduces multiple potential infection vectors that malware authors actively exploit.

UAV-specific malware exhibits unique characteristics adapted to the operational environment and objectives of aerial platforms. Payload modules focus on flight control manipulation, sensor data exfiltration, and communication interception rather than traditional cybercrime activities. Persistence mechanisms exploit UAV-specific features such as firmware update processes and configuration storage to survive system resets. The limited user interaction with UAV systems reduces the effectiveness of traditional anti-malware solutions that rely on user awareness and manual intervention.

3.2.3 *(B3) Zero-day vulnerabilities exploit*

Zero-day vulnerabilities in UAV firmware present critical risks due to the extended patch cycles characteristic of embedded systems. The discovery-to-patch timeline often spans months or years, during which systems remain vulnerable to exploitation [48]. Unlike traditional software platforms with automated update mechanisms, UAV firmware updates require manual intervention and often involve operational downtime that users reluctantly accept. This creates a large population of vulnerable systems even after patches become available.

The complexity of modern UAV software stacks multiplies the potential for undiscovered vulnerabilities. Integration points between components from different vendors create unexpected interactions that security testing may not adequately cover. Vulnerabilities frequently emerge from the adaptation of general-purpose software components to UAV-specific use cases without sufficient security hardening. The real-time requirements of flight control systems introduce race conditions and timing-dependent bugs that traditional testing methodologies fail to detect.

3.2.4 *(B4) Supply chain compromise*

Supply chain attacks against UAV ecosystems represent an emerging threat vector with potentially catastrophic consequences. These attacks target the software development and distribution pipeline rather than individual deployed systems, achieving scalable compromise across entire fleets. Attackers infiltrate development environments, build systems, and distribution networks to inject malicious code that appears legitimate to downstream consumers. The trust relationships inherent in software supply chains transform single compromises into industry-wide vulnerabilities. The UAV industry's reliance on open-source components and third-party SDKs creates numerous entry points for supply chain attacks. Malicious contributions to popular open-source projects may remain undetected for extended periods while being incorporated into commercial products. Compromised development tools inject backdoors during the compilation process, ensuring that even source code audits fail to detect the malicious modifications. The lack of reproducible builds in many UAV development environments prevents effective verification of binary integrity against known-good sources.

Distribution channel compromises multiply the impact of supply chain attacks by targeting the final delivery mechanism to end users. Attackers compromise update servers, signing certificates, or distribution platforms to deliver malicious firmware disguised as legitimate updates. The automatic update mechanisms intended to improve security become vectors for mass compromise when the distribution infrastructure lacks adequate protection. The difficulty of attribution in supply chain attacks enables adversaries to maintain a long-term presence while avoiding detection, extracting intelligence, and maintaining control capabilities for future activation.

3.3 (C) AI security

Artificial intelligence security in UAV systems encompasses the protection of machine learning models and autonomous decision-making processes from adversarial manipulation [83, 84]. The integration of AI capabilities transforms UAVs from remotely piloted vehicles into autonomous agents capable of complex environmental interpretation and independent action [23]. This autonomy introduces novel attack surfaces where adversaries exploit the probabilistic nature of machine learning to induce incorrect behaviors without traditional system compromise.

The opacity of deep learning models creates fundamental security challenges distinct from conventional software vulnerabilities. The inability to formally verify neural network behavior leaves systems vulnerable to carefully crafted inputs that exploit model blind spots [49]. The data-driven nature of modern AI systems means that security depends not only on algorithm implementation but also on training data integrity and model update processes. These characteristics require fundamentally different security approaches that account for the unique properties of learning-based systems.

3.3.1 *(C1) Perception attacks*

Perception attacks against UAV AI systems exploit the sensitivity of machine learning models to adversarial inputs specifically crafted to cause misclassification or detection failures. These attacks manipulate the mathematical properties of neural networks, where small perturbations to input data cause disproportionate changes in model output [52]. In the digital domain, attackers modify sensor data streams by injecting carefully calculated noise patterns that remain imperceptible to human observers but cause catastrophic failures in AI perception systems. Physical-world adversarial attacks present unique challenges for UAV security by manipulating the environment rather than the UAV itself. Adversarial patches and objects placed in the UAV's operational environment exploit model vulnerabilities through visual patterns designed to trigger specific misclassifications [51]. These attacks demonstrate particular effectiveness against object detection and navigation systems where misclassification of

obstacles or landmarks causes collision or navigation failures. The robustness challenges extend beyond simple accuracy metrics to encompass the entire perception pipeline from sensor input to decision output.

The transferability of adversarial examples between models amplifies the threat by enabling attacks without detailed knowledge of the target system. Adversarial patterns crafted against publicly available models often succeed against proprietary systems due to shared architectural features and training methodologies. This creates an asymmetric advantage for attackers who can develop and test exploits against surrogate models before deploying them against actual UAV systems. The challenge of defending against adversarial inputs without compromising legitimate functionality remains an open research problem with significant implications for autonomous UAV deployment.

3.3.2 *(C2) Decision manipulation*

Decision manipulation attacks target the higher-level reasoning and planning components of autonomous UAV systems, moving beyond perception to corrupt the actual decision-making process. These attacks exploit vulnerabilities in reinforcement learning algorithms and policy networks that govern UAV behavior [39]. By manipulating the reward signals or state representations that drive learning processes, attackers can gradually shift UAV behavior toward adversarial objectives while maintaining apparent normal operation.

Reward hacking represents a fundamental vulnerability in reinforcement learning systems where attackers exploit misaligned reward functions to induce unintended behaviors. Through careful manipulation of environmental feedback or direct interference with reward calculation, adversaries cause UAVs to optimize for malicious objectives disguised as legitimate goals. The temporal nature of these attacks makes detection particularly challenging as behavioral changes occur gradually over multiple interactions rather than through sudden system compromise.

State deception attacks corrupt the UAV's internal representation of its environment and operational context, leading to decisions based on false premises. By injecting misleading state information or manipulating state estimation processes, attackers trick autonomous systems into taking actions appropriate for fictitious scenarios rather than actual conditions. Model poisoning extends these attacks into the training phase, where compromised training data introduces backdoors and biases that activate under specific operational conditions. The challenge of securing the entire learning pipeline from data collection through model deployment requires comprehensive approaches that address both technical vulnerabilities and procedural weaknesses in AI system development.

3.3.3 *(C3) Training data poisoning*

Training data poisoning attacks compromise UAV AI systems by injecting malicious samples into training datasets, causing models to learn backdoors or biased behaviors that activate under specific trigger conditions [85, 86]. Unlike perception attacks that target inference-time inputs, poisoning attacks manipulate the learning process itself, embedding persistent vulnerabilities that survive model updates and defensive preprocessing.

Backdoor injection represents the most severe form of training poisoning, where adversaries introduce trigger patterns that cause misclassification only when specific inputs are present [86]. Research demonstrates that poisoning as few as 0.5%–1% of training samples can achieve >90% attack success rates while maintaining >95% accuracy on clean data [85]. For UAV applications, poisoned object detection models might fail to recognize obstacles marked with adversarial patterns, or navigation systems could be triggered to deviate from safe trajectories when encountering specific visual cues.

Label manipulation attacks corrupt the ground-truth annotations used during supervised learning, causing models to associate incorrect labels with legitimate inputs. In UAV contexts, this could manifest as misclassified landing zones, incorrectly identified friendly/hostile entities, or corrupted semantic segmentation maps. The difficulty of detecting poisoned labels, especially in large-scale datasets collected from distributed sources, makes this attack vector particularly concerning for collaborative UAV training pipelines [87].

The supply chain nature of modern AI development amplifies poisoning risks, as UAV manufacturers often rely on pre-trained models, public datasets, or third-party labeling services. Adversaries may target upstream data collection platforms, crowdsourced annotation systems, or model repositories to inject poisoned samples that propagate across multiple deployed systems. Defending against such attacks requires provenance tracking, statistical outlier detection, and Byzantine-resilient training algorithms that remain effective even when a fraction of training data is compromised [88].

3.3.4 *(C4) Model extraction and intellectual property theft*

Model extraction attacks enable adversaries to steal proprietary UAV AI models through black-box query access, undermining intellectual property protections and enabling subsequent adversarial attacks [89]. By systematically

querying a target model and observing its outputs, attackers can train surrogate models that approximate the original's decision boundaries with high fidelity. These extracted models facilitate transferable adversarial attacks and expose manufacturers' investments in custom model architectures and training procedures.

Query-based extraction exploits the API or inference interfaces exposed by UAV systems, where attackers submit carefully crafted inputs and record the corresponding predictions [89]. Research shows that high-fidelity extraction is achievable with queries numbering 10^3–10^5 samples, which is far fewer than the original training set size [90]. For UAVs, this vulnerability is particularly acute in fleet management scenarios where multiple drones share inference through cloud-based or edge-based services, providing adversaries with scalable query access.

Side-channel extraction leverages physical emanations or timing characteristics to infer model parameters without direct API access. Power consumption patterns, electromagnetic emissions, and cache timing have all been demonstrated as viable side channels for extracting neural network weights from embedded UAV processors [91,92]. The resource-constrained nature of UAV platforms, which often lack sophisticated side-channel protections found in data centers, makes them particularly susceptible to such attacks.

Protecting against model extraction requires multi-layered defenses, including query rate limiting, output perturbation that maintains utility while preventing accurate extraction, and watermarking techniques that enable ownership verification of extracted models [93]. However, these defenses must be carefully balanced against operational requirements, as excessive query restrictions could impair legitimate UAV operations in collaborative multi-agent scenarios.

4 Mitigation strategies and solutions

Current research addresses the security vulnerabilities of the low-altitude economy through comprehensive defense frameworks that integrate multiple protection layers.

As illustrated in Figure 4, defensive approaches converge on three coordinated strategies that address the primary attack vectors identified in modern UAV systems. Communication hardening implements cryptographic protocols and real-time anomaly detection mechanisms alongside hardware-based authentication to counter protocol exploits and man-in-the-middle attacks. Firmware and software integrity assurance utilizes blockchain verification technologies combined with cross-platform fuzzing and behavioral analysis to mitigate tampering risks and supply chain vulnerabilities. AI system resilience engineering applies adversarial training methodologies and model hardening techniques with input sanitization to defend against perception manipulation and decision-layer attacks.

The landscape of security implementations across major UAV platforms varies significantly [13, 28, 32, 54, 56, 68], as detailed in Table 5. The comparative analysis reveals that while commercial platforms offer integrated security features, they often lack transparency and community scrutiny. Conversely, open-source platforms provide full visibility but require manual implementation of security measures. This dichotomy underscores the need for standardized security frameworks that combine the robustness of commercial solutions with the transparency of open-source development.

Feasibility considerations, in Table 6, defense mechanisms exhibit significant trade-offs between security effectiveness and operational constraints. Lightweight cryptographic primitives (ChaCha20, PUF authentication) impose minimal overhead and are readily deployable on current UAV hardware. In contrast, blockchain-based firmware verification, while providing strong integrity guarantees, requires off-board computation and introduces verification latencies (100–500 ms) that may be incompatible with time-critical firmware updates during flight.

AI-based defenses present a different challenge on adversarial training and defensive distillation incur substantial computational costs during the training phase but minimal inference-time overhead. However, their effectiveness remains attack-specific, with models showing continued vulnerability to novel adversarial strategies not represented in training data. Real-world deployment must therefore combine multiple defense layers. For instance, pairing lightweight anomaly detection (LSTM-based, 5%–10% CPU overhead) with cryptographic authentication, which achieves defense-in-depth without exhausting UAV battery or processing budgets.

The analysis reveals that no single defense provides comprehensive protection. Blockchain verification excels at supply chain integrity but cannot prevent runtime exploitation; anomaly detection identifies behavioral deviations but may generate false positives during legitimate aggressive maneuvers; adversarial training hardens models against known attacks but offers limited generalization. Effective UAV security architectures must strategically compose these mechanisms based on mission profile, threat model, and platform capabilities.

These strategies share fundamental security principles that guide their implementation across diverse UAV platforms. The elimination of static credentials reduces the attack surface available to adversaries while hardware-rooted security provides tamper-resistant trust anchors. Adaptive runtime protection mechanisms enable a dynamic re-

Table 5 Comparison of security features in major UAV platforms. ✓= fully supported, ✗ = not supported, N/A = not applicable. [a] Hardware-dependent, requires compatible flight controller [56]. [b] Proposed in research but not standardized [54]. [c] Proprietary protocol, details undisclosed. [d] Requires MAVSec implementation [13]. [e] ChaCha20 recommended for resource-constrained devices [13]. [f] Unencrypted broadcast, privacy concerns identified [32]. [g] Third-party module integration required. [h] Research implementations available [68]. [i] Multiple security analyses published [13, 28]. [j] Responsible disclosure with delayed public release [32].

Security feature	DJI	PX4	ArduPilot	MAVLink protocol
Authentication mechanisms				
User authentication	Proprietary App	Optional	Optional	Not built-in
Device authentication	UAVID	Hardware ID	Hardware ID	System ID only
Mutual authentication	✗	✗	✗	✗
PUF-based authentication	✗	Supported[a]	Supported[a]	Extension[b]
Encryption capabilities				
Command encryption	Proprietary[c]	✗	✗	✗
Telemetry encryption	✗	✗	✗	✗
Video stream encryption	OcuSync 2.0	✗	✗	N/A
MAVSec support	✗	✓[d]	✓[d]	ChaCha20[e]
Firmware security				
Secure boot	✓	Optional	Optional	N/A
Firmware signing	✓	✓	✓	N/A
OTA updates	Encrypted	Plain	Plain	N/A
Rollback protection	✓	✗	✗	N/A
Access control				
Role-based access	✓	Basic	Basic	✗
Geofencing	Mandatory	Optional	Optional	Message type
No-fly zone updates	Automatic	Manual	Manual	N/A
Remote ID broadcast	UAVID[f]	Optional	Optional	Extension
Runtime protection				
Anomaly detection	Limited	✗	✗	✗
Anti-jamming	Frequency hop	✗	✗	✗
GPS spoofing detection	Basic	Module[g]	Module[g]	✗
Fail-safe mechanisms	✓	✓	✓	Message type
Audit & compliance				
Flight logging	Encrypted	Plain	Plain	Message Type
Tamper detection	✓	✗	✗	✗
Blockchain support	✗	Extension[h]	Extension[h]	✗
Forensic capabilities	Limited	Full	Full	Full
Development model				
Source availability	Closed	Open	Open	Open
Security audits	Internal	Community	Community	Academic[i]
Vulnerability disclosure	Controlled[j]	Public	Public	Public
Update frequency	Regular	Continuous	Continuous	Stable

Table 6 Feasibility analysis of defense mechanisms for resource-constrained UAV platforms.

Defense mechanism	Comp. cost	Memory	Latency	Deploy complex.	Effective.	Trade-offs
ChaCha20 encryption (α1)	Low (1%–2% CPU)	<50 kB	<2 ms	Low	High (95%+)	Minimal battery impact; key mgmt.
PUF authentication (α2)	Very low	<10 kB	<1 ms	Medium	High (99%+)	HW-dependent; not retrofittable
Blockchain firmware verif. (β1)	High (off-board)	2–5 MB	100–500 ms	High	Very high	Requires connectivity; delays
Fuzzing (β2)	N/A (pre-deploy)	N/A	N/A	High	Med-high	Development-phase only
LSTM anomaly detection (β3)	Med (5%–10% CPU)	500 kB–2 MB	5–15 ms	Medium	High (90%+)	False positives; labeled data
Adversarial training (γ)	Very high (training)	+20%–40% model	Minimal	High	Med (40%–60%)	Clean accuracy loss
Defensive distillation (γ)	High (training)	Same	Minimal	Medium	Med (50%–60%)	Accuracy loss; limited transfer

sponse to emerging threats without requiring system downtime or manual intervention. The integrated framework prioritizes resource-efficient security implementations that acknowledge the computational constraints of embedded systems while bridging pre-deployment verification with operational threat response capabilities.

4.1 (α) Communication hardening

Research into securing UAV communication channels addresses the fundamental vulnerabilities inherent in wireless transmission systems. The persistent weaknesses in established protocols such as MAVLink create exploitable

attack surfaces that adversaries actively target [13]. Man-in-the-middle attacks exploit these protocol deficiencies to intercept and modify communication streams between UAVs and control stations [53]. Network service exposure compounds these risks by providing additional attack vectors through inadequately secured interfaces [94]. The resource constraints characteristic of embedded UAV platforms create unique challenges for implementing robust security measures. Traditional network security solutions designed for enterprise environments prove unsuitable for direct implementation due to excessive computational overhead and memory requirements [55]. Real-time flight operations impose strict latency bounds that preclude the use of heavyweight cryptographic operations typically employed in ground-based systems. These constraints necessitate the development of purpose-built security solutions that balance protection effectiveness with operational requirements.

4.1.1 *(α1) Protocol security enhancement*

Protocol security enhancement efforts focus on addressing the fundamental cryptographic deficiencies present in legacy UAV communication systems. Early protocols transmitted sensitive operational data without encryption, enabling trivial eavesdropping attacks [54]. Authentication mechanisms relied on static credentials that, once compromised, provided permanent unauthorized access to UAV systems [56]. These vulnerabilities stemmed from design decisions that prioritized simplicity and performance over security, reflecting the limited threat awareness during initial protocol development. Modern protocol security research emphasizes lightweight cryptographic primitives specifically optimized for resource-constrained environments. Stream ciphers such as ChaCha20 provide encryption capabilities with reduced computational overhead compared to block ciphers like advanced encryption standard (AES) [13]. The MAVSec framework demonstrates the practical implementation of these lightweight primitives within existing protocol structures while maintaining compatibility with legacy systems. Performance evaluations indicate that ChaCha20 implementations achieve encryption throughput suitable for real-time video streaming while consuming minimal processor resources on embedded platforms. Specifically, ChaCha20 encryption adds only 0.8–1.2 ms latency per packet on ARM Cortex-M4 processors, well within the 50 ms control loop requirements for stable flight [13]. Hardware-accelerated implementations achieve throughput of 150–200 Mbps while consuming $<$5% CPU overhead, demonstrating feasibility for real-time video streaming applications [95].

Dynamic credential generation represents a paradigm shift from static authentication methods vulnerable to theft and replay attacks. Physically unclonable functions exploit manufacturing variations in semiconductor devices to generate unique, unclonable cryptographic keys [56]. Each UAV possesses a hardware-specific PUF response that serves as a digital fingerprint, enabling authentication without storing secret keys in vulnerable memory locations. Zero-Knowledge Proof protocols further enhance authentication security by proving identity without revealing the underlying secrets [54]. These cryptographic innovations eliminate entire classes of attacks that exploit stolen or intercepted credentials.

The integration of forward secrecy mechanisms ensures that the compromise of current session keys does not enable decryption of past communications. Ephemeral key exchange protocols generate unique encryption keys for each communication session, limiting the impact of any single key compromise [53]. Perfect forward secrecy implementations in UAV protocols require careful optimization to minimize the computational overhead of frequent key generation while maintaining cryptographic strength. Research demonstrates that optimized elliptic curve Diffie-Hellman implementations achieve acceptable performance on UAV processors while providing robust forward secrecy guarantees.

4.1.2 *(α2) Identity authentication*

Identity authentication in UAV systems extends beyond simple credential verification to encompass continuous validation of communication partners throughout operational sessions. Traditional authentication schemes suffer from fundamental limitations when applied to dynamic aerial environments [64]. Session hijacking attacks exploit the gap between initial authentication and subsequent communication, allowing adversaries to commandeer established connections [65]. Impersonation attacks leverage weaknesses in identity verification to masquerade as legitimate control stations or UAVs within swarm configurations [66].

Hardware-rooted authentication leverages tamper-resistant security elements to establish strong identity guarantees without relying on software-stored secrets. The SecAuthUAV framework exemplifies this approach by deriving authentication credentials from physical unclonable functions embedded within UAV hardware [68]. PUF-based authentication resists cloning attacks as the physical characteristics generating credentials cannot be replicated even with complete knowledge of the authentication protocol. Integration with secure elements provides protected storage for derived keys and cryptographic operations isolated from potentially compromised application processors.

Behavioral authentication introduces an additional security layer by continuously validating UAV identity through operational characteristics. The BEAM-UAV system models unique flight dynamics including acceleration patterns, control response characteristics, and power consumption profiles [69]. Machine learning algorithms analyze these behavioral signatures to detect anomalies indicative of unauthorized control or UAV substitution. This passive authentication operates transparently without additional communication overhead, providing defense-in-depth against sophisticated impersonation attempts.

Distributed ledger integration enhances authentication frameworks through immutable audit trails and decentralized trust management [67]. Blockchain-based authentication logs create tamper-evident records of all authentication events, enabling forensic analysis and regulatory compliance. Smart contracts automate credential lifecycle management including issuance, renewal, and revocation without centralized control points vulnerable to compromise. The distributed nature of blockchain systems ensures authentication service availability even when individual nodes fail or come under attack.

4.2 (β) Firmware & software integrity assurance

Firmware and software integrity assurance addresses the critical challenge of maintaining trustworthy code execution throughout the UAV operational lifecycle. The attack surface encompasses multiple threat vectors including direct code modification, supply chain infiltration, and runtime exploitation [70]. Resource constraints inherent in embedded systems preclude the deployment of traditional endpoint protection solutions, necessitating novel approaches tailored to UAV platforms [71]. The dynamic nature of modern threats requires adaptive protection mechanisms capable of detecting and responding to previously unknown attacks.

The complexity of modern UAV software stacks amplifies integrity challenges through extensive component interdependencies. Flight control systems integrate modules from multiple vendors, each potentially introducing vulnerabilities or backdoors [96]. The lack of comprehensive visibility into third-party component security postures creates blind spots that adversaries exploit. Supply chain attacks targeting upstream dependencies achieve widespread impact by compromising commonly used libraries or development tools integrated across multiple UAV platforms.

4.2.1 *(β1) Firmware verification*

Firmware verification establishes the foundation for trusted UAV operation by ensuring code authenticity and integrity from development through deployment. Traditional verification approaches rely on centralized certificate authorities vulnerable to compromise or coercion [72]. The global nature of UAV operations requires verification mechanisms that function across jurisdictional boundaries without depending on specific infrastructure availability. Decentralized verification paradigms address these limitations through cryptographic proofs validated by distributed consensus rather than central authority.

Blockchain-based firmware verification creates immutable audit trails documenting the entire firmware lifecycle from compilation through installation. The ChainVeri framework demonstrates practical implementation of blockchain verification for resource-constrained devices [72]. Firmware hashes recorded on distributed ledgers enable independent verification by any party without relying on manufacturer-provided checksums. Smart contracts enforce firmware update policies including multi-signature requirements for critical system components and automated rollback upon verification failure.

Hardware security modules provide tamper-resistant roots of trust for firmware verification processes. Trusted platform modules integrated into UAV hardware store cryptographic keys and perform attestation operations isolated from potentially compromised application processors [96]. Secure boot mechanisms leverage TPM capabilities to verify firmware signatures before execution, preventing unauthorized code from gaining control during system initialization. Runtime attestation extends verification beyond boot time by periodically validating firmware integrity throughout operational sessions.

Machine learning approaches to firmware verification detect anomalous execution patterns indicative of code modification or injection. Behavioral analysis systems model normal firmware operation through metrics including function call sequences, memory access patterns, and timing characteristics [71]. Deviations from established baselines trigger alerts enabling rapid response to zero-day exploits or sophisticated tampering attempts. The integration of hardware performance counters provides low-overhead monitoring capabilities suitable for continuous operation on resource-constrained platforms [70].

4.2.2 *(β2) Vulnerability detection*

Proactive vulnerability identification prevents exploitation by discovering and remediating security flaws before adversaries can leverage them. The scale and complexity of modern UAV firmware necessitate automated analysis techniques capable of processing millions of lines of code [97]. Static analysis alone proves insufficient due to the prevalence of runtime-dependent vulnerabilities that manifest only under specific operational conditions. Dynamic analysis complements static techniques but faces challenges in achieving comprehensive coverage of all execution paths.

Binary analysis techniques address the reality that source code remains unavailable for many UAV components due to proprietary restrictions or supply chain complexity. The VulHawk system pioneers architecture-agnostic vulnerability detection through intermediate representation analysis [79]. By translating diverse binary formats into normalized representations, VulHawk enables cross-platform vulnerability correlation and pattern matching. Experimental results demonstrate the detection of known vulnerability classes across ARM, MIPS, and x86 firmware with minimal false positives.

Fuzzing techniques systematically explore program behavior by generating inputs designed to trigger crashes or unexpected behavior indicative of exploitable vulnerabilities. Coverage-guided fuzzing maximizes code exploration efficiency by prioritizing inputs that exercise previously untested execution paths [98]. The AFL++ framework extends traditional fuzzing with UAV-specific optimizations including protocol-aware input generation and real-time constraint handling [99]. Integration with hardware-in-the-loop testing enables fuzzing of complete UAV systems including interactions between firmware components and physical sensors.

Specialized fuzzing frameworks address unique challenges in UAV firmware testing including diverse input channels and real-time processing requirements. Research identifies key adaptations required for effective UAV fuzzing including multi-channel input coordination for systems accepting commands via UART, SPI, and network interfaces simultaneously [78]. Time-sensitive bug detection requires fuzzing harnesses that maintain realistic timing relationships between inputs [76]. The HiFuzz framework specifically targets human-UAV interaction vulnerabilities by fuzzing gesture recognition and voice command processing subsystems [73].

4.2.3 *(β3) Dynamic anomaly detection*

Dynamic anomaly detection provides runtime protection against zero-day exploits and sophisticated attacks that evade static defenses. The approach leverages machine learning to model normal system behavior and identify deviations potentially indicating compromise [57]. Unlike signature-based detection limited to known threats, anomaly detection can identify novel attacks based on their behavioral impact rather than specific implementation details [58]. The challenge lies in achieving sufficient sensitivity to detect subtle attacks while minimizing false positives that could disrupt legitimate operations.

Unsupervised learning algorithms prove particularly valuable for UAV anomaly detection due to the scarcity of labeled attack data in operational environments. Isolation Forest algorithms efficiently identify outliers in high-dimensional sensor data streams without requiring prior knowledge of attack patterns [62]. The algorithm's tree-based structure enables real-time processing suitable for onboard implementation with minimal memory overhead. Adaptive threshold mechanisms adjust detection sensitivity based on operational context, reducing false alarms during legitimate but unusual maneuvers. Experimental deployments show that Isolation Forest implementations achieve 91%–94% detection accuracy for UAV hijacking scenarios with false positive rates below 2% [62]. LSTM-based temporal anomaly detectors demonstrate 88%–93% precision in identifying command injection attempts while maintaining inference latency under 10 ms on embedded platforms [63], making them suitable for real-time onboard deployment.

Temporal modeling captures the sequential nature of UAV operations where current behavior depends on historical context. Long short-term memory networks excel at learning complex temporal dependencies in flight telemetry data [63]. LSTM-based detectors identify subtle anomalies in control sequences that might indicate hijacking attempts or sensor manipulation. The recurrent architecture naturally handles variable-length input sequences corresponding to missions of different durations without preprocessing requirements.

Semi-supervised approaches bridge the gap between fully unsupervised methods and supervised learning by incorporating limited labeled data when available [60]. One-class classification algorithms train on normal behavior examples to establish decision boundaries separating legitimate from anomalous operations. The incorporation of expert knowledge through feature engineering improves detection accuracy for specific attack types while maintaining generalization to unknown threats [61]. Ensemble methods combining multiple detection algorithms achieve robust performance across diverse attack scenarios by leveraging complementary strengths of different approaches.

4.3 (γ) AI system resilience engineering

AI system resilience engineering addresses vulnerabilities in machine learning components that enable adversarial manipulation of UAV perception and decision-making capabilities. The integration of deep learning models for tasks including obstacle detection, path planning, and target recognition creates novel attack surfaces absent in traditional rule-based systems [51]. Adversarial examples crafted to exploit model weaknesses can cause catastrophic failures in safety-critical operations without triggering conventional security alerts [100]. Resilience engineering develops defensive techniques that maintain model performance under adversarial conditions while preserving legitimate functionality.

The fundamental challenge in AI resilience stems from the inherent trade-off between model expressiveness and robustness. Models capable of handling complex real-world scenarios exhibit increased susceptibility to adversarial perturbations [23]. Defensive techniques must balance protection against adversarial inputs with maintaining accuracy on benign data. The computational constraints of embedded UAV platforms further complicate defense implementation by limiting the complexity of protection mechanisms that can be deployed in real-time operational contexts.

Adversarial training represents the primary defense paradigm for hardening models against malicious inputs. The technique augments training datasets with adversarially generated examples designed to exploit model weaknesses [101]. Models trained on these augmented datasets learn robust features less susceptible to adversarial manipulation. However, the computational cost of generating adversarial examples during training increases resource requirements significantly. Quantitative studies show that adversarial training increases model robustness by 40%–60% against PGD attacks while incurring 15%–25% additional training time [23, 101]. The effectiveness varies across attack types, with models exhibiting continued vulnerability to novel attack strategies not represented in training data.

For defensive distillation, empirical results demonstrate that this approach reduces attack success rates from 85%–90% (undefended models) to 30%–45% with temperature scaling factors of 10%–20 [102]. However, this robustness improvement comes at the cost of 2%–4% degradation in clean accuracy on benign inputs [103]. Implementation requires careful tuning to balance robustness gains against accuracy degradation on legitimate inputs.

Input preprocessing and detection mechanisms provide complementary protection by identifying and filtering adversarial inputs before they reach vulnerable models. Statistical analysis of input characteristics can reveal anomalies indicative of adversarial crafting [51]. Ensemble methods combining multiple models with diverse architectures reduce vulnerability to attacks targeting specific model weaknesses [100]. The integration of formal verification techniques for critical decision paths provides provable guarantees against certain attack classes, though computational limitations restrict verification to simplified model components.

5 Future directions and challenges

Building on the state-of-the-art review, this section synthesises future research direction, future policy focus, and open challenges that will shape the security posture of the low-altitude economy over the next decade.

5.1 Open challenges

Despite rapid progress in drone autonomy, AI security, and communication resilience, the broader ecosystem of the low-altitude economy continues to face unresolved challenges. These issues cut across technical, legal, and societal domains, and their resolution will be essential for safe, scalable, and globally interoperable deployment over the next decade.

(i) Privacy-preserving data governance. As drones become pervasive across commercial and public domains, their passive data collection capabilities raise significant privacy concerns. High-resolution sensors, GPS telemetry, and cloud-connected analytics systems can capture sensitive information, from residential layouts and behavioral patterns to industrial infrastructure details. Attackers may exploit these data streams through interception, aggregation, or unauthorized inference [43, 104]. Existing frameworks like GDPR (General Data Protection Regulation) and CCPA (California Consumer Privacy Act) remain reactive and ill-suited for managing decentralized, continuously streamed data. Future efforts must focus on privacy-by-design approaches: on-device federated learning [105], synthetic data generation for AI model training without identity leakage [106], and zero-trust, end-to-end encrypted communication protocols [107].

(ii) Trust and explainability in autonomous decision-making. As AI agents increasingly drive flight decisions [10], including obstacle avoidance, route optimization, and target identification, ensuring human trust in these decisions becomes crucial. Many AI modules, especially deep learning-based ones, operate as black boxes with

little transparency into why a specific action was taken. In high-stakes scenarios like urban navigation or emergency response, a lack of interpretability limits accountability and regulatory acceptance. Developing explainable AI (XAI) tailored for resource-constrained aerial systems, alongside verifiable decision logs and human-on-the-loop override mechanisms, remains an urgent research priority.

(iii) Fragmented infrastructure and spectrum coordination. The low-altitude space is becoming increasingly congested, with a mix of recreational, commercial, and emergency UAVs operating across overlapping airspace. This congestion is worsened by the lack of unified infrastructure for spectrum allocation, real-time air traffic coordination, and inter-platform communication. Ad hoc communication protocols and inconsistent ground station integration increase the risk of interference, collision, and systemic failure. Solving this challenge will require cooperative infrastructure planning, standardization of UAV-specific wireless protocols, and investment in intelligent airspace management systems, which is possibly backed by AI-enhanced software-defined networking.

5.2 Future research directions

(i) AI-enabled, resource-aware defense. The increasing integration of AI into the system of low-altitude economy, ranging from computer vision and voice recognition to real-time path planning, has unlocked new operational capabilities but simultaneously introduced an expanded attack surface. Traditional adversarial research has largely concentrated on visual perturbations targeting object detection and navigation systems [108, 109]. However, as drones begin to rely on a broader suite of AI modules, including audio, multimodal sensor fusion, and context-aware route optimization, the scope and complexity of potential threats multiply.

Future research must go beyond isolated adversarial scenarios and focus on holistic, resource-aware AI defense architectures. These should be capable of adapting to diverse operational environments while accounting for the constraints typical of edge-deployed systems. Specifically, the following directions are critical. (1) Cross-domain adversarial robustness. As drones adopt multimodal AI pipelines (e.g., simultaneous use of vision and voice interfaces), unified defense frameworks are essential. These must protect against attacks exploiting interdependencies across data modalities, such as audio-visual or vision-planning interferences, ensuring that perturbations in one domain do not propagate failures in another. (2) Edge-AI-driven defense mechanisms. Real-time defense requires moving AI threat detection and response closer to the edge. Edge-optimized adversarial training pipelines, including those leveraging federated learning, allow distributed UAV swarms to collaboratively improve threat models without relying on latency-prone cloud infrastructure. These systems should support sparse model updates, bandwidth-efficient aggregation, and resilience to malicious nodes through Byzantine-robust protocols. (3) Energy-aware threat mitigation. AI defenses must not only be effective but also energy-efficient, particularly on battery-limited aerial platforms. Future work should explore lightweight defense algorithms that intelligently schedule defensive operations based on mission-criticality, threat probability, and system load.

(ii) Quantum-resilient, crypto-agile communications. This risk is particularly pressing for the low-altitude economy, where UAVs are increasingly responsible for critical tasks such as coordinated swarm operations, logistics delivery, and emergency response. These applications demand secure, real-time communication with strong guarantees of confidentiality, integrity, and authentication. Yet, many existing UAS protocols (e.g., MAVLink) suffer from weak or absent encryption, unauthenticated telemetry, and limited resistance to spoofing or command injection. In a future where quantum attacks are feasible, such vulnerabilities could be catastrophic.

To safeguard the integrity of low-altitude infrastructure, quantum-resilient and crypto-agile communication systems must become a key research priority [110–112]. This includes not only cryptographic algorithm development but also systemic innovations in protocol design, deployment strategies, and operational robustness. (1) Post-quantum cryptography (PQC) adoption. Emphasis should be placed on lattice-based key encapsulation mechanisms (e.g., RLWE-KEM) and hash-based digital signatures (e.g., SPHINCS+) that offer quantum resistance while remaining efficient for bandwidth- and power-constrained UAV platforms. (2) Crypto-agility at the system level. Future UAS must support seamless algorithm and key updates to remain secure as standards evolve. Agile cryptographic stacks will allow dynamic adaptation to threat environments without compromising operational continuity. (3) Secure SDN integration. Software-defined networking (SDN) holds promise for dynamic airspace management and adaptive trust zoning. Embedding quantum-safe primitives into both data plane and control channel communications is essential for maintaining trust in decentralized aerial networks. (4) Side-channel resilience. Quantum safety cannot rely solely on algorithmic strength. UAV hardware must integrate lightweight countermeasures against side-channel attacks, including constant-time execution and masking, especially given the physical accessibility of drone systems. (5) Standardization and real-world validation. Research should drive the development of testbeds and threat modeling frameworks tailored to low-altitude environments, ensuring that post-quantum protocols are practically deployable, secure, and performant in real flight conditions.

(iii) Cross-domain lessons and standardized benchmarking. The low-altitude economy can benefit significantly from security innovations in adjacent domains, particularly automotive cybersecurity and IoT device security. The automotive industry's adoption of hardware security modules (HSMs) for secure key storage and the AUTOSAR security architecture provides proven templates for resource-constrained, safety-critical embedded systems [113]. Similarly, IoT security frameworks such as ARM TrustZone and IETF's SUIT manifest specification offer lessons in secure firmware update and attestation that are directly applicable to UAV platforms [114, 115].

However, meaningful progress requires a standardized benchmarking infrastructure currently absent in UAV security research. Existing datasets and testbeds remain fragmented and domain-specific: adversarial robustness is often evaluated on static image datasets (ImageNet, COCO) rather than real-time UAV video streams; protocol security assessments use simulated environments that fail to capture RF propagation complexities and interference patterns encountered in operational airspace; and anomaly detection research lacks publicly available flight telemetry datasets capturing diverse attack scenarios across multiple UAV platforms.

We advocate for community-driven initiatives to establish open UAV security datasets containing labeled collections of attack and benign traffic for communication protocols (MAVLink, DJI protocols), flight telemetry data with injected anomalies, and adversarial examples targeting real UAV perception systems. Equally important are hardware-in-the-loop (HIL) testbeds that provide publicly accessible platforms enabling researchers to evaluate defenses against real UAVs with standardized attack scenarios, eliminating reproducibility issues inherent in simulation-only studies. Finally, the community needs security metrics standardization that encompasses not only detection accuracy but also false positive rates under operational stress, defense overhead on representative UAV hardware (Pixhawk, Jetson), and resilience to adaptive adversaries. Such infrastructure would enable rigorous comparison of defense mechanisms and accelerate translation of academic research into deployed systems.

(iv) Interdisciplinary collaboration requirements. Securing the low-altitude economy demands expertise spanning AI/ML security, wireless communications, control theory, and aviation safety, which are domains that traditionally operate in silos. Effective defenses must simultaneously satisfy AI security requirements including robustness against adversarial perturbations and data poisoning; communication security needs such as authentication, encryption, and anti-jamming under bandwidth and latency constraints; control system safety guarantees ensuring stability even when sensors or communication channels are compromised; and regulatory compliance mandating adherence to airworthiness standards (RTCA DO-178C for software, DO-326A for security) and privacy regulations (GDPR, CCPA).

Current research often optimizes for one dimension while neglecting others. For example, adversarial training improves robustness but may increase inference latency beyond flight control tolerances, while cryptographic protocols enhance communication security but complicate real-time controller verification. Future work should prioritize co-design methodologies that jointly optimize security, safety, and performance. These include control-aware adversarial training that constrains perturbations to maintain closed-loop stability, cross-layer security architectures integrating physical-layer anti-jamming with protocol-layer authentication and application-layer anomaly detection, and formal verification frameworks bridging AI model assurance with control system certification requirements [116, 117].

Achieving such integration requires institutional changes beyond technical innovation. Funding mechanisms must encourage collaboration between computer science, aerospace engineering, and regulatory bodies rather than reinforcing disciplinary boundaries. Academic programs should train engineers in both cybersecurity and unmanned systems, developing professionals fluent in the languages of both domains. Industry consortia similar to automotive AUTOSAR or aviation RTCA should establish shared security requirements and reference implementations for LAE platforms, enabling interoperability and raising the security baseline across manufacturers. Only through such systematic interdisciplinary coordination can the low-altitude economy achieve the integrated, resilient security posture necessary for safe and trustworthy deployment at scale.

5.3 Future policy focus

The rapid expansion of the low-altitude economy demands a forward-looking regulatory vision that treats cybersecurity not as a static compliance issue, but as a continuously evolving operational requirement. As drone systems become more autonomous, interconnected, and AI-driven, policy frameworks are increasingly shaping how software is developed, deployed, and defended [118].

Recent regulatory developments demonstrate this shift toward proactive, security-by-design mandates. For instance, China's Shenzhen SILAS platform requires manufacturers to embed real-time vulnerability disclosure mechanisms directly into drone firmware, while the EU's SORA framework mandates dynamic threat modeling for all urban air mobility operations [119]. These policies promote alignment between threat intelligence and the software development lifecycle, enabling adaptive security postures.

However, regulatory fragmentation remains a major barrier to secure global drone operations. Disparate frameworks, such as the FAA's UTM guidelines in the United States [120] and ICAO's global airspace recommendations [121] which often adopt incompatible approaches to secure telemetry, authentication protocols, and airspace integration. This divergence imposes operational and compliance overhead on manufacturers and service providers aiming for cross-border interoperability.

To address these gaps and support the secure scaling of low-altitude operations, future policy initiatives should emphasize the following. (1) Standards harmonization and interoperability. Promote convergence between regional policies via multilateral frameworks (e.g., ICAO, ISO), enabling consistent security expectations across jurisdictions. (2) Policy sandboxes for emerging security technologies. Establish safe regulatory test zones to trial innovative architectures, such as quantum-resistant encryption schemes or AI-based behavioral anomaly detection, under real-world constraints. (3) Incentives for secure toolchains. Governments can play a role in promoting open source, security-vetted software libraries for cryptographic operations, adversarial testing, and continuous firmware assurance, lowering barriers to secure deployment at scale.

6 Conclusion

Software security for LAE demands integrated defenses across communication, firmware, and AI layers, engineered with 5G/5.5G connectivity and edge capabilities, aligned with evolving standards and policy. Our revised taxonomy, standards mapping, and feasibility analysis aim to guide researchers, practitioners, and regulators toward resilient, certifiable, and resource-aware protection of UAV/UAM systems.

Open Access funding enabled and organized by CAUL and its Member Institutions.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

References

1 Siripurapu S, Darimireddy N K, Chehri A, et al. Technological advancements and elucidation gadgets for healthcare applications: an exhaustive methodological review-Part-I (AI, Big Data, Block Chain, Open-Source Technologies, and Cloud Computing). Electronics, 2023, 12: 750
2 Laghari A A, Jumani A K, Laghari R A, et al. Unmanned aerial vehicles: a review. Cogn Robotics, 2023, 3: 8–22
3 Hayat S, Yanmaz E, Muzaffar R. Survey on unmanned aerial vehicle networks for civil applications: a communications viewpoint. IEEE Commun Surv Tutorials, 2016, 18: 2624–2661
4 Rejeb A, Rejeb K, Simske S J, et al. Drones for supply chain management and logistics: a review and research agenda. Int J Logistics Res Appl, 2023, 26: 708–731
5 Jin Y. The evolution and challenges of low-altitude economy: insights from experience in China. In: Proceedings of the 1st International Conference on Modern Logistics and Supply Chain Management (MLSCM 2024), 2024. 32–36
6 Routray S K, Singh M, Samal L, et al. 5G advanced: a step towards 6G. In: Proceedings of 2024 IEEE International Conference on Communication, Computing and Signal Processing (IICCCS), 2024. 1–5
7 Porres I, Azimi S, Lafond S, et al. On the verification and validation of AI navigation algorithms. In: Proceedings of Global Oceans 2020, 2020. 1–8
8 Liu Y, Chen C, Wang Y, et al. A fast formation obstacle avoidance algorithm for clustered UAVs based on artificial potential field. Aerospace Sci Tech, 2024, 147: 108974
9 Bhanu B. Automatic target recognition: state of the art survey. IEEE Trans Aerosp Electron Syst, 1986, AES-22: 364–379
10 Deng Z, Guo Y, Han C, et al. AI agents under threat: a survey of key security challenges and future pathways. ACM Comput Surv, 2025, 57: 1–36
11 Zhou W, Zhu X, Han Q L, et al. The security of using large language models: a survey with emphasis on ChatGPT. IEEE CAA J Autom Sin, 2025, 12: 1–26
12 Joksimovic A, Lourenco-Feio A M, Gavrilovic N. Integrated preliminary sizing environment for hydrogen-powered drones. In: Proceedings of AIAA SCITECH 2025 Forum, 2025. 1246
13 Allouch A, Cheikhrouhou O, Koubâa A, et al. Mavsec: securing the MAVLink protocol for ArduPilot/px4 unmanned aerial systems. In: Proceedings of 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC), 2019. 621–628
14 Zhu X, Wen S, Camtepe S, et al. Fuzzing: a survey for roadmap. ACM Comput Surv, 2022, 54: 1–36
15 Zhu X, Zhou W, Han Q L, et al. When software security meets large language models: a survey. IEEE CAA J Autom Sin, 2025, 12: 317–334
16 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 Netws, 2022, 133: 102894
17 Feng X, Zhu X, Han Q L, et al. Detecting vulnerability on IoT device firmware: a survey. IEEE CAA J Autom Sin, 2022, 10: 25–41

18 Duan X Y, Zhang X Q, Xia S Q, et al. Machine learning empowered UAV-based beamforming design in ISAC systems. Sci China Inf Sci, 2025, 68: 150307
19 Deng Z, Ma W, Han Q L, et al. Exploring DeepSeek: a survey on advances, applications, challenges and future directions. IEEE CAA J Autom Sin, 2025, 12: 872–893
20 Lu Z, Sun H, Xu Y. Adversarial robustness enhancement of UAV-oriented automatic image recognition based on deep ensemble models. Remote Sens, 2023, 15: 3007
21 Shachtman N. Computer virus hits U.S. drone fleet. CNN, 2011. https://edition.cnn.com/2011/10/10/tech/innovation/virus-hits-drone-fleet-wired
22 Pleban J S, Band R, Creutzburg R. Hacking and securing the AR.Drone 2.0 quadcopter: investigations for improving the security of a toy. In: Proceedings of Mobile Devices and Multimedia: Enabling Technologies, Algorithms, and Applications 2014, 2014. 168–179
23 Tian J, Wang B, Guo R, et al. Adversarial attacks and defenses for deep-learning-based unmanned aerial vehicles. IEEE Internet Things J, 2021, 9: 22399–22409
24 Pacheco D A J, Sarker S, Bilal M, et al. Opportunities and challenges of drones and the Internet of Drones in healthcare supply chains under disruption. Production PlAnning Control, 2025, 36: 2009–2031
25 Pandey G K, Gurjar D S, Nguyen H H, et al. Security threats and mitigation techniques in UAV communications: a comprehensive survey. IEEE Access, 2022, 10: 112858
26 Sharma J, Mehra P S. Secure communication in IOT-based UAV networks: a systematic survey. Internet Things, 2023, 23: 100883
27 Fotouhi A, Qiang H, Ding M, et al. Survey on UAV cellular communications: practical aspects, standardization advancements, regulation, and security challenges. IEEE Commun Surv Tutorials, 2019, 21: 3417–3442
28 Kumar N, Chaudhary A. Surveying cybersecurity vulnerabilities and countermeasures for enhancing UAV security. Comput Netws, 2024, 252: 110695
29 Tlili F, Ayed S, Fourati L C. Advancing UAV security with artificial intelligence: a comprehensive survey of techniques and future directions. Internet Things, 2024, 27: 101281
30 Samland F, Fruth J, Hildebrandt M, et al. Ar.Drone: security threat analysis and exemplary attack to track persons. In: Proceedings of SPIE, 2012. 8301: 158–172
31 Highnam K, Angstadt K, Leach K, et al. An uncrewed aerial vehicle attack scenario and trustworthy repair architecture. In: Proceedings of 2016 46th annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshop (DSN-W), 2016. 222–225
32 Schiller N, Chlosta M, Schloegel M, et al. Drone security and the mysterious case of DJI's droneid. In: Proceedings of NDSS, 2023
33 Choi J, Son S, Kwon D, et al. A PUF-based secure authentication and key agreement scheme for the internet of drones. Sensors, 2025, 25: 982
34 Aposporis P. A review of global and regional frameworks for the integration of an unmanned aircraft system in air traffic management. Transp Res Interdisciplinary Perspect, 2024, 24: 101064
35 Zhu A, Pauwels P, Torta E, et al. Data linking and interaction between BIM and robotic operating system (ROS) for flexible construction planning. Automation Construction, 2024, 163: 105426
36 Doornbos J, Bennin K E, Babur Ö, et al. Drone technologies: a tertiary systematic literature review on a decade of improvements. IEEE Access, 2024, 12: 23220–23239
37 IEEE. IEEE STD 1588-2008: IEEE standard for a precision clock synchronization protocol for networked measurement and control systems. Technical Report, Institute of Electrical and Electronics Engineers, 2008
38 NVIDIA. Jetson Benchmarks. NVIDIA Developer. https://developer.nvidia.com/embedded/jetson-benchmarks. 2025
39 Wang X, Gursoy M C. Resilient path planning for UAVs in data collection under adversarial attacks. IEEE TransInformForensic Secur, 2023, 18: 2766–2779
40 He D, Chan S, Guizani M. Communication security of unmanned aerial vehicles. IEEE Wireless Commun, 2016, 24: 134–139
41 Abro G, Zulkifli S, Masood R, et al. Comprehensive review of UAV detection, security, and communication advancements to prevent threats. Drones, 2022, 6: 284
42 Wang L, Chen Y, Wang P, et al. Security threats and countermeasures of unmanned aerial vehicle communications. IEEE Comm Stand Mag, 2021, 5: 41–47
43 Zhi Y, Fu Z, Sun X, et al. Security and privacy issues of UAV: a survey. Mobile Netw Appl, 2020, 25: 95–101
44 Dey V, Pudi V, Chattopadhyay A, et al. Security vulnerabilities of unmanned aerial vehicles and countermeasures: an experimental study. In: Proceedings of 2018 31st International Conference on VLSI Design and 2018 17th International Conference on Embedded Systems (VLSID), 2018. 398–403
45 Hooper M, Tian Y, Zhou R, et al. Securing commercial Wi-Fi-based UAVs from common security attacks. In: Proceedings of IEEE Military Communications Conference, 2016. 1213–1218
46 Petrovsky O, Prague V. Attack on the drones. In: Proceedings of the Virus Bulletin Conference, Prague, 2015. 16
47 Kim T, Ding A, Etigowni S, et al. Reverse engineering and retrofitting robotic aerial vehicle control firmware using dispatch. In: Proceedings of the 20th Annual International Conference on Mobile Systems, Applications and Services, 2022. 69–83
48 Lakew Yihunie F, Singh A K, Bhatia S. Assessing and exploiting security vulnerabilities of unmanned aerial vehicles. In: Proceedings of Smart Systems and IoT: Innovations in Computing, 2020. 701–710
49 Fu C, Li S, Yuan X, et al. Ad2attack: adaptive adversarial attack on real-time uav tracking. In: Proceedings of 2022 International Conference on Robotics and Automation (ICRA), 2022. 5893–5899
50 Lee P, Su V, Chen P. The drone supply chain's grand siege: from initial breaches to long-term espionage on high-value targets. In: Proceedings of Black Hat Asia 2025 Briefings, 2025
51 Raja A, Njilla L, Yuan J. Adversarial attacks and defenses toward AI-assisted UAV infrastructure inspection. IEEE Internet Things J, 2022, 9: 23379–23389
52 Shrestha S, Pathak S, Viegas E K. Towards a robust adversarial patch attack against unmanned aerial vehicles object detection. In: Proceedings of 2023 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), 2023. 3256–3263
53 Salam W, Raazi S K U R, Ansari N H. Seltha: secure, efficient and lightweight authentication mechanism for unmanned aerial vehicle network. In: Proceedings of 2023 7th International Multi-Topic ICT Conference (IMTIC), 2023. 1–7

54 Chen L, Zhu Y, Liu S, et al. PUF-based dynamic secret-key strategy with hierarchical blockchain for UAV swarm authentication. Comput Commun, 2024, 218: 31–43
55 Sen M A, Al-Rubaye S, Tsourdos A. Developing secure hardware for UAV authorisation using lightweight authentication. In: Proceedings of 2023 IEEE/AIAA 42nd Digital Avionics Systems Conference (DASC), 2023. 1–9
56 Elhence A, Chamola V. HardSecUAV: a hardware-based mutual authentication protocol for network of drones. Comput Electrical Eng, 2025, 123: 110286
57 Bell V, Rengasamy D, Rothwell B, et al. Anomaly detection for unmanned aerial vehicle sensor data using a stacked recurrent autoencoder method with dynamic thresholding. 2022. ArXiv:2203.04734
58 Yang L, Li S, Zhang Y, et al. Deep learning-assisted unmanned aerial vehicle flight data anomaly detection: a review. IEEE Sens J, 2024, 24: 31681–31695
59 He Y, Peng Y, Wang S, et al. ADMOST: UAV flight data anomaly detection and mitigation via online subspace tracking. IEEE Trans Instrum Meas, 2018, 68: 1035–1044
60 Pan D, Nie L, Kang W, et al. Uav anomaly detection using active learning and improved S3VM model. In: Proceedings of 2020 International Conference on Sensing, Measurement & Data Analytics in the era of Artificial Intelligence (ICSMD), 2020. 253–258
61 Keipour A, Mousaei M, Scherer S. ALFA: a dataset for UAV fault and anomaly detection. Int J Robotics Res, 2021, 40: 515–520
62 Khan S, Liew C F, Yairi T, et al. Unsupervised anomaly detection in unmanned aerial vehicles. Appl Soft Computing, 2019, 83: 105650
63 Zhong J, Zhang Y, Wang J, et al. Unmanned aerial vehicle flight data anomaly detection and recovery prediction based on spatio-temporal correlation. IEEE Trans Rel, 2021, 71: 457–468
64 Rodrigues M, Amaro J, Osório F S, et al. Authentication methods for UAV communication. In: Proceedings of 2019 IEEE Symposium on Computers and Communications (ISCC), 2019. 1210–1215
65 Teng L, Jianfeng M, Pengbin F, et al. Lightweight security authentication mechanism towards UAV networks. In: Proceedings of 2019 International Conference on Networking and Network Applications (NaNA), 2019. 379–384
66 Xia T, He J, Lakshmanna K. An identity authentication scheme based on SM2 algorithm in UAV communication network. Wireless Commun Mobile Computing, 2022, 2022: 7537764
67 de Melo C F E, e Silva T D, Boeira F, et al. UAVouch: a secure identity and location validation scheme for UAV-networks. IEEE Access, 2021, 9: 82930–82946
68 Alladi T, Naren T, Bansal G, et al. SecAuthUAV: a novel authentication scheme for UAV-ground station and UAV-UAV communication. IEEE Trans Veh Technol, 2020, 69: 15068–15077
69 Jiang C, Fang Y, Zhao P, et al. Intelligent UAV identity authentication and safety supervision based on behavior modeling and prediction. IEEE Trans Ind Inf, 2020, 16: 6652–6662
70 Lee B, Lee J H. Blockchain-based secure firmware update for embedded devices in an Internet of Things environment. J Supercomput, 2017, 73: 1152–1167
71 Wang X, Konstantinou C, Maniatakos M, et al. Confirm: detecting firmware modifications in embedded systems using hardware performance counters. In: Proceedings of 2015 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), 2015. 544–551
72 Lim J M, Kim Y, Yoo C. Chain veri: blockchain-based firmware verification system for IoT environment. In: Proceedings of 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2018. 1050–1056
73 Chambers T, Vierhauser M, Agrawal A, et al. Hifuzz: human interaction fuzzing for small unmanned aerial vehicles. In: Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems, 2024. 1–14
74 Malviya V K, Minn W, Shar L K, et al. Fuzzing drones for anomaly detection: a systematic literature review. Comput Security, 2025, 148: 104157
75 Chang Z, Zhang H, Jia Y, et al. Low-cost fuzzing drone control system for configuration errors threatening flight safety in edge terminals. Comput Commun, 2024, 220: 138–148
76 Alrabaee S, Debbabi M, Wang L. A survey of binary code fingerprinting approaches: taxonomy, methodologies, and features. ACM Comput Surv, 2022, 55: 1–41
77 Zhao D, Lin H, Ran L, et al. CVSkSA: cross-architecture vulnerability search in firmware based on kNN-SVM and attributed control flow graph. Software Qual J, 2019, 27: 1045–1068
78 Kim Y, Cho K, Kim S. Challenges in drone firmware analyses of drone firmware and its solutions. 2024. ArXiv:2312.16818
79 Luo Z, Wang P, Wang B, et al. Vulhawk: cross-architecture vulnerability detection with entropy-based binary code search. In: Proceedings of NDSS, 2023
80 Wang C-X, Lv Z, Huang C, et al. An enhanced 6G pervasive channel model towards standardization. Sci China Inf Sci, 2025, 68: 162301
81 Cui Q M, You X H, Wei N, et al. Overview of AI and communication for 6G network: fundamentals, challenges, and future research opportunities. Sci China Inf Sci, 2025, 68: 171301
82 Sheng C, Zhou W, Han Q L, et al. Network traffic fingerprinting for IIoT device identification: a survey. IEEE Trans Ind Inf, 2025, 21: 3541–3554
83 He X L, Xu G W, Han X S, et al. Artificial intelligence security and privacy: a survey. Sci China Inf Sci, 2025, 68: 181101
84 Yang Z H, Xu W, Liang L, et al. On privacy, security, and trustworthiness in distributed wireless large AI models. Sci China Inf Sci, 2025, 68: 170301
85 Chen F, Ding X, Feng Y, et al. Targeted activation of diverse CRISPR-Cas systems for mammalian genome editing via proximal CRISPR targeting. Nat Commun, 2017, 8: 14958
86 Gu T, Dolan-Gavitt B, Garg S. Badnets: identifying vulnerabilities in the machine learning model supply chain. 2017. ArXiv:1708.06733
87 Biggio B, Nelson B, Laskov P. Poisoning attacks against support vector machines. 2012. ArXiv:1206.6389
88 Blanchard P, El Mhamdi E M, Guerraoui R, et al. Machine learning with adversaries: Byzantine tolerant gradient descent. In: Proceedings of Advances in Neural Information Processing Systems, 2017. 30
89 Tramèr F, Zhang F, Juels A, et al. Stealing machine learning models via prediction APIs. In: Proceedings of the 25th USENIX Security Symposium (USENIX Security 16), 2016. 601–618
90 Jagielski M, Carlini N, Berthelot D, et al. High accuracy and high fidelity extraction of neural networks. In: Proceedings of the 29th

USENIX Security Symposium (USENIX Security 20), 2020. 1345–1362
91 Batina L, Bhasin S, Jap D, et al. CSI NN: reverse engineering of neural network architectures through electromagnetic side channel. In: Proceedings of the 28th USENIX Security Symposium (USENIX Security 19), 2019. 515–532
92 Wei L, Luo B, Li Y, et al. I know what you see: power side-channel attack on convolutional neural network accelerators. In: Proceedings of the 34th Annual Computer Security Applications Conference, 2018. 393–406
93 Orekondy T, Schiele B, Fritz M. Prediction poisoning: towards defenses against DNN model stealing attacks. 2019. ArXiv:1906.10908
94 Sharma J, Mehra P S. HCFAIUN: a novel hyperelliptic curve and fuzzy extractor-based authentication for secure data transmission in IoT-based UAV networks. Vehicular Commun, 2024, 49: 100834
95 Bernstein D J. Chacha, a variant of salsa20. In: Proceedings of Workshop Record of SASC, Lausanne, 2008. 3–5
96 Coppolino L, D'Antonio S, Mazzeo G, et al. A comprehensive survey of hardware-assisted security: from the edge to the cloud. Internet Things, 2019, 6: 100055
97 Liu Z, Chen C, Ejaz A, et al. Automated binary analysis: a survey. In: Proceedings of International Conference on Algorithms and Architectures for Parallel Processing, 2022. 392–411
98 Fioraldi A, Maier D, Eißfeldt H, et al. AFL++: combining incremental steps of fuzzing research. In: Proceedings of the 14th USENIX Workshop on Offensive Technologies (WOOT 20), 2020
99 Pham V T, Boehme M, Santosa A E, et al. Smart Greybox fuzzing. IEEE Trans Software Eng, 2020, 47: 1980–1997
100 Fan C, Liu H, Li B, et al. Adversarial game against hybrid attacks in UAV communications with partial information. IEEE Trans Veh Technol, 2021, 71: 2204–2208
101 Bai T, Luo J, Zhao J, et al. Recent advances in adversarial training for adversarial robustness. 2021. ArXiv:2102.01356
102 Papernot N, McDaniel P, Wu X, et al. Distillation as a defense to adversarial perturbations against deep neural networks. In: Proceedings of 2016 IEEE symposium on security and privacy (SP), 2016. 582–597
103 Carlini N, Wagner D. Towards evaluating the robustness of neural networks. In: Proceedings of 2017 IEEE Symposium on Security and Privacy (SP), 2017. 39–57
104 Ch R, Srivastava G, Reddy Gadekallu T, et al. Security and privacy of UAV data using blockchain technology. J Inf Security Appl, 2020, 55: 102670
105 Xing H, Simeone O, Bi S. Federated learning over wireless device-to-device networks: algorithms and convergence analysis. IEEE J Sel Areas Commun, 2021, 39: 3723–3741
106 Figueira A, Vaz B. Survey on synthetic data generation, evaluation methods and GANs. Mathematics, 2022, 10: 2733
107 He Y, Huang D, Chen L, et al. A survey on zero trust architecture: challenges and future trends. Wireless Commun Mobile Computing, 2022, 2022: 6476274
108 Huang C Y, Lin Y Y, Lee H Y, et al. Defending your voice: adversarial attack on voice conversion. In: Proceedings of 2021 IEEE Spoken Language Technology Workshop (SLT), 2021. 552–559
109 Yuan X, Chen Y, Zhao Y, et al. CommanderSong: a systematic approach for practical adversarial voice recognition. In: Proceedings of 27th USENIX Security Symposium, 2018. 49–64
110 Dam D T, Tran T H, Hoang V P, et al. A survey of post-quantum cryptography: start of a new race. Cryptography, 2023, 7: 40
111 Kumar M, Pattnaik P. Post quantum cryptography (pqc)-an overview. In: Proceedings of 2020 IEEE High Performance Extreme Computing Conference (HPEC), 2020. 1–9
112 Mohammad K. Cyber shield: advances in detection, isolation, and containment mechanisms. In: Proceedings of AIAA SCITECH 2025 Forum, 2025. 2724
113 Wolf M, Weimerskirch A, Paar C. Security in automotive bus systems. In: Proceedings of Workshop on Embedded Security in Cars, 2004. 1–13
114 Pinto S, Santos N. Demystifying arm TrustZone: a comprehensive survey. ACM Comput Surv, 2019, 51: 1–36
115 Moran B, Tschofenig H, Brown D, et al. A firmware update architecture for Internet of Things. RFC 9019, 2021
116 Huang X, Kwiatkowska M, Wang S, et al. Safety verification of deep neural networks. In: Proceedings of International Conference on Computer Aided Verification, 2017. 3–29
117 Katz G, Barrett C, Dill D L, et al. Reluplex: an efficient smt solver for verifying deep neural networks. In: Proceedings of International Conference on Computer Aided Verification, 2017. 97–117
118 Sun X, Wang S, Zhang X, et al. LAERACE: taking the policy fast-track towards low-altitude economy. J Air Transp Res Soc, 2025, 4: 100058
119 Rauhala A, Tuomela A, Leviäkangas P. An overview of unmanned aircraft systems (UAS) governance and regulatory frameworks in the European Union (EU). In: Unmanned Aerial Systems in Agriculture: Eyes Above Fields. Amsterdam: Elsevier, 2023. 269–285
120 Lieb J, Volkert A. Unmanned aircraft systems traffic management: a comparsion on the FAA UTM and the European CORS conops based on u-space. In: Proceedings of 2020 AIAA/IEEE 39th Digital Avionics Systems Conference (DASC), 2020. 1–6
121 International Civil Aviation Organization. Manual on Space Weather Information in Support of International Air Navigation. Montreal, 2018. Approved by the Secretary General and published under ICAO authority. https://store.icao.int/en/manual-on-space-weather-information-in-support-of-international-air-navigation-doc-10100