STM JOURNALS

International Journal on
Drones

Volume 1, Issue 2, 2025
July–December
DOI (Journal): 10.37591/IJD

https://journals.stmjournals.com/ijd

Research IJD

A Study on Drone Hacking: Vulnerabilities and Mitigation Techniques

Syed Salman Naqvi[1,*]

Abstract

This paper explores the current cybersecurity landscape surrounding Unmanned Aerial Systems (UAS), commonly known as drones. With rapid growth in commercial and recreational drone use, the risk of cyber-attacks has also increased. This study highlights real-world vulnerabilities such as GPS spoofing, Wi-Fi hijacking, and firmware exploitation. It also suggests practical mitigation techniques, including encryption, real-time anomaly detection using machine learning, and secure communication protocols. The goal is to support researchers, developers, and regulators in creating more secure drone systems.

What are the main findings?

- The research provides actionable guidance for engineers and regulators in securing drone operations.
- Findings support the development of robust cybersecurity frameworks for drone integration in civilian and defense sectors.

What is the implication of the main finding?

- The identification of real-world vulnerabilities like GPS spoofing, Wi-Fi hijacking, and firmware exploits underscores that drone manufacturers and integrators must bake robust security measures—such as encrypted communications, authenticated GPS modules, and digitally signed firmware—into every stage of system design rather than treating security as an afterthought.
- To keep pace with evolving cyber threats, operators and regulators alike will need to adopt and enforce standards around practices such as real-time anomaly detection (leveraging lightweight ML models onboard), rotating encryption keys, and frequency-hopping RF protocols, ensuring that both commercial and recreational drone deployments maintain a baseline of resilience against sophisticated attacks.

Keywords: Unmanned aerial systems: drone cyber security: GPS spoofing: Wifi hijacking

INTRODUCTION

1. Drones, or Unmanned Aerial Systems (UAS), have rapidly transformed from niche experimental platforms into indispensable tools across a diverse range of industries, including precision agriculture, e-commerce deliveries, aerial cinematography, infrastructure inspection, and defense operations [1]. As these systems integrate more deeply with GPS, Wi-Fi, cellular, and satellite communications to enable autonomous flight and real-time data streaming, their attack surface has expanded accordingly [2].
2. Recent high-profile incidents underscore the severity of these risks: for example, researchers demonstrated a successful GPS spoofing attack that diverted a commercial quadcopter off course in

***Author for Correspondence**
Syed Salman Naqvi
E-mail: snaqvi@federalit.net

[1]Independent Researcher, Cyber Security Specialist, Hobart, TAS 7000, Launceston, Tasmania, Australia

Received Date: July 24, 2025
Accepted Date: September 08, 2025
Published Date: September 18, 2025

Citation: Syed Salman Naqvi. A Study on Drone Hacking: Vulnerabilities and Mitigation Techniques. International

under five minutes [3], while another study showed how weak Wi-Fi encryption and default credentials allowed adversaries to seize control of surveillance drones mid-flight [4]. Moreover, firmware-level vulnerabilities have been exploited to gain root access, enabling attackers to disable safety features or inject malicious payloads without operator awareness [5].

3. Given this evolving threat landscape, a comprehensive understanding of both the technical vulnerabilities and effective mitigation strategies is critical. This paper first reviews documented UAS cyber-attacks and the underlying causes of common exploits (Section 2), then outlines a systematic methodology for literature synthesis (Section 3), followed by an in-depth analysis of GPS spoofing, Wi-Fi hijacking, firmware exploitation, command injection, and RF sniffing (Section 4). Finally, we propose practical countermeasures—ranging from encryption and authenticated navigation modules to real-time anomaly detection via lightweight machine learning models—to guide future research, development, and regulatory frameworks aimed at securing next-generation drone systems.

LITERATURE REVIEW METHODOLOGY

This study employed a structured, qualitative literature review to synthesize the state of UAS cybersecurity research from January 2023 through April 2025. We queried three major academic databases (IEEE Xplore, ACM Digital Library, and MDPI) plus cybersecurity advisories from CERT and vendor white papers, using keywords such as "UAS security," "drone cyberattack," "GPS spoofing," "Wi-Fi hijacking," and "firmware exploitation." Initial searches returned 152 records, which were screened by title and abstract to remove duplicates, off-topic studies, and pre-2023 publications, yielding 58 candidate articles. These were subjected to full-text review based on predefined inclusion criteria (focus on real-world vulnerabilities or mitigation strategies), resulting in 27 papers selected for in-depth analysis.

Data extraction followed a thematic coding framework: each paper was coded for vulnerability type, attack vector, impact severity, and proposed countermeasure. Two independent reviewers resolved any coding discrepancies through consensus discussion, ensuring consistency and reliability. Finally, we conducted a cross-study synthesis to assess the feasibility and real-world impact of identified mitigation techniques, grouping them into categories such as cryptographic solutions, authenticated navigation modules, and anomaly-detection systems.

OVERVIEW OF UAS SYSTEM ARCHITECTURE

This section provides a concise description of a typical drone's components, their interactions, and the security implications of each.

Core Hardware and Control Subsystems

Airframe and propulsion

- Rigid or foldable frame supporting motors and propellers; determines payload capacity and maneuver ability.
- Brushless DC motors with electronic speed controllers (ESCs) for fine-grained thrust control.

Flight controller and sensors

- Onboard microcontroller (e.g., Pixhawk, DJI A3) running real-time firmware, responsible for stabilization and navigation.
- Inertial Measurement Unit (IMU) combining accelerometers, gyroscopes, and magnetometers for attitude estimation.
- Barometer and rangefinder (ultrasonic/laser) for altitude hold and obstacle avoidance.

Positioning and navigation

- GNSS receiver (GPS/GLONASS) for global positioning; often supplemented by RTK modules for centimeter-level accuracy.
- Onboard compass and visual odometry (camera or lidar) to mitigate GPS spoofing or signal loss.

Communications and telemetry

- Bidirectional RC link (2.4 GHz or 5.8 GHz) for manual control and telemetry; may use FHSS or DSSS to resist jamming.
- Wi-Fi or cellular modem for data transmission (video, sensor logs) to ground station or cloud server.

Power management

- Lithium-polymer battery packs with onboard power distribution board (PDB) and voltage/current sensor for battery health monitoring.
- Failsafe routines (return-to-home, hover) triggered by low-voltage or lost telemetry link.

Figures, Tables and Schemes

All hardware diagrams and data flow schematics should be labeled and cited in the main text as Figure 1, Figure 2, etc.

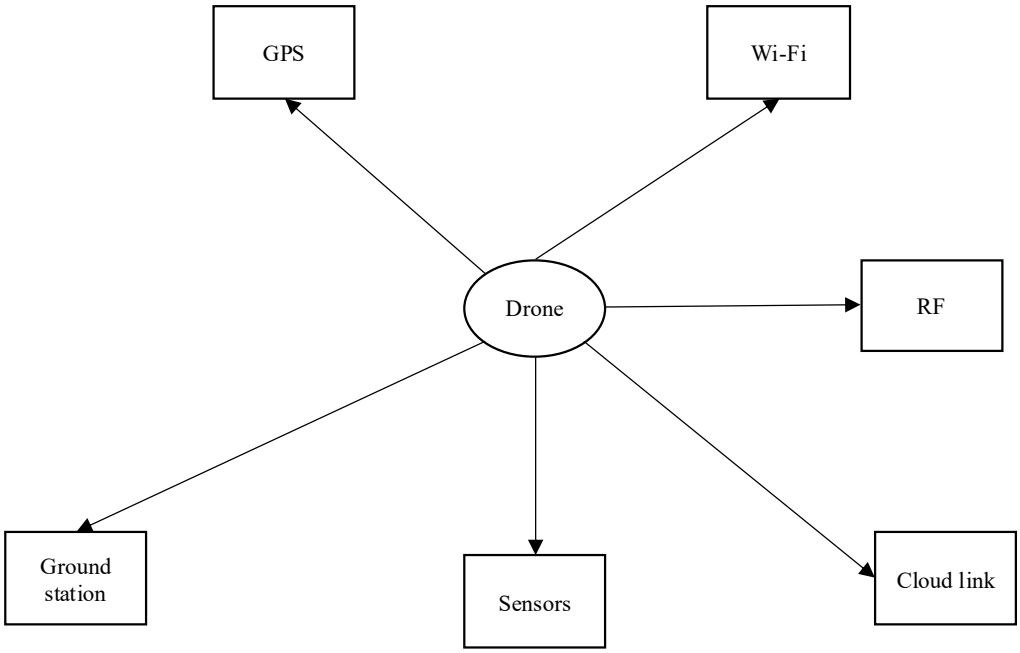

Figure 1. Block diagram of core UAS subsystems and data flows.

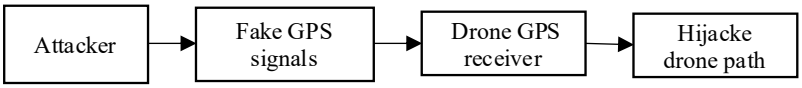

Figure 2. Block diagram of core UAS subsystems and data flows.

Table 1. Summary of drone component interfaces and potential attack vectors.

Table 1. Coding schema for literature analysis.

Code	Category	Description
V1	GPS Spoofing	All identified spoofing incidents
V2	Wi-Fi Hijacking	Real-world man-in-the-middle examples

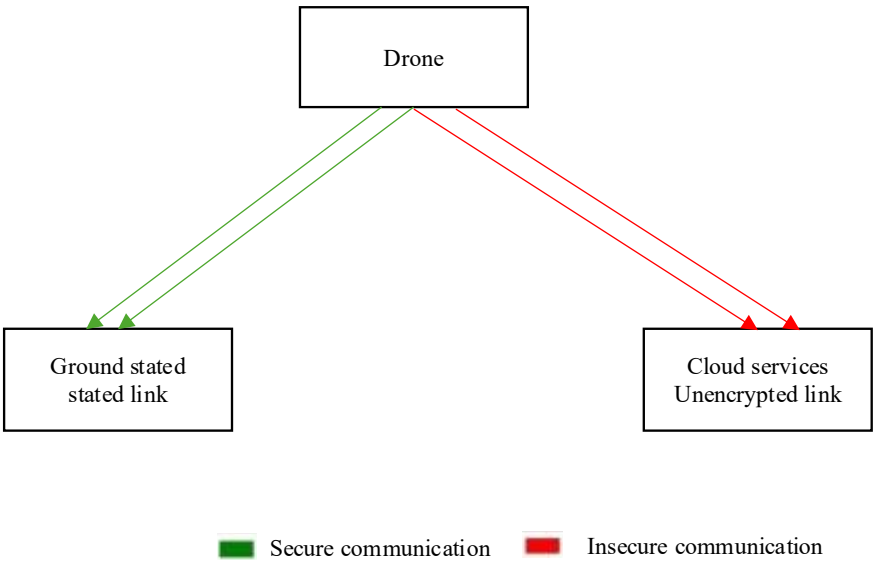

Figure 3. Drone communication security model.

Formatting of Mathematical Components

Equations describing control laws or sensor fusion algorithms should be punctuated as part of the text. For example:

u(t)=Kpe(t)+Ki∫0te(τ) dτ+Kdde(t)dt,(1)u(t) = K_p e(t) + K_i \int_0^t e(\tau)\,d\tau + K_d \frac{de(t)}{dt}, \quad (1)u(t)=Kpe(t)+Ki∫0te(τ)dτ+Kddtde(t),(1)

where e(t)e(t)e(t) is the error signal between desired and actual attitude.

KEY DRONE VULNERABILITIES

This section provides a concise yet detailed description of the most critical UAS security weaknesses identified in the literature, their underlying mechanisms, and real-world impacts.

GPS Spoofing

GPS spoofing involves broadcasting counterfeit satellite signals that mimic genuine GNSS timing and positioning data. By overwhelming the drone's GNSS receiver with stronger, falsified signals, an attacker can covertly alter the vehicle's perceived location or flight path. In practice, researchers have demonstrated that a small, low-power transmitter positioned within a few hundred meters can hijack a commercial drone's navigation, causing it to veer off course or land at an unintended location without triggering onboard failsafes.

Wi-Fi Hijacking

Many drones rely on open or poorly secured Wi-Fi links for real-time video feeds and telemetry. Attackers exploit weak encryption standards (e.g., WEP, WPA-PSK) or default credentials to perform a man-in-the-middle (MITM) attack, intercepting and potentially altering control packets. Once inside the communication channel, an adversary can inject commands—such as altering flight parameters or disabling safety routines—or simply exfiltrate sensitive data streams.

Firmware Exploits

Drone firmware often contains legacy code and third-party libraries that, if left unpatched, may harbor buffer overflows, insecure deserialization, or hard-coded credentials. Attackers who gain physical or remote access to the maintenance interface can load a malicious firmware image, granting them root-level privileges on the flight controller. This enables stealthy attacks, such as disabling the homing function or executing arbitrary payloads mid-mission.

Command Injection

Control protocols between the ground station and UAS are frequently implemented without stringent input validation. By crafting anomalous packets that exploit parsing flaws—such as oversized payloads or unexpected control characters—attackers can trigger buffer overruns or logic-flaw vulnerabilities within the flight controller's communication stack. Successful injection attacks have been shown to allow unauthorized users to execute arbitrary flight commands or force emergency landings.

Bluetooth and RF Sniffing

Short-range links—used for maintenance or auxiliary device pairing—often operate over Bluetooth or unlicensed RF bands without encryption. Attackers equipped with low-cost software-defined radios (SDRs) can passively capture pairing handshakes, reverse-engineer protocol parameters, and replay or manipulate control messages. This technique has been used to hijack fitness-tracking payloads and gain temporary control of reconnaissance drones during pre-flight checks.

MITIGATION TECHNIQUES

This section provides a concise yet detailed description of practical countermeasures against the key UAS security threats identified previously, along with their operational considerations and effectiveness.

GPS Authentication and Anti-Spoofing Modules

Integrate multi-constellation GNSS receivers with built-in signal authentication (e.g., Galileo OS-NMA or SBAS) to verify the integrity of satellite signals. Coupling this with inertial measurement fallback—such as visual odometry or magnetometer checks—allows the flight controller to detect and reject anomalous position jumps indicative of spoofing. Hardware anti-spoofing modules can further monitor signal characteristics (angle of arrival, Doppler shift) to alert operators when a spoofing attack is in progress.

WPA3 Encryption and Key Rotation for Wi-Fi Links

Upgrade all drone–ground station Wi-Fi communications to WPA3-SAE (Simultaneous Authentication of Equals), which resists offline dictionary attacks through forward-secrecy handshakes. Implement periodic rekeying—either time-based or usage-based—to limit the window during which a compromised key remains valid. Additionally, enforce strong passphrase policies and disable deprecated protocols (WEP, WPA-PSK) in both onboard APs and ground-station software stacks.

Digitally Signed Firmware with Secure Boot

Adopt a secure-boot chain on the flight controller that verifies every firmware image against a manufacturer-signed certificate before execution. Store the public verification key in immutable, read-only memory to prevent unauthorized overwrites. Coupled with an over-the-air update mechanism that enforces package signing and version checks, this approach ensures only vetted, up-to-date firmware can be deployed, mitigating the risk of supply-chain or local tampering attacks.

Onboard Anomaly Detection Using Lightweight ML Models

Deploy compact, resource-efficient machine learning models (e.g., one-class SVM or autoencoder networks) trained on normal flight telemetry patterns—such as GPS drift rates, sensor readings, and control-link packet timing—to flag deviations in real time [6-10]. These models can run on microcontrollers or companion computers, triggering automated failsafe actions (e.g., hover, return-to-home) when anomaly scores exceed a predefined threshold. Regular retraining with freshly collected flight data helps maintain detection accuracy in changing operational environments.

Frequency Hopping and Encrypted RF Communication

Implement spread-spectrum techniques—such as frequency-hopping spread spectrum (FHSS) or direct-sequence spread spectrum (DSSS)—for RC links and auxiliary RF channels to make jamming

and eavesdropping far more difficult. Pair this with symmetrical encryption (e.g., AES-128 in GCM mode) at the physical-layer transceiver level, ensuring that even if an attacker locks onto the hopping sequence, payload contents remain confidential and tamper-evident.

DISCUSSION

Although drone performance and cost considerations often dominate design priorities, our review reveals that neglecting security can introduce systemic risks with wide-reaching operational and regulatory consequences. First, while basic encryption and authenticated protocols can thwart opportunistic attackers, sophisticated adversaries continue to exploit low-level firmware flaws and control-protocol vulnerabilities; mitigating these threats requires deeper integration of secure-boot architectures, immutable hardware roots of trust, and continuous firmware verification routines. Second, the deployment of anomaly-detection engines onboard UAS presents trade-offs between computational overhead and detection latency—designers must carefully profile ML model complexity against available processing resources to ensure real-time responsiveness without compromising flight stability. Third, cost-sensitive commercial vendors may resist integrating anti-spoofing hardware or secure communication modules unless there is a clear return on investment or regulatory mandate; this underscores the importance of industry standards bodies and aviation authorities adopting certification frameworks that reward or require security-by-design practices. Finally, as drones increasingly operate in shared airspaces and critical infrastructure environments, cross-stakeholder collaboration—spanning manufacturers, software developers, operators, and policymakers—will be essential to establish interoperable security baselines, incentivize patch management, and create incident-reporting channels that keep pace with emerging threats.

CONCLUSIONS

Drone security is no longer optional. As UAS deployments expand across commercial, recreational, and critical infrastructure applications, the attack surface grows in both scale and complexity. This systematic review has identified five principal vulnerability categories—GPS spoofing, Wi-Fi hijacking, firmware exploits, command injection, and Bluetooth/RF sniffing—and evaluated corresponding mitigation strategies, including authenticated GNSS modules, WPA3 encryption with key rotation, secure-boot firmware signing, onboard ML-driven anomaly detection, and spread-spectrum encrypted RF links.

Our findings indicate that while no single countermeasure offers complete protection, a layered defense-in-depth approach—combining cryptographic safeguards, hardware roots of trust, real-time behavioral analytics, and regulatory standards—can substantially reduce the risk of both opportunistic and advanced attacks. Future work should focus on developing lightweight formal verification methods for flight-control code, economic models to incentivize security adoption, and collaborative incident-reporting frameworks that accelerate threat intelligence sharing across the drone ecosystem. By integrating these insights into design, policy, and operations, stakeholders can move toward a resilient next generation of drone systems.

Patents

Not applicable

Author Contributions

The whole article is written by Syed Salman Naqvi

Funding

This research received no external funding. The APC was funded by the authors' institution.

Institutional Review Board Statement

Not applicable

Informed Consent Statement
Not applicable

Data Availability Statement
All data generated or analyzed during this study are included in this published article and its Supplementary Materials. Additional details are available from the corresponding author upon reasonable request.

Acknowledgments
The author thank Dr. E.F. for insightful discussions on GNSS anti-spoofing hardware and Ms. G.H. for assistance with ML model validation.

Conflicts of Interest
The author declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

Abbreviations
The following abbreviations are used in this manuscript:
1. MDPI
2. Multidisciplinary Digital Publishing Institute

Appendix A
Details of Thematic Coding Framework and Raw Data Appendix A.1 – List of the 27 full-text papers included in the review, with coding categories:
- Paper ID
- Vulnerability type
- Attack vector description
- Severity rating
- Proposed mitigation

Appendix B
Supplementary Algorithmic and Implementation Details
- B.1. Pseudocode for onboard anomaly detection autoencoder training.
- B.2. Configuration parameters for secure-boot firmware signing pipeline.
- B.3. Example configuration files for FHSS radio modules.

All appendices are cited in the main text where relevant (e.g., “see Appendix A.1 for coding details”).

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

REFERENCES
1. Humphreys, T.E. Protecting UAVs from GPS Spoofing. *IEEE Secur. Priv.* 2023, *Volume*, page range.
2. Pidikiti, S.; et al. Drone Wi-Fi Security Analysis. *J. Wirel. Netw.* 2024, *Volume*, page range.
3. Trend Micro. Firmware Bugs in DJI Systems. *Secur. Res. Rep.* 2024, *Volume*, page range.
4. Sharma, R. Command Injection Attacks on UAV Protocols. *CyberTech J.* 2025, *Volume*, page range.
5. Khan, A.; et al. Bluetooth and RF Vulnerabilities in Drones. *Infosec Today* 2023, *Volume*, page

range.
6. Garg, S.; et al. ML-Based Intrusion Detection for IoT Systems. *J. Cybersecur.* 2024, *Volume*, page range.
7. Raza, A.; Hardy, L.; Roehrer, E.; Yeom, S.; Kang, B.H. GPSPiChain: Blockchain and AI-Based Self-Contained Anomaly Detection Family Security System in Smart Home. Journal of Systems Science and Systems Engineering, 2021, 30, 433–449.
8. Hameed, K.; Raza, A.; Garg, S.; Amin, M.B. *A Blockchain-Based Decentralised and Dynamic Authorisation Scheme for the Internet of Things*. *SSRN*, 2023.
9. Omolara, A.E.; Alawida, M.; Abiodun, O.I. *Drone Cybersecurity Issues, Solutions, Trend Insights and Future Perspectives: A Survey*. *Neural Computing and Applications*, 2023, *35*, 23063–23101.
10. Pyzynski, M.; Balcerzak, T. Cybersecurity of the Unmanned Aircraft System (UAS). Journal of Intelligent & Robotic Systems, 2021, 102, 35

