http://www.jctjournals.com ISSN(ONLINE):2278 – 3814

Volume-15, Issue-09, September 2026
JOURNAL OF COMPUTING TECHNOLOGIES (JCT)
International Journal
Page Number: 01-07

UAV GPS Spoofing Cyber Attacks and the Importance of IoT in Countermeasures and Prevention

[1]Shivangi Jain, [2]Smriti Dubey, [3]Anusha Lahoti, [4]Yogita Mishra
[1, 2, 3, 4] Assistant Professor
[1, 3, 4]Department of Cyber security and IoT, [2] Department of Artificial intelligence and data science
[1,2,3,4] Samrat Ashok Technological Institute (S.A.T.I.), Vidisha, M.P., INDIA

***Abstract*— Unmanned aerial vehicles (UAVs) increasingly depend on global navigation satellite systems (GNSS), especially the Global Positioning System (GPS), for navigation, timing, geo fencing, return-to-home functions, and mission coordination. This dependence creates a high-impact cyber-physical attack surface: GPS spoofing can make a vehicle accept counterfeit position, velocity, or timing information and consequently drift from its route, violate restricted airspace, crash, or disclose sensitive mission data. This review surveys representative research published during the last ten years on UAV GNSS spoofing, detection, localization, resilient navigation, and Internet of Things (IoT)-enabled countermeasures. Fifteen influential studies are compared according to attack model, sensing strategy, detection method, evaluation environment, and limitations. The review also develops a comparative taxonomy of jamming, mea coning, coherent spoofing, replay, cyber-compromise, and hybrid attacks. Particular attention is given to IoT architectures that combine UAV telemetry, edge computing, cooperative sensing, trusted time, block chain or distributed ledgers, and software-defined radios. The survey identifies research gaps in realistic multi-UAV testing, cross-layer security, explainable detection, energy-aware defense, standard datasets, and coordinated response. It concludes that robust prevention requires layered navigation rather than reliance on GPS alone, with IoT acting as a distributed trust and sensing fabric.**

Keywords—UAV; GPS spoofing; GNSS security; cyber-physical systems; Internet of Things; edge computing; sensor fusion; anomaly detection; resilient navigation; drone security

I. INTRODUCTION

Unmanned Aerial Vehicles (UAVs) have evolved from specialized aerospace and military platforms into increasingly important components of modern civilian and industrial infrastructure. Their applications encompass logistics, precision agriculture, environmental monitoring, infrastructure inspection, emergency response, geographical mapping, surveillance, and smart-city services. The operational efficiency of UAVs depends on the integration of navigation sensors, wireless communication networks, embedded control systems, onboard computing, and cloud-based services. Global Positioning System (GPS) and Global Navigation Satellite System (GNSS) technologies play a fundamental role in autonomous navigation by providing positioning, velocity, and timing information. However, the low received power and limited authentication capabilities of conventional civilian navigation signals expose UAV systems to intentional radio-frequency interference and cyber-physical attacks [1], [2]. Among navigation-related cyber security threats, GPS spoofing represents a particularly significant challenge because it manipulates the positioning information used by autonomous flight-control systems. Unlike GPS jamming, which primarily disrupts satellite signal reception, GPS spoofing attempts to deceive navigation receivers through counterfeit or manipulated satellite-like signals [3], [4]. A successful spoofing attack may gradually introduce false positioning information while maintaining apparently valid receiver tracking and navigation-filter operation. Consequently, an affected UAV may deviate from its intended trajectory, experience mission disruption, or execute unsafe navigation decisions without immediately identifying the underlying manipulation.

Several countermeasures have been investigated to strengthen UAV navigation security, including signal-quality monitoring, angle-of-arrival estimation, multi-antenna processing, inertial navigation integration, visual odometer, cooperative positioning, machine learning, and cryptographic authentication. Nevertheless, many existing approaches face challenges related to computational overhead, environmental variability, sensor uncertainty, communication constraints, and limited validation under realistic operating conditions [4], [5].

The Internet of Things (IoT) offers additional opportunities for developing distributed and context-aware security mechanisms. By integrating UAVs with ground-based

 Copyright © 2026. JCT Publications. All Rights Reserved

sensors, wireless networks, edge-computing infrastructure, and interconnected monitoring devices, IoT-enabled architectures can support cooperative anomaly detection, independent positioning verification, real-time threat assessment, and coordinated defensive responses. These capabilities motivate the investigation of integrated cyber security frameworks that combine onboard navigation resilience with distributed sensing and intelligent decision-making.

1.1 Background of the Study

The increasing deployment of UAVs in autonomous and semi-autonomous operations has introduced new cyber security requirements for navigation, communication, and flight-control systems. Modern UAV architectures integrate several interdependent components, including GNSS receivers, inertial measurement units (IMUs), flight controllers, wireless communication modules, onboard processors, and external monitoring infrastructure. These components enable autonomous flight, waypoint navigation, obstacle avoidance, mission planning, and communication with ground-control stations. However, their interconnected nature creates multiple potential attack surfaces through which adversaries may compromise navigation integrity and operational reliability.

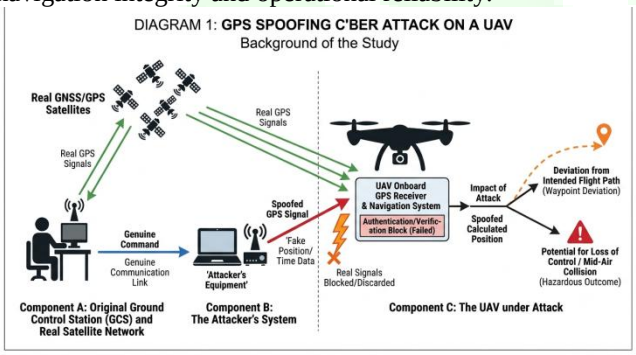


Fig.1 : GPS Spoofing C'BER Attack on a UAV

GPS is widely employed in UAV navigation because it provides globally accessible positioning and timing services without requiring extensive local infrastructure. Nevertheless, conventional civilian GPS signals are transmitted at extremely low power levels when received on Earth and, for many widely deployed signal services, do not provide cryptographic authentication of navigation information [2], [1]. This creates opportunities for adversaries to introduce counterfeit satellite-like signals capable of influencing receiver measurements and position estimation.

GPS spoofing is generally characterized by the intentional manipulation of GNSS observations to produce incorrect position, velocity, or timing estimates [3], [4]. Depending on attacker capabilities and receiver behavior, spoofing may involve the introduction of fabricated navigation signals, synchronization with legitimate signals, or gradual manipulation of receiver tracking solutions. Such attacks can affect autonomous UAV operations by corrupting waypoint navigation, geo fencing decisions, return-to-home functions, and other position-dependent control mechanisms.

The consequences of GPS spoofing extend beyond positioning errors. In applications involving autonomous delivery, infrastructure inspection, emergency operations, and coordinated UAV missions, compromised navigation information can undermine operational safety, mission continuity, and the reliability of collected geospatial data. Furthermore, when corrupted positioning information is transmitted to connect monitoring platforms, the resulting data may influence external decision-support systems.

Traditional GPS spoofing countermeasures can be broadly classified into signal-based, sensor-based, navigation-based, and data-driven approaches [4], [5]. Signal-based approaches examine radio-frequency characteristics, received signal strength, correlation patterns, and spatial properties to identify abnormalities. Sensor-based methods exploit inconsistencies between GNSS measurements and independent sources, such as IMUs, cameras, barometers, and magnetometers. Navigation-based techniques use estimation and consistency-checking mechanisms to identify potentially manipulated position solutions. More recently, machine-learning approaches have been investigated for identifying complex spoofing patterns from multidimensional sensor and receiver measurements.

Despite these developments, individual countermeasures may be constrained by environmental conditions, hardware requirements, limited computational resources, or dependencies on particular attack characteristics. Sensor fusion can improve consistency checking, but its reliability depends on sensor calibration, estimation uncertainty, and the availability of sufficiently independent measurements. Similarly, machine-learning systems may exhibit limited generalization when deployed against spoofing patterns that differ from their training data.

IoT technologies introduce a complementary security perspective by extending navigation monitoring beyond the UAV itself. IoT-enabled systems can incorporate distributed ground sensors, interconnected UAV platforms, edge servers, cellular communication infrastructure, and external monitoring stations. These resources can provide independent observations, contextual information, and cooperative anomaly indicators that may assist in identifying discrepancies between reported navigation states and independently observed system behavior.

Through edge computing, selected detection and validation tasks can be performed near the UAV operating environment, potentially reducing dependence on distant cloud services. However, IoT-based protection also introduces security and reliability challenges involving communication latency, network availability, device authentication, data integrity, interoperability, and the trustworthiness of distributed observations.

Therefore, the development of secure UAV navigation requires a comprehensive understanding of GPS spoofing mechanisms, conventional mitigation strategies, and the potential benefits and limitations of IoT-enabled cyber security architectures.

 Copyright © 2026. JCT Publications. All Rights Reserved

1.2 Research Motivation

The growing dependence on autonomous UAV operations has intensified the need for reliable navigation security mechanisms capable of identifying and mitigating GPS spoofing attacks under dynamic operating conditions. Although substantial research has examined GNSS interference detection and navigation resilience, the development of practical, scalable, and operationally validated protection frameworks remains an important research challenge.

The primary motivation for this study arises from the limitations of relying exclusively on onboard GPS receivers or isolated detection mechanisms. A UAV operating in a complex environment may encounter GNSS signal degradation, multipath propagation, sensor disturbances, and intentional navigation manipulation. These phenomena can produce overlapping measurement abnormalities, making it difficult to distinguish malicious spoofing from non-malicious navigation errors. Detection methods based on individual signal characteristics or fixed thresholds may therefore be insufficient across diverse flight conditions.

The motivation for this review can be summarized through five research priorities:

- Navigation integrity and operational safety: Investigating how GPS spoofing compromises UAV positioning, trajectory control, and mission reliability.
- Limitations of conventional countermeasures: Evaluating the strengths and weaknesses of signal monitoring, sensor fusion, navigation consistency checks, and machine-learning-based detection.
- IoT-enabled cooperative defense: Examining the potential of distributed sensors, interconnected UAVs, edge computing, and secure communication networks to support independent navigation verification and coordinated threat detection.
- Intelligent and adaptive cyber security: Assessing the role of artificial intelligence, machine learning, and hybrid detection mechanisms in identifying navigation anomalies under varying environmental and attack conditions.
- Research standardization and practical deployment: Identifying unresolved challenges involving detection accuracy, false-alarm rates, computational complexity, communication latency, scalability, cyber security, and real-world validation.

Accordingly, this review seeks to establish a systematic understanding of GPS spoofing threats affecting UAV systems and critically examine the contribution of IoT-enabled technologies to attack detection, mitigation, and prevention. Particular attention is given to the integration of distributed sensing, intelligent anomaly detection, secure communication, and resilient navigation mechanisms.

The study aims to identify opportunities for developing practical defense architectures that maintain navigation integrity while satisfying the operational constraints of autonomous UAV platforms.

II. LITERATURE REVIEW

The survey considers representative work published from 2016 through 2026, emphasizing studies that address UAV navigation, GNSS spoofing, detection, or networked countermeasures. The selected papers are grouped into five themes: (i) attack construction and threat modeling, (ii) signal and receiver-level detection, (iii) sensor fusion and alternative navigation, (iv) machine learning and distributed intelligence, and (v) IoT, edge, and cooperative defense.

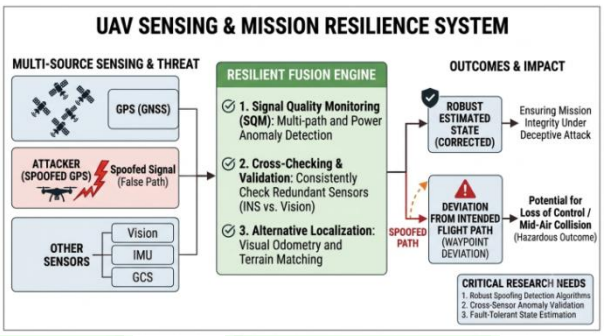


Fig. 2: UAV Sensing & Mission Resilience system

2.1 Literature Survey

Research on UAV GPS spoofing has moved from demonstrating attacks, to receiver-level detection, to sensor fusion, machine learning, and IoT-based cooperative defense. Early work showed that a UAV could be captured and steered through GPS spoofing [6]. In 2016, Psiaki and Humphreys formalized the stages of GNSS deception and their effect on receivers [3], although this taxonomy had limited UAV-specific validation. In the same year, Huang et al. analyzed the Ratio Test metric, which monitors distortions of the signal correlation, and derived a model of its false-alarm and detection probabilities [7]. Krishna and Murphy reviewed cyber security vulnerabilities of UAVs [8].

Multi-antenna detection estimates the direction of arrival of signals. Psiaki et al. exploited the fact that a single spoofer produces one arrival direction, whereas authentic signals arrive from many directions [9]. Later work extended this with antenna arrays. Magiera combined antenna-array processing with multipath detection to catch intermediate spoofing early [10]. Van der Merwe et al. used a multi-antenna snapshot receiver, noting that direction-of-arrival detection requires array calibration, which raises cost and complexity [11].

For inertial and GNSS fusion, Tanıl et al. proposed an innovation-based INS monitor using a tightly coupled Kalman filter [12] and later evaluated it against worst-case spoofing attacks, including spoofers able to track vehicle position [13]. The weakness is that inertial drift grows during long GNSS outages. Vision has been used as a further independent source: Varshosaz et al. proposed a UAV spoofing-detection method based on visual odometry that is independent of other complementary sensors [14],

 Copyright © 2026. JCT Publications. All Rights Reserved

and Gu et al. detected spoofing using a coupled visual/inertial/GNSS navigation system [15].

On the attack side, Noh et al. analyzed the GPS fail-safe modes of consumer drones and designed adaptive spoofing strategies, which they verified in field experiments and simulations [16]. Sathaye et al. experimentally studied GPS spoofing and takeover attacks on UAVs [17]. Machine-learning detection also began classifying signal and telemetry anomalies; Jullian et al. used a multilayer perceptron that processes flight parameters and GPS signals to raise spoofing alarms [18]. This family of methods is limited by scarce datasets and poor transferability between environments.

Cooperative and edge-based defenses build on these ideas. Mykytyn et al. compared inter-UAV distances calculated from GPS coordinates with distances measured by ultra-wideband ranging [1]. Bi et al. cast malicious-UAV detection in a swarm as a localization feasibility problem using reported positions and distance measurements [19]. Cooperative methods of this kind add trust and bandwidth overhead. For edge-assisted detection, Dang et al. used path losses between base stations and cellular-connected UAVs to indicate trajectory deviation caused by spoofing [20], and used transfer learning to move CNN knowledge between edge servers as a UAV hands over between base stations [21]. Edge-node compromise is still unsolved.

Authentication is a separate line of defense. In November 2020, Galileo became the first GNSS to broadcast authentication data in an Open Service signal, allowing users to verify the authenticity of the navigation message [2]. Navigation message authentication alone does not authenticate the range measurements, so it is insufficient for full position, velocity and timing authentication [22]. Deployment across GNSS constellations remains uneven. Simulation and emulation test beds support repeatable cyber-physical experiments: Pant et al. proposed a mixed-reality sensor emulation framework for testing UAVs against false data injection attacks and demonstrated an emulated GNSS attack on an actual UAV [23]. Such frameworks are motivated by the limited fidelity of purely software-in-the-loop tests [23].

Broader surveys now consolidate the field. Khan et al. reviewed GPS spoofing threats with a focus on UAVs and other GPS-dependent mobile platforms [4]. Restivo et al. surveyed spoofing attacks, detection, and safeguards on UAVs [5]. More recent work adds federated learning and resilient autonomy. She et al. trained an anomaly-detection model across multiple base stations with federated learning, adding a shrink auto encoder to handle differing data distributions [24]. Non-identically distributed UAV data and poisoning risks remain open challenges [25]. For trust in IoT-enabled UAV networks, Hafeez et al. surveyed block chain-assisted UAV communication, noting that decentralization improves trust and data integrity but that its computational delay can be unsuitable for swarm applications [26]. Finally, Kujur et al. addressed the hardest-to-detect case, in which a spoofer replicates the authentic signal with only tracking errors [27]. Resilient autonomy that integrates GNSS, inertial, vision, RF, and network evidence still needs open field benchmarks and standards.

TABLE - 1. Representative Literature Survey

Author/ Year/ Ref.	Focus	Main contribution	Observed limitation
Psiaki & Humphreys, 2016 [3]	GNSS spoofing taxonomy	Formalized deception stages and receiver effects	Limited UAV-specific validation
Huang et al., 2016 [7]	GNSS signal monitoring	Used correlation and signal-quality indicators	Sensitive to receiver diversity
Krishna & Murphy, 2017 [8]	UAV navigation security	Linked spoofing to autonomous flight risk	Mostly simulation based
Psiaki et al., 2014 [9]; Magiera, 2019 [10]	Multi-antenna detection	Estimated direction of arrival and consistency	Hardware cost and calibration
Tanıl et al., 2018 [13]	Inertial/GNSS fusion	Used residuals to detect inconsistent navigation	Drift grows during long outages
Varshosaz et al., 2020 [14]; Gu et al., 2021 [15]	Vision-aided navigation	Added optical flow and visual odometry	Lighting and weather dependence
Noh et al., 2019 [16]; Sathaye et al., 2022 [17]	Software-defined radio attacks	Demonstrated accessible spoofing prototypes	Controlled test conditions
Jullian et al., 2022 [18]	Machine-learning detection	Classified signal and telemetry anomalies	Dataset scarcity and transferability
Mykytyn et al., 2023 [1]; Bi et al., 2024 [19]	Cooperative UAV defense	Shared observations across a swarm	Trust and bandwidth overhead
Dang et al., 2022 [20], [21]	Edge-assisted security	Moved analytics closer to the flight path	Edge node compromise not solved
Köller et al., 2023 [2]	GNSS authentication	Reviewed signal and navigation-message protection	Authentication deployment is uneven
Pant et al., 2024 [23]	Digital-twin simulation	Created repeatable cyber-physical experiments	Model fidelity remains a concern
She et al., 2024 [24]	Federated learning	Trained detectors without centralizing raw data	Non-IID UAV data and poisoning risks
Hafeez et al., 2023 [26]	IoT trust management	Combined device identity, attestation, and telemetry	Interoperability is immature
Kujur et al., 2024 [27]	Resilient autonomy	Integrated GNSS, inertial, vision, RF, and network evidence	Need open field benchmarks and standards

2.1 Synthesis of the Reviewed Literature

 Copyright © 2026. JCT Publications. All Rights Reserved

The reviewed studies show a clear progression. Early work concentrated on demonstrating that low-cost transmitters and software-defined radios could manipulate a receiver [6], [16], [17]. The next wave focused on indicators available inside the receiver, such as carrier-to-noise ratio, correlation-peak distortion, Doppler consistency, clock behavior, and navigation residuals [3], [7]. More recent research treats spoofing as a cyber-physical anomaly and combines RF evidence with inertial, visual, acoustic, map, and network data [13], [15], [20].

A second trend is the shift from single-UAV protection to cooperative defense [1], [19]. A UAV may be uncertain about its own GNSS state, but a nearby aircraft, base station, cellular tower, or edge node may observe an inconsistent time, direction, or trajectory. IoT architectures make it possible to fuse these observations, assign confidence scores, and distribute alerts [20], [21]. The main unresolved issue is trust: compromised devices can send false evidence, and poorly designed consensus mechanisms can amplify rather than suppress deception [19], [26].

A third trend is the movement of detection from rule-based thresholds toward adaptive learning [18], [24]. Machine learning can recognize multidimensional patterns that are difficult to encode manually, but performance depends on representative data. Spoofing waveforms, aircraft dynamics, antenna layouts, weather, and receiver firmware vary widely. Therefore, a detector trained in one environment can produce false alarms or miss attacks in another. The literature increasingly supports hybrid systems in which physical constraints and model-based residuals constrain the learning component.

TABLE - II. Comparative Assessment Of Countermeasures

Attack type	Primary objective	Typical mechanism	Observable symptoms	Useful countermeasure
Jamming	Deny navigation	Broadband or narrowband interference	Loss of lock, rising noise, navigation outage	Interference detection, inertial/vision fallback
Meaconing	Replay authentic signals later or elsewhere	Record and retransmit GNSS signals	Timing/position inconsistency, delayed solution	Time checks, multi-source comparison
Coherent spoofing	Gradually move the UAV	Matched counterfeit code/carrier signals	Smooth but false trajectory	RF consistency, inertial and map residuals
Non-coherent spoofing	Create false satellite set	Independent counterfeit channels	Abrupt jumps or satellite inconsistency	Receiver integrity monitoring
Replay of telemetry	Mislead remote operator or autonomy	Reuse old position or status packets	Stale timestamps, impossible dynamics	Freshness, sequence numbers, secure time
Firmware compromise	Change navigation or control logic	Malware, supply-chain or update attack	Unexpected settings or control outputs	Secure boot, attestation, signed updates
IoT/edge compromise	Corrupt cooperative defense	False reports or denial of service	Conflicting observations and trust anomalies	PKI, attestation, quorum and isolation
Hybrid cyber-physical attack	Maximize mission impact	Combine spoofing, jamming and link attacks	Ambiguous or cascading failures	Layered detection and fail-safe autonomy

III. RESEARCH GAP AND LIMITATIONS

Despite meaningful progress, the literature leaves several research gaps:

- Lack of common datasets: Many studies use private recordings, simulated signals, or a single
- receiver, preventing fair comparison.
- Insufficient field realism: Laboratory spoofing rarely captures multipath, urban blockage, weather, antenna motion, and mixed legitimate traffic.
- Weak cross-layer modeling: RF anomalies, flight-control behavior, command-and-control links, cloud services, and ground infrastructure are often analyzed separately.
- Limited adversarial evaluation: Detectors are seldom tested against adaptive attackers that know the detection features or poison training data.
- Energy and latency constraints: Sophisticated multi-sensor and deep-learning defenses may be too costly for small UAVs.
- Inadequate trust models for IoT: Cooperative defense requires device identity, attestation, secure time, revocation, and protection from compromised participants.
- Poor explainability: Safety-critical operators need a reason for an alert, not only a probability score.
- Unclear response policies: Detection is not enough; systems need safe fallback modes, controlled landing, navigation-source switching, and evidence preservation.

IV. IoT-BASED ATTACK PRESENTATION AND COUNTERMEASURE ARCHITECTURE

IoT changes the problem from a single receiver defending itself to a distributed cyber-physical system. In a representative architecture, the UAV collects GNSS, inertial, barometric, magnetic, visual, RF-spectrum, and flight-controller evidence. Nearby IoT devices—ground sensors, roadside units, cellular infrastructure, weather stations, and neighboring UAVs—submit signed observations to an edge gateway [20]. The gateway performs low-latency fusion and forwards summarized events to a cloud or command center for fleet-level analytics.

An IoT-based spoofing attack may proceed in stages. First, the adversary identifies a weakly protected receiver or edge node. Second, it transmits counterfeit GNSS signals or injects false telemetry. Third, it exploits trust relationships so that false data are treated as corroboration. Finally, it attempts to suppress alarms by jamming,

 Copyright © 2026. JCT Publications. All Rights Reserved

flooding the network, or compromising the model-update process. This attack chain demonstrates why navigation security cannot be separated from identity, communication, firmware, and cloud security.

A practical countermeasure architecture should include: (1) device identity using certificates or hardware-backed keys; (2) secure boot and signed firmware; (3) authenticated, fresh telemetry with timestamps and sequence numbers; (4) local anomaly detection that remains functional during disconnection; (5) edge fusion of RF, inertial, visual, map, and neighboring-device evidence; (6) trust scores that decay when a device disagrees with validated physics; (7) safe navigation modes such as inertial hold, visual odometry, terrain-relative navigation, or controlled landing; and (8) forensic logging for post-incident analysis.

The IoT layer should not blindly average all reports. A robust design assigns confidence according to sensor health, geographic relevance, time synchronization, device attestation, and historical consistency. Byzantine-resilient aggregation or quorum-based decisions can limit the effect of compromised nodes [28]. Federated learning can reduce raw-data exposure, but model updates must be authenticated and checked for poisoning [24], [25]. Block chain or distributed ledgers may help with audit ability and identity, yet they should not be treated as a substitute for real-time detection because consensus latency and resource cost may be unacceptable for flight control [26].

V. CHALLENGES FOR THE CURRENT GENERATION

Heterogeneous platforms: Consumer, industrial, and defense UAVs expose different processors, receivers, buses, and update mechanisms.

- Real-time constraints: A correct decision that arrives too late can still cause a collision or loss of the vehicle.
- GNSS-denied environments: Urban canyons, indoor areas, tunnels, and heavy foliage can resemble attack conditions.
- Adversarial adaptation: Attackers can vary power, dynamics, modulation, timing, and target behavior to imitate legitimate signals.
- Certification and safety: Defensive software must be explainable, testable, and compatible with aviation assurance processes.
- Privacy and governance: IoT telemetry can reveal routes, operators, infrastructure, and sensitive mission information.
- Interoperability: UAVs, IoT gateways, cloud services, and emergency systems often lack common security and data models.

VI. CONCLUSION AND FUTURE SCOPE

GPS spoofing is a serious cyber-physical threat because it attacks the information used to make physical decisions. The literature shows that no single defense is sufficient. Signal-quality checks can miss low-and-slow deception; inertial systems drift; cameras fail in poor visibility; machine-learning models face dataset shift; and cryptographic authentication does not prevent all denial or receiver-level manipulation. The most credible direction is layered resilient autonomy that combines independent sensors, physical consistency checks, authenticated communications, and carefully designed fallback behavior.

IoT is important not merely because it connects more devices, but because it enables distributed evidence and shared situational awareness. Edge nodes can detect local anomalies with low latency, neighboring devices can provide independent observations, and fleet-level services can learn from incidents. However, IoT also expands the attack surface. Future systems should therefore combine zero-trust identity, hardware-backed attestation, secure time, privacy-preserving analytics, Byzantine-resilient fusion, and explicit safety policies.

Future research should prioritize open multi-environment datasets, reproducible SDR-based testbeds, hardware-in-the-loop validation, adaptive adversarial evaluation, explainable hybrid models, energy-aware edge inference, and formal verification of fallback modes. Research should also examine coordinated attacks against multi-UAV swarms and the interaction between GNSS spoofing, 5G/6G networks, cloud control, and autonomous mission planning. Progress in these areas can move UAV security from isolated detection demonstrations toward measurable, certifiable, and operationally trustworthy resilience.

References

[1] P. Mykytyn, M. Brzozowski, Z. Dyka, and P. Langendoerfer, “GPS-spoofing attack detection mechanism for UAV swarms,” in Proc. Mediterranean Conf. Embedded Computing (MECO), 2023, arXiv:2301.12766.

[2] E. Köller, I. Viciano-Semper, D. Oskam, J. Simon, et al., “Galileo Open Service Navigation Message Authentication: Preparation phase and drivers for future service provision,” NAVIGATION, vol. 70, no. 3, 2023.

[3] M. L. Psiaki and T. E. Humphreys, “GNSS spoofing and detection,” Proc. IEEE, vol. 104, no. 6, pp. 1258–1270, Jun. 2016.

[4] S. Z. Khan, M. Mohsin, and W. Iqbal, “On GPS spoofing of aerial platforms: A review of threats, challenges, methodologies, and future research directions,” PeerJ Comput. Sci., vol. 7, Art. no. e507, 2021, doi: 10.7717/peerj-cs.507.

[5] R. D. Restivo, L. C. Dodson, J. Wang, W. Tan, Y. Liu, H. Wang, and H. Song, “GPS spoofing on UAV: A survey,” in Proc. IEEE INFOCOM Workshops (AidTSP), 2023.

[6] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, “Unmanned aircraft capture and control via GPS spoofing,” J. Field Robotics, vol. 31, no. 4, pp. 617–636, 2014.

[7] J. Huang, L. Lo Presti, B. Motella, and M. Pini, “GNSS spoofing detection: Theoretical analysis and performance of the Ratio Test metric in open sky,” ICT Express, Mar. 2016, doi: 10.1016/j.icte.2016.02.006.

[8] C. L. Krishna and R. R. Murphy, “A review on cybersecurity vulnerabilities for unmanned aerial vehicles,” in Proc. IEEE Int. Symp. Safety, Security and Rescue Robotics (SSRR), 2017, pp. 194–199.

[9] M. L. Psiaki, B. W. O’Hanlon, S. P. Powell, J. A. Bhatti, K. D. Wesson, and T. E. Humphreys, “GNSS spoofing detection using two-antenna differential carrier phase,” in Proc. ION GNSS+, 2014.

 Copyright © 2026. JCT Publications. All Rights Reserved

[10] J. Magiera, “A multi-antenna scheme for early detection and mitigation of intermediate GNSS spoofing,” Sensors, vol. 19, no. 10, Art. no. 2411, 2019, doi: 10.3390/s19102411.
[11] J. R. van der Merwe, A. Rügamer, and W. Felber, “Blind spoofing GNSS constellation detection using a multi-antenna snapshot receiver,” Sensors, vol. 19, Art. no. 5439, 2019.
[12] Ç. Tanıl, S. Khanafseh, M. Joerger, and B. Pervan, “Kalman filter-based INS monitor to detect GNSS spoofers capable of tracking aircraft position,” in Proc. IEEE/ION Position, Location and Navigation Symp. (PLANS), 2016.
[13] Ç. Tanıl, S. Khanafseh, M. Joerger, and B. Pervan, “An INS monitor to detect GNSS spoofers capable of tracking vehicle position,” IEEE Trans. Aerosp. Electron. Syst., vol. 54, no. 1, pp. 131–143, Feb. 2018.
[14] M. Varshosaz, A. R. Afary, B. Mojaradi, M. Saadatseresht, and E. Ghanbari Parmehr, “Spoofing detection of civilian UAVs using visual odometry,” ISPRS Int. J. Geo-Inf., vol. 9, no. 1, Art. no. 6, 2020, doi: 10.3390/ijgi9010006.
[15] N. Gu, F. Xing, and Z. You, “GNSS spoofing detection based on coupled visual/inertial/GNSS navigation system,” Sensors, vol. 21, no. 20, Art. no. 6769, 2021, doi: 10.3390/s21206769.
[16] J. Noh, Y. Kwon, Y. Son, H. Shin, D. Kim, J. Choi, and Y. Kim, “Tractor Beam: Safe-hijacking of consumer drones with adaptive GPS spoofing,” ACM Trans. Priv. Secur., vol. 22, no. 2, Art. no. 12, Apr. 2019.
[17] H. Sathaye, M. Strohmeier, V. Lenders, and A. Ranganathan, “An experimental study of GPS spoofing and takeover attacks on UAVs,” in Proc. 31st USENIX Security Symp., 2022, pp. 3503–3520.
[18] O. Jullian et al., “Deep learning detection of GPS spoofing,” in Machine Learning, Optimization, and Data Science (LOD 2021), Springer, 2022, pp. 527–540, doi: 10.1007/978-3-030-95467-3_38.
[19] S. Bi, K. Li, S. Hu, W. Ni, C. Wang, and X. Wang, “Detection and mitigation of position spoofing attacks on cooperative UAV swarm formations,” IEEE Trans. Inf. Forensics Security, vol. 19, pp. 1883–1895, 2024.
[20] Y. Dang, C. Benzaïd, B. Yang, T. Taleb, and Y. Shen, “Deep-ensemble-learning-based GPS spoofing detection for cellular-connected UAVs,” IEEE Internet Things J., vol. 9, no. 24, pp. 25068–25085, Dec. 2022, doi: 10.1109/JIOT.2022.3195320.
[21] Y. Dang, C. Benzaïd, T. Taleb, B. Yang, and Y. Shen, “Transfer learning based GPS spoofing detection for cellular-connected UAVs,” in Proc. Int. Wireless Commun. and Mobile Computing Conf. (IWCMC), 2022, pp. 629–634, doi: 10.1109/IWCMC55113.2022.9824124.
[22] “Brussels View: Galileo to transmit Open Service authentication,” Inside GNSS. [Online]. Available: https://insidegnss.com/brussels-view-galileo-to-transmit-open-service-authentication/
[23] K. A. Pant, L.-Y. Lin, J. Kim, W. Sribunma, J. M. Goppert, and I. Hwang, “MIXED-SENSE: A mixed reality sensor emulation framework for test and evaluation of UAVs against false data injection attacks,” arXiv:2407.09342, Jul. 2024.
[24] D. She, W. Wang, J. Wang, et al., “Collaborative detection method of UAV GPS spoofing attack based on shrink autoencoder,” J. Signal Process., vol. 40, no. 4, pp. 706–718, 2024, doi: 10.16798/j.issn.1003-0530.2024.04.009.
[25] P. Kairouz et al., “Advances and open problems in federated learning,” Found. Trends Mach. Learn., 2021.
[26] S. Hafeez, A. R. Khan, M. M. Al-Quraan, L. Mohjazi, et al., “Blockchain-assisted UAV communication systems: A comprehensive survey,” IEEE Open J. Veh. Technol., 2023, doi: 10.1109/OJVT.2023.3295208.
[27] B. Kujur, S. Khanafseh, and B. Pervan, “Optimal INS monitor for GNSS spoofer tracking error detection,” NAVIGATION, vol. 71, no. 1, 2024, doi: 10.33012/navi.629.
[28] M. Castro and B. Liskov, “Practical Byzantine fault tolerance,” in Proc. OSDI, 1999.

 Copyright © 2026. JCT Publications. All Rights Reserved