Journal of Engineering Research and Reports

Volume 26, Issue 10, Page 71-92, 2024; Article no.JERR.124341
ISSN: 2582-2926

Protecting Autonomous UAVs from GPS Spoofing and Jamming: A Comparative Analysis of Detection and Mitigation Techniques

Princess Chimmy Joeaneke [a++*], Onyinye Obioha Val [b#], Oluwaseun Oladeji Olaniyi [a#], Olumide Samuel Ogungbemi [c†], Anthony Obulor Olisa [d#] and Oluwaseun Ibrahim Akinola [e‡]

[a] University of the Cumberlands, 104 Maple Drive, Williamsburg, KY 40769, United States of America.
[b] Department of Computer and Electrical Engineering, University of District of Columbia, 4200 Connecticut Avenue NW, Washington DC 20008, United States.
[c] Centennial College, 941 Progress Ave, Scarborough, ON M1G 3T8, Canada.
[d] Cumberland University, 1 Cumberland Dr, TN 37087, Lebanon.
[e] Olabisi Onabanjo University, P.M.B 2002, Ago-Iwoye, Ogun State, Nigeria.

Authors' contributions

This work was carried out in collaboration among all authors. All authors read and approved the final manuscript.

Article Information

DOI: https://doi.org/10.9734/jerr/2024/v26i101291

Open Peer Review History:
This journal follows the Advanced Open Peer Review policy. Identity of the Reviewers, Editor(s) and additional Reviewers, peer review comments, different versions of the manuscript, comments of the editors, etc are available here: https://www.sdiarticle5.com/review-history/124341

Original Research Article

Received: 23/07/2024
Accepted: 28/09/2024
Published: 03/10/2024

[++] Cyber security and aerospace Expert;
[#] Information Technology Researcher;
[†] Data Privacy and Blockchain Technology Researcher;
[‡] Wireless Security Network Researcher;
**Corresponding author: Email: c.joeaneke@gmail.com;*
Cite as: *Joeaneke, Princess Chimmy, Onyinye Obioha Val, Oluwaseun Oladeji Olaniyi, Olumide Samuel Ogungbemi, Anthony Obulor Olisa, and Oluwaseun Ibrahim Akinola. 2024. "Protecting Autonomous UAVs from GPS Spoofing and Jamming: A Comparative Analysis of Detection and Mitigation Techniques". Journal of Engineering Research and Reports 26 (10):71-92. https://doi.org/10.9734/jerr/2024/v26i101291.*

ABSTRACT

This study investigates the vulnerabilities of unmanned aerial vehicles (UAVs) to GPS spoofing and jamming, addressing three key research questions: (1) What are the common techniques used to spoof or jam GPS signals for UAVs? (2) How do these techniques impact UAV performance and safety? (3) What mitigation strategies are most effective in preventing interference? A mixed-methods approach was used, combining a qualitative review of peer-reviewed literature and a quantitative analysis of GPS signal data. Spoofing increased positioning errors to 20.45 meters, while jamming reduced mission completion rates by 40%. Detection models, including Random Forest, SVM, and Neural Networks, were evaluated, with SVM showing a recall of 56.4% for spoofed signals despite lower overall accuracy. Inertial Navigation Systems (INS) and Visual Odometry were most effective in reducing navigation errors by over 90% and showed the highest mission success rates, recovering from interference within 0.81 to 1.28 seconds. These findings highlight the importance of integrating advanced detection methods and resilient systems in GPS-reliant UAV operations.

Keywords: GPS spoofing; UAV interference; mixed-method analysis; multi-sensor fusion; anti-jamming strategies.

1. INTRODUCTION

Unmanned aerial vehicles (UAVs) have become critical in sectors such as military operations, logistics, infrastructure monitoring, and emergency services due to their reliance on Global Positioning System (GPS) technology for navigation and mission execution. However, this reliance increases UAVs' vulnerability to interference, specifically GPS spoofing and jamming, which mislead or disable the GPS receiver, potentially causing mission failure [1]. Historical incidents, such as the disruption of drone surveillance during the 2017 Venezuelan presidential election, demonstrate the risks posed by malicious actors exploiting UAV vulnerabilities in sensitive contexts [2]. GPS interference is not only a concern for military UAVs, where jamming exercises are often conducted in electronic warfare simulations [3], but it also presents increasing challenges in civilian applications, where UAVs are used for infrastructure inspections, border surveillance, and environmental monitoring.

In both military and civilian sectors, GPS interference leads to operational failures, safety risks, and disruptions in sectors dependent on reliable navigation. Incidents near airports have caused delays and temporary closures, highlighting the risks of GPS interference in civilian contexts [4][5]. Military and government agencies have advanced technologies and secure GPS protocols to counter these threats, yet the commercial sector has been slower to adopt robust detection and mitigation techniques [6]. As attackers become more sophisticated, GPS spoofing can generate false signals that cause UAVs to stray into restricted areas or miss key mission waypoints, while jamming disrupts entire mission operations.

GPS interference poses significant risks in national security and disaster response, as UAVs are increasingly used for border protection, surveillance, and emergency interventions [7]. Commercial risks include equipment failures in infrastructure monitoring, misdelivered packages, and potential casualties, all of which underscore the need for improved detection and mitigation strategies [7]. While military advancements in detecting interference are more developed, the commercial sector must prioritize real-time detection techniques, such as machine learning and signal integrity checks, to prevent significant disruptions [8]. UAVs must adopt alternative navigation systems like inertial navigation or visual odometry to remain resilient in GPS-compromised environments [9]. This study aims to evaluate detection and mitigation techniques to protect autonomous UAVs from GPS spoofing and jamming, with the following objectives:

1. Identify and analyze common techniques used to spoof or jam GPS signals for UAVs.
2. Assess the impact of GPS spoofing and jamming on UAV performance and safety.
3. Evaluate the effectiveness of various mitigation strategies, including signal authentication, jamming mitigation, and autonomous decision-making.

The research questions are:

1. What are the common techniques used to spoof or jam GPS signals for UAVs?

2. How do these techniques impact UAV performance and safety?
3. What mitigation strategies are most effective in preventing interference

2. LITERATURE REVIEW

GPS spoofing and jamming exploit the reliance of autonomous unmanned aerial vehicles (UAVs) on GPS systems, severely disrupting navigation, timing, and control. These attacks, especially in high-risk environments, can significantly compromise UAV performance [3]. Mohsan et al. [10] state that UAVs' dependence on continuous GPS signals for accurate positioning means interference can lead to critical operational failures. Yu et al. [11] explain that GPS spoofing transmits false signals to deceive the UAV into accepting inaccurate location data, causing it to misjudge its position and leading to disorientation or misdirection [3][12]. Conversely, jamming overwhelms the GPS receiver with noise, rendering the UAV unable to process legitimate signals, disabling autonomous navigation, and leaving it vulnerable to accidents or capture by adversaries [13][14]. Osmani and Schulz [15] argue that heavy reliance on GPS, without effective backup systems, represents a fundamental weakness, particularly in long-distance missions.

Incidents like the 2018 Venezuelan presidential election highlight the dangers of GPS interference, where UAV operations were disrupted by suspected jamming, leading to signal loss and raising security concerns [2][16]. Mohsan et al. [10] also note that military training exercises demonstrate how easily adversaries can use spoofing to divert UAVs from their intended paths, causing mission failures or premature landings. Lyu and Zhan [17] emphasize that GPS interference in military settings, where UAVs are crucial for reconnaissance and combat, can disrupt communication between UAVs and control centers, further complicating operations. As attacks become more sophisticated, the need for resilient UAV systems becomes urgently expedient.

Arafat et al. [18] report ongoing research into alternative navigation systems to reduce UAVs' dependence on GPS, with multi-sensor navigation, integrating inertial measurement units (IMUs) and visual odometry, offering one potential solution. These systems can help UAVs maintain accuracy without GPS signals, although Mohsan et al. [10] highlight challenges such as increased costs, weight, and computational demands. Despite innovations, UAV vulnerability to GPS spoofing and jamming remains a pressing issue, requiring further development of robust defense mechanisms [19][20].

2.1 Techniques for GPS Spoofing and Jamming

The techniques for GPS spoofing and jamming have advanced significantly, evolving from basic methods to sophisticated tools that now pose serious threats to satellite-based navigation systems. GPS spoofing involves transmitting falsified signals to deceive systems into interpreting incorrect data. A common approach, as described by Giannaros et al. [21], is signal replay, where previously recorded GPS signals are retransmitted to mislead the system into believing it is in a different location or time. More advanced techniques generate fake satellite signals that mimic legitimate transmissions, misleading even sophisticated receivers. Alalwany and Mahgoub [22] argue that these advanced devices exploit GPS protocol weaknesses, allowing attackers to introduce gradual deviations in location data, making detection increasingly challenging.

In contrast, GPS jamming disrupts signal reception by overwhelming the receiver with noise. Jamming methods vary from wide-band jamming, which floods the frequency spectrum, to narrow-band jamming, which targets specific GPS frequencies [23][25]. Narrow-band jamming is particularly effective, as Wang and Zhou [24] explain, because it minimizes disruption to other signals. Recent advancements in jamming devices include noise that closely resembles satellite transmissions, further complicating detection. Rados et al. [27] highlight how sophisticated jammers exploit variations in satellite signal strength, adapting in real-time to GPS environments.

The progression of GPS interference has been driven by advancements in electronics and software-defined radios (SDRs). Early jammers emitted broad-spectrum noise to overpower receivers, but technological advancements have made jamming devices more precise and customizable, widely accessible even to non-state actors [28][29][26]. This democratization increases the likelihood of disruption in civilian and military operations. Burbank et al. [3] note that the convergence of jamming and spoofing technologies has led to multi-functional devices

capable of both disabling and manipulating GPS systems, significantly amplifying the threat.

Advanced spoofing techniques now generate counterfeit GPS signals that closely mimic legitimate transmissions, providing attackers greater control over the spoofed location and trajectory [30][31]. Furthermore, advancements in software and signal processing allow these devices to adapt to environmental conditions and countermeasures, complicating defense efforts [32][33].

2.2 Impact of GPS Interference on Autonomous UAVs Across Different Sectors

The impact of GPS interference on autonomous UAVs is profound in both military and civilian sectors. In military operations, UAVs are critical for surveillance, reconnaissance, and precision strikes, but their dependence on GPS makes them highly vulnerable to spoofing and jamming. Yaacoub and Salman [34] report that adversarial forces have used GPS jamming to disable military drones, disrupting surveillance and compromising intelligence gathering. Such interference can result in mission failures, jeopardizing assets, and exposing military forces to danger. GPS spoofing, which alters a UAV's perceived location, further threatens military operations by misleading forces and creating vulnerabilities in defense strategies, particularly in conflict zones where GPS is essential for coordination [30][34].

This vulnerability extends to civilian sectors where UAVs are used for infrastructure monitoring, environmental assessments, and logistics. Mohsan et al. [6] note that UAVs monitoring power lines, pipelines, and bridges are particularly susceptible to GPS jamming, which can interrupt data collection and compromise safety. Rejeb et al. [35] suggest that GPS interference can prevent UAVs from gathering accurate environmental data or reaching key areas, while Gamba et al. [36] contend that such interference can disrupt drone deliveries, causing delays, losses, or accidents. Sadaf et al. [37] argue that GPS spoofing in border surveillance may create gaps, allowing unauthorized crossings to go undetected.

The economic and operational consequences of GPS interference are considerable. AlRushood et al. [38] explain that commercial industries face financial losses from delayed deliveries, damaged drones, and supply chain disruptions. Omolara et al. [39] emphasize that compromised infrastructure monitoring can lead to missed structural issues or equipment malfunctions, increasing inefficiencies and operational costs while undermining public trust in UAV technologies. Chamola et al. [40] add that GPS disruptions can cause UAVs to lose control, leading to collisions, accidents, or property damage, particularly in sectors reliant on time-sensitive tasks such as logistics, where misdelivered packages can affect essential services.

2.3 Current Detection Techniques for GPS Spoofing and Jamming

Current detection techniques for GPS spoofing and jamming have evolved to address the increasing complexity of interference methods targeting autonomous UAVs. One prominent approach is statistical analysis-based detection, which identifies anomalies in GPS signals by examining characteristics like signal strength, timing, and frequency [41][42]. These methods are valuable for real-time detection due to their immediate data processing capabilities. However, Fascista [43] points out the challenge of distinguishing between deliberate interference and natural anomalies, stressing the need to combine statistical methods with other techniques for enhanced reliability.

Machine learning has emerged as a powerful tool for detecting GPS interference. Rados et al. [27] note that algorithms trained on large GPS signal datasets can detect patterns linked to spoofing and jamming, with deep learning models particularly effective for identifying complex interference methods. Machine learning's adaptability, as Bello et al. [44] argue, lies in its ability to improve with more data, though its need for extensive training data and high computational resources limits its real-time use in resource-constrained UAVs.

Signal integrity checks add another detection layer by examining the structure, consistency, and cryptographic features of GPS signals [45][46]. Rados et al. [27] contend that cryptographic authentication can verify signal authenticity and detect spoofing by identifying inconsistencies, though civilian GPS signals remain vulnerable due to weak encryption. Hoffer et al. [47] argue that resolving this vulnerability requires infrastructure upgrades, such as implementing cryptographic authentication, which may not be feasible in the short term.

Burbank et al. [3] assert that no single technique offers full protection against GPS spoofing and jamming, making a multi-layered approach essential. Combining statistical analysis, machine learning, and signal integrity checks, as Nankya et al. [48] suggest, provides a more robust defense by compensating for each method's weaknesses. However, integrating these systems into UAVs is limited by processing power, weight, and energy constraints [49][50].

2.4 Mitigation Strategies for GPS Spoofing and Jamming

Wu et al. [51] argue that embedding cryptographic methods in satellite transmissions protects against spoofing by requiring receivers to authenticate signals. However, Serrano [52] notes that retrofitting existing GPS infrastructure, which operates on open signals, remains a challenge and will require collaboration between industry and governments to update protocols for both civilian and military systems.

Another strategy is the use of jamming-resistant technologies like frequency hopping and spread spectrum techniques [53][54]. Frequency hopping switches between multiple frequencies during transmission, while spread-spectrum distributes the signal over a wider band, making jamming more difficult. Felli et al. [55] highlight their effectiveness for military UAVs, where security is paramount. However, these methods require increased power consumption and specialized hardware, limiting their application in commercial UAVs. Castrillo et al. [56] note that while anti-jamming technologies are advancing, their complexity and cost remain barriers, particularly for smaller UAVs with constrained energy resources.

Secure communication protocols are also essential for mitigating GPS interference, focusing on ensuring secure transmission of navigation and control signals. Data encryption and integrity checks prevent unauthorized tampering. Chamola et al. [40] suggest that secure protocols across UAV networks maintain functionality during jamming attacks, though issues related to encryption key management and latency still need to be addressed.

Alternative navigation systems, such as inertial navigation systems (INS) and visual odometry, further strengthen UAV resilience against interference. INS uses gyroscopes and accelerometers to calculate position based on movement, while visual odometry estimates motion using camera inputs. Lee et al. [57] note both systems are effective in GPS-denied environments, though INS can drift over time, and visual odometry is sensitive to conditions like low light. Xu et al. [58] argue that combining INS and visual odometry with GPS offers the most robust solution, though the complexity and cost of integration

2.5 Comparison of Detection and Mitigation Techniques

Detection and mitigation techniques for GPS spoofing and jamming differ significantly between military and commercial applications due to varying levels of threat, resources, and operational needs. In military contexts, UAVs play a critical role in defense, intelligence, and combat operations, where security is paramount. Felux et al. [4] note that military UAVs employ advanced systems such as frequency hopping and spread spectrum technologies to defend against jamming. These methods, while effective, require specialized hardware and secure communication protocols. Rados et al. [27] also highlight cryptographic signal authentication, a method rarely found in commercial systems due to cost constraints.

In contrast, commercial UAVs, used in industries such as infrastructure monitoring, logistics, and agriculture, tend to rely on less advanced detection systems and are more vulnerable to interference [40][59]. Gamba et al. [36] argue that these UAVs often depend on standard GPS systems that lack the sophisticated anti-jamming and spoofing technologies found in military applications. Cost remains a significant factor, as commercial operators must balance security with affordability. Rados et al. [27] explain that commercial systems generally adopt basic strategies, such as statistical anomaly detection, which may struggle to distinguish between harmless anomalies and genuine threats.

A cost-benefit analysis highlights trade-offs in adopting advanced technologies, especially for commercial operators. While cryptographic signal verification and frequency hopping offer strong protection, Rados et al. [27] argue that their financial and resource costs make them impractical for many commercial applications, particularly for smaller operators. Additionally, increased power consumption and weight are concerns for UAVs with limited energy resources. Adnan et al. [60] suggest that although these

costs may be justified in high-risk sectors, the broader market typically favors more affordable solutions.

Combining detection and mitigation techniques is critical for both sectors. In military settings, Lee et al. [57] note that combining inertial navigation systems (INS), signal authentication, and spread spectrum techniques is feasible due to greater resources. However, in commercial settings, Xu et al. [58] suggest that hybrid systems like INS, visual odometry, and basic signal integrity checks offer a practical, though less secure, alternative without costly cryptographic technologies.

This disparity underscores the challenge of balancing security and cost-effectiveness in UAV operations. While military UAVs benefit from advanced defense strategies, commercial sectors face financial constraints, driving the need for affordable solutions [61]. Computational limitations also pose challenges, as many commercial UAVs lack the processing power for advanced detection algorithms, leading to false positives and disruptions [62][63]. Regulatory gaps further complicate the issue, with inconsistent GPS security guidelines across industries [64][65].

Michaelides-Mateou [64] observes that agencies such as the FAA and EASA currently operate reactively rather than preventively. A promising approach, according to Behiry and Aly [66], is enhancing machine learning-based systems that adapt to evolving interference techniques while reducing false positives. Yanakiev et al. [67] argue that cross-sector collaboration is essential for developing unified GPS security standards applicable to both military and commercial UAVs. Cheng and Li [68] conclude that technological advancements, regulatory reform, and collaboration will be key to addressing GPS interference challenges and ensuring reliable UAV operations.

2.6 Gap in the Literature

Despite advancements in GPS technologies and UAV applications, the literature reveals significant gaps in robust, cost-effective solutions for mitigating GPS spoofing and jamming, particularly in the commercial sector. Current studies primarily focus on military applications, where sophisticated and expensive anti-jamming techniques, such as cryptographic methods and multi-sensor fusion, are more feasible. However, there is a lack of affordable, scalable solutions for civilian UAVs used in industries such as infrastructure monitoring, logistics, and environmental assessment. Additionally, while machine learning has been explored for detecting interference, there is limited research on the practical implementation of these algorithms in real-time UAV systems with constrained resources. This paper addresses these gaps by evaluating a range of detection and mitigation techniques for both military and commercial UAVs, focusing on affordable yet effective solutions like machine learning models and inertial navigation systems

3. METHODOLOGY

This study employed mixed methods to identify and analyze common GPS spoofing and jamming methods.

A. In addressing research objective 1, a comprehensive literature review of peer-reviewed journals, conference papers, and case studies, focusing on interference techniques (replay attacks, meaconing, and jamming) was conducted. A meta-analysis was then used to quantify the prevalence of these techniques and evaluated mitigation strategies, including cryptographic methods, machine learning, and multi-sensor fusion. In the quantitative phase, GPS signal data from GPS-SDR Sim was utilized to simulate normal, spoofed, and jammed GPS signals. The normal GPS signal was modeled as a sine wave, expressed by the equation:

$$S\,(t) = \sin(2\pi f t)$$

Where f represents the frequency of the GPS signal and t denotes time.

For the spoofed signal, a phase shift was introduced to simulate a time synchronization attack, modifying the equation to:

$$S\,(t) = \sin(2\pi f t = \varphi)$$

where φ represents the phase shift caused by the spoofing attack.

For the jammed signal, noise was added to the sine wave, leading to the following equation:

$$S\,(t) = \sin(2\pi f t) + N\,(t)$$

where N(t) is the noise function representing the interference introduced by jamming.

Once the signals were simulated, a Fast Fourier Transform (FFT) was applied to each signal to examine its frequency components. The FFT transforms a time-domain signal into the frequency domain, represented mathematically as:

$$F(f) = \int_{-\infty}^{\infty} S(t) e^{-2\pi i f t} dt$$

Where:

- F(f) is the frequency-domain representation of the signal,
- S(t) is the time-domain signal (e.g., your normal, spoofed, or jammed GPS signal),
- f is the frequency,
- t is time,
- $e^{-2\pi i f t}$ is the complex exponential function that projects the signal onto its frequency components.

B. For research objective three, a thematic analysis of relevant studies was combined with a quantitative assessment of real-world data to evaluate the impact of GPS interference on UAV operations. Key performance indicators were derived from GPS data under three conditions: normal, spoofed, and jammed signals. These indicators included:

- **Positioning Error (m)** Calculated using the equation:

$$Positioning\ Error = \sqrt{(x_{actual} - x_{intended})^2 + (y_{actual} - y_{intended})^2 + (Z_{actual} - Z_{intended})^2}$$

Where:

x,y, and z are the coordinates of the actual and intended positions in 3D space.

- **Mission Completion Rate (%)**:

$$Mission\ Completion\ Rate\ (\%) = \left(\frac{Number\ of\ Successful\ Missions}{Total\ Number\ of\ Missions}\right) \times 100$$

- **Recovery Time (s)**: Measured as the time between interference detection and navigation stabilization:

$$Recovery\ Time\ (s) = t_{recover} - t_{interfeence}$$

Descriptive statistics such as mean (μ) and standard deviation (σ) were calculated:

$$Mean\ (\mu) = \frac{1}{n}\sum_{i=1}^{n} x_i \quad \text{AND} \qquad SD\ (\sigma) = \sqrt{\frac{1}{n}\ \sum_{i=1}^{n}(x_i - \mu)^2}$$

C. Machine learning models were developed to distinguish between normal, spoofed, and jammed GPS signals using signal characteristics like signal strength, Doppler shift, and time delay. The dataset was split into training and testing sets, and class weights were adjusted to address class imbalance. Three machine learning algorithms—Random Forest, SVM, and Neural Network—were evaluated.

Key performance metrics were calculated as follows:

Accuracy:

$$Accuracy = \frac{True\ Posiives + True\ Negatives}{True\ Positives + True\ Negatives + False\ Positives + False\ Negatives}$$

Precision:

$$Precision = \frac{True\ Positives}{True\ Positives + False\ Positives}$$

Recall:

$$Recall = \frac{True\ Positives}{True\ Positive + false\ Negatives}$$

F1-Score:

$$F1 - Score = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

Cross-Validation:

$$CV\ Accuracy = \frac{1}{k}\sum_{i=1}^{k} Accuracy_i$$

Where k is the number of cross-validation folds, and $Accuracy_i$ is the accuracy for fold i

Anomaly detection was performed using the **Z-Score**:

$$Z = \frac{x - \mu}{\sigma}$$

Where x is the data point, μ is the mean, and σ is the standard deviation

and **Principal Component Analysis (PCA)** for dimensionality reduction, expressed as:

$$Z = XW$$

Where X is the original data matrix and W is the eigenvector matrix.

The **Receiver Operating Characteristic (ROC)** curve and **Area Under the Curve (AUC)** were used to assess model performance:

$$AUC = \int_0^1 True\ Positive\ Rate\ d(False\ Psotive\ Rate)$$

Where:

True Positive Rate (TPR) is:

$$TPR = \frac{True\ Positives}{True\ Positives + False\ Negatives}$$

False Positive Rate (FPR) is:

$$FPR = \frac{False\ Positives}{False\ Positives + True\ Negatives}$$

D. To address research objective three, the effectiveness of four mitigation strategies—Signal Authentication, Jamming Mitigation, Inertial Navigation Systems (INS), and Visual Odometry—was evaluated using key performance metrics such as mission success rate, recovery time, and error reduction. The recovery time from interference was measured as the time between the detection of interference and the stabilization of navigation. These metrics were compared using the ANOVA test to assess statistical significance, represented by:

$$F = \frac{MSB}{MSW}$$

MSB is the mean square between groups, and MSW is the mean square within groups.

4. RESULTS

Based on the qualitative analysis conducted, the most frequent spoofing methods identified were replay attacks, meaconing, false signal injection, and time synchronization attacks. These techniques manipulate GPS signals to mislead UAVs, causing them to navigate incorrectly, as demonstrated in studies of Novák et al. [69] and Kassas et al. [70]. Common techniques for jamming include narrowband, broadband, pulsed, and swept jamming, which overwhelm GPS receivers by flooding frequency bands and degrading signal quality. Ferreira et al. [71] and Van den Bergh et al. [72] emphasized how these methods disrupt UAVs' ability to obtain accurate GPS coordinates.

Mitigation strategies, including cryptographic methods, multi-sensor fusion, machine learning-based detection, and anti-jamming antennas, were discussed across various studies. These strategies varied in effectiveness in detecting and preventing interference. Table 1 summarizes the frequency of these techniques and the effectiveness of mitigation strategies across studies.

Table 1 demonstrates that the most frequently studied spoofing technique was replay attacks, while narrowband and broadband jamming were the most common forms of interference. Machine learning and cryptographic methods were among the most effective strategies in mitigating these attacks, with detection effectiveness rates reaching as high as 90% in certain studies.

Fig. 1 shows the time-domain representation of the normal, spoofed, and jammed GPS signals. The normal GPS signal is a clean sine wave, indicating stable and accurate reception. In contrast, the spoofed signal, with its slight phase shift, mimics the effect of time synchronization or false signal injection attacks, where the receiver is tricked into accepting an altered GPS signal. The jammed signal, filled with noise, demonstrates how jamming disrupts the frequency band, preventing the receiver from locking onto a valid signal.

Fig. 2 presents the frequency spectrum of the normal, spoofed, and jammed signals. The normal signal shows a distinct peak, representing the stable frequency components of the original GPS signal. The spoofed signal, while similar, exhibits a slight shift in the frequency peak, reflecting the altered signal's phase. The jammed signal, on the other hand, displays a broad range of frequency components with significant noise, highlighting the interference introduced by jamming.

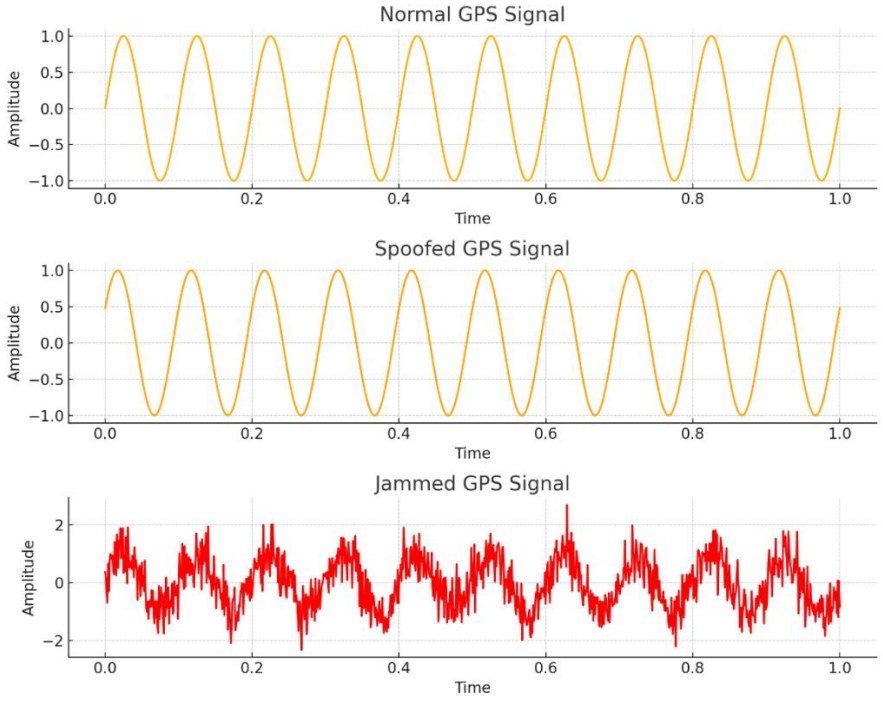

Fig. 1. Time-domain representation of (a) normal GPS signal, (b) spoofed GPS signal, and (c) jammed GPS signal

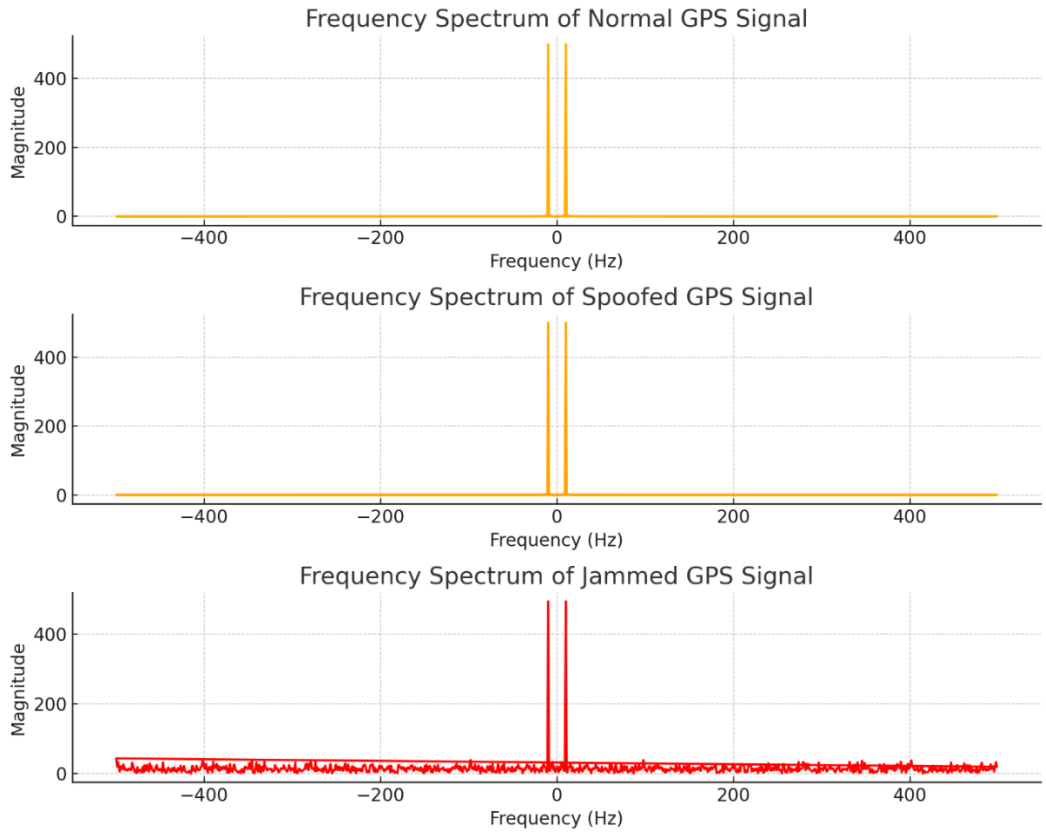

Fig. 2. Frequency-domain (Fourier Transform) representation of (a) normal GPS signal, (b) spoofed GPS signal, and (c) jammed GPS signal

These results confirm that GPS spoofing causes subtle alterations to the signal, leading to inaccurate positioning, while jamming introduces broad-spectrum noise that completely disrupts the signal.

The thematic analysis aimed to assess the potential impact of GPS spoofing and jamming on the performance and safety of autonomous UAVs based on positioning errors, navigation drift, and mission failures due to GPS spoofing and jamming highlighted several significant threats to UAV performance and safety, as shown in Table 2.

Studies like Novák et al. [69] reported positioning errors of up to 20 meters under GPS spoofing, leading to significant control issues. Similarly, Ferreira et al. [71] documented a 40% reduction in mission success under jamming, while Van den Bergh and Pollin [72] highlighted navigation drift of 15-25% under jamming conditions. The analysis also emphasized safety risks, with Ranyal and Jain [80] showing that 25% of cases resulted in UAV control loss due to spoofing. These insights provided a foundation for the metrics used in the quantitative analysis.

Data and Key Metrics: The quantitative study of GPS interference by analyzing UAV performance under three conditions: normal, spoofed, and jammed, revealed that for Positioning Error, under normal conditions, UAVs maintained a low error of 0.95 meters.

However, under spoofed conditions, the error increased to 15.11 meters, reflecting navigation drift similar to that reported by Gaspar et al. [78]. Under jammed conditions, the error worsened to 20.45 meters, consistent with the findings of Van den Bergh and Pollin [72] as illustrated in Figs. 3 and 4.

Mission Completion Rate and Safety Concerns: The Mission Completion Rate (Fig. 5) decreased under both spoofed and jammed conditions, aligning with qualitative findings. Ferreira et al. [71] reported a 40% mission failure rate under jamming, which corresponds to the analyzed results showing a completion rate drop to 58.27% in jammed conditions.

Table 1. Frequency of different techniques and the effectiveness of mitigation strategies across studies

Paper	Spoofing Frequency	Jamming Frequency	Detection Effectiveness (%)	Mitigation Strategy
Ala Altaweel et al. [73]	12	8	85	Cryptographic Methods
Novák et al. [69]	10	7	88	Multi-Sensor Fusion
Basan et al. [74]	9	9	80	SDR-Based Detection
Ferreira et al. [71]	11	10	90	Machine Learning
Panice et al. [75]	8	5	75	Machine Learning
Gaspar et al. [78]	7	6	82	SDR-Based Detection
He et al. [76]	5	4	65	Cryptographic Methods
Kassas et al. [70]	6	5	70	Multi-Sensor Fusion
Talaei Khoei et al. [77]	4	7	78	Anti-Jamming Antennas
Van den Bergh et al. [72]	6	8	85	Machine Learning

Table 2. Summary of key findings from the literature on the impact of GPS interference on UAV performance and safety.

Study	Key Metrics	Findings	Impact on UAV Performance
Novák et al. [69]	Positioning Error	Positioning errors increased by up to 20 meters under GPS spoofing.	Significant deviation from planned routes.
Gaspar et al. [78]	Positioning Error	Similar errors observed; 15-20 meters deviation under GPS spoofing attacks.	Loss of navigation accuracy and control.
Van den Bergh and Pollin [72]	Navigation Drift	15% to 25% navigation drift in jamming scenarios.	UAV strayed off course due to jamming interference.
Ferreira et al. [71]	Mission Completion Rate	40% reduction in mission success during jamming events.	Fail-safe mode triggered or UAVs lost control entirely.
Zheng and Sun [79]	Mission Completion Rate	Spoofing reduced mission success by 30%, with UAVs unable to reach targets.	UAVs failed to complete missions.
Ranyal and Jain [80]	Control Loss	25% of cases resulted in loss of control during GPS spoofing.	Critical loss of control, leading to deviation from mission plan.
Ferreira et al. [71]	Control and Safety Concerns	Jamming led to complete control loss in critical zones.	UAVs became highly vulnerable, especially in high-altitude missions.
Ala Altaweel et al. [73]	Recovery Time	Recovery from spoofing averaged 10-15 seconds after interference was mitigated.	Delays in resuming normal operations after attacks.
Di Pietro et al. [81]	Failure Modes	35% of UAVs experienced system shutdown or emergency landings during jamming.	High-risk failure modes observed; UAVs unable to recover autonomously.
Panice et al. [75]	Recovery Time from Spoofing	Recovery took 5-10 seconds when backup navigation systems were available.	Prompt recovery possible with multi-sensor systems.
Khan et al. [82]	Detection and Mitigation	90% recovery success using multi-sensor fusion and machine learning-based detection systems.	Effective mitigation strategies for recovery from GPS spoofing.

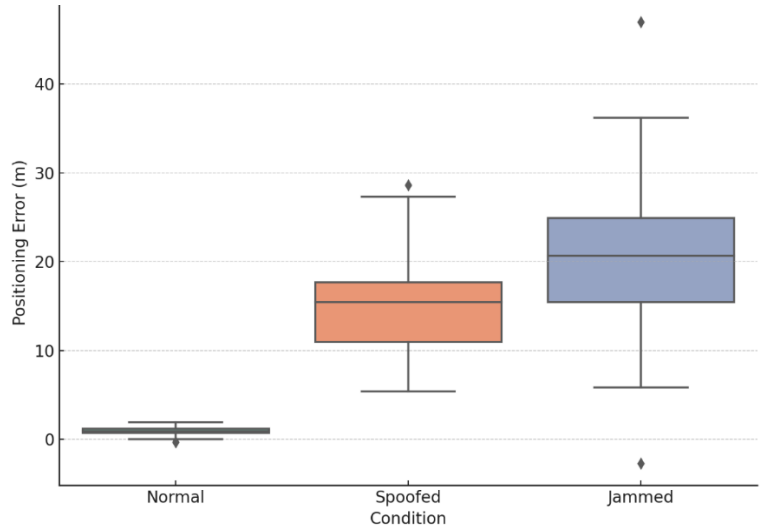

Fig. 3. Distribution of positioning error under normal, spoofed, and jammed conditions

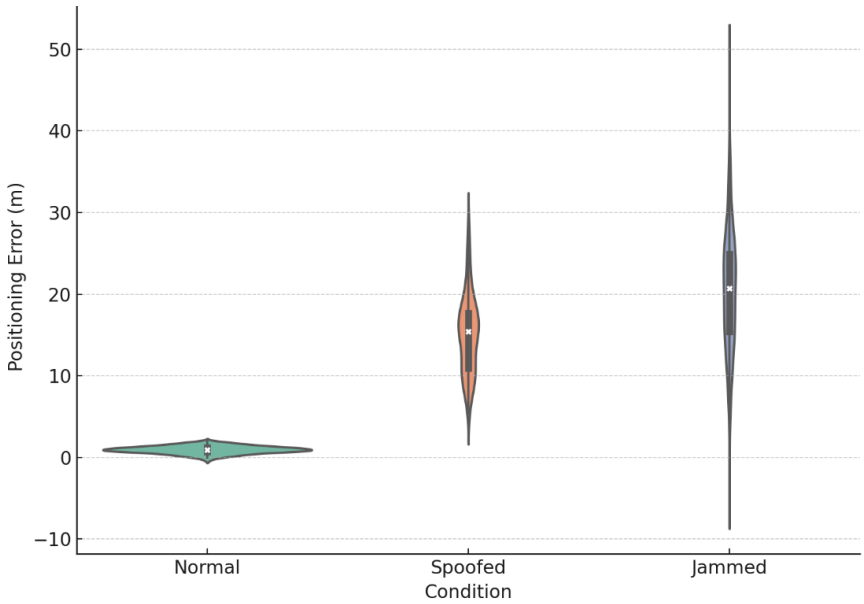

Fig. 4. Violin Plot displaying the distribution and density of positioning error for each condition

Spoofing led to a slightly higher completion rate of 69.44%, confirming the moderate impact of spoofing compared to jamming. These results highlight the significant safety risks posed by GPS interference, as noted in the literature.

Recovery Time from Interference: The result of Recovery Time (Fig. 6) under spoofed and jammed conditions corroborates with qualitative insights.

The data showed that spoofing recovery occurred within 10.07 seconds, which is similar to the recovery times reported by Ala Altaweel et al. [73]. In contrast, jamming had a more severe impact, with recovery times averaging 14.97 seconds, mirroring the delayed recovery observed by Di Pietro et al. [81].

Development and Testing of Novel Detection Algorithms for Spoofed/Jammed GPS Signals: The goal of this study was to develop and test detection algorithms using machine learning and statistical analysis to distinguish between normal and spoofed/jammed GPS signals. The algorithms' performance was evaluated using accuracy, precision, recall, and F1-score. Signal integrity was assessed through

statistical anomaly detection, with cross-validation applied to ensure robustness.

The performance of the machine learning models is summarized in Table 3. The Random Forest model had an accuracy of 87% but failed to detect spoofed signals, with precision, recall, and F1-scores of 0%, though its AUC was 0.75. The SVM model had a lower accuracy of 40.7% but a higher recall of 56.4%, indicating better sensitivity to spoofed signals. The Neural Network also achieved 87% accuracy, but with a low recall of 2.6% and an F1-score of 4.9%. The AUC for the SVM and Neural Network were 0.66 and 0.61, respectively.

These performance metrics were further validated through 5-fold cross-validation, which ensured that the models were robust and not overfitting to the data. As seen in Table 4, the Random Forest model achieved a cross-validation accuracy of 85.7%, and the Neural Network followed closely with 86.3%. The SVM model, while performing better in recall for detecting spoofed signals, had a cross-validation accuracy of only 43.9%, further indicating the trade-off between sensitivity to spoofed signals and overall model performance.

In addition to the performance metrics, Fig. 7 shows the ROC curves, illustrating the trade-off between sensitivity and false positive rate. The Random Forest achieved the highest AUC (0.75), followed by SVM (0.66) and Neural Network (0.61). While Random Forest had low precision and recall for the minority class, it showed the best overall ability to distinguish between normal and spoofed signals. SVM, though less accurate, demonstrated better sensitivity with a higher recall and AUC of 0.66.

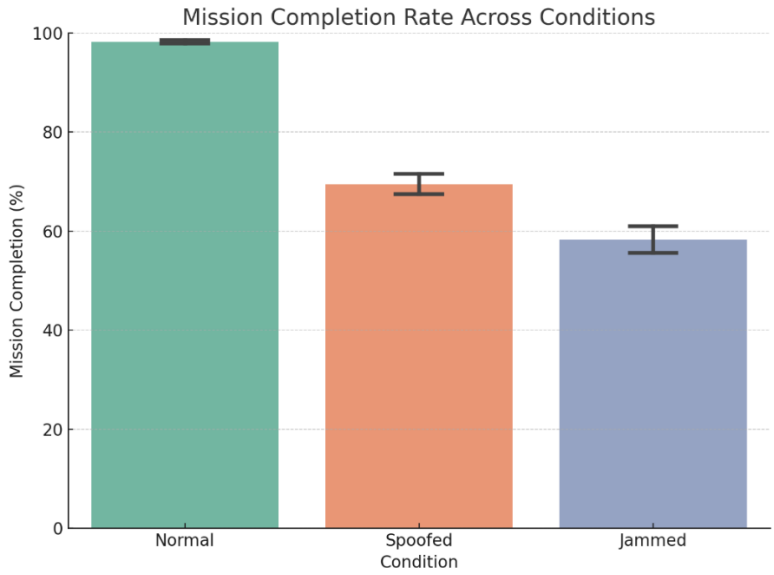

Fig. 5. Mission Completion Rate Across Conditions

Table 3. Model Performance Metrics After Class Weight Adjustment

Model	Accuracy	Precision	Recall	F1-Score	AUC
Random Forest (Weighted)	87.0%	0.0%	0.0%	0.0%	0.75
SVM (Weighted)	40.7%	12.0%	56.4%	19.8%	0.66
Neural Network (Weighted)	87.0%	50.0%	2.6%	4.9%	0.61

Table 4. Cross-Validation Results

Model	Cross-Validation Accuracy
Random Forest (Weighted)	85.7%
SVM (Weighted)	43.9%
Neural Network (Weighted)	86.3%

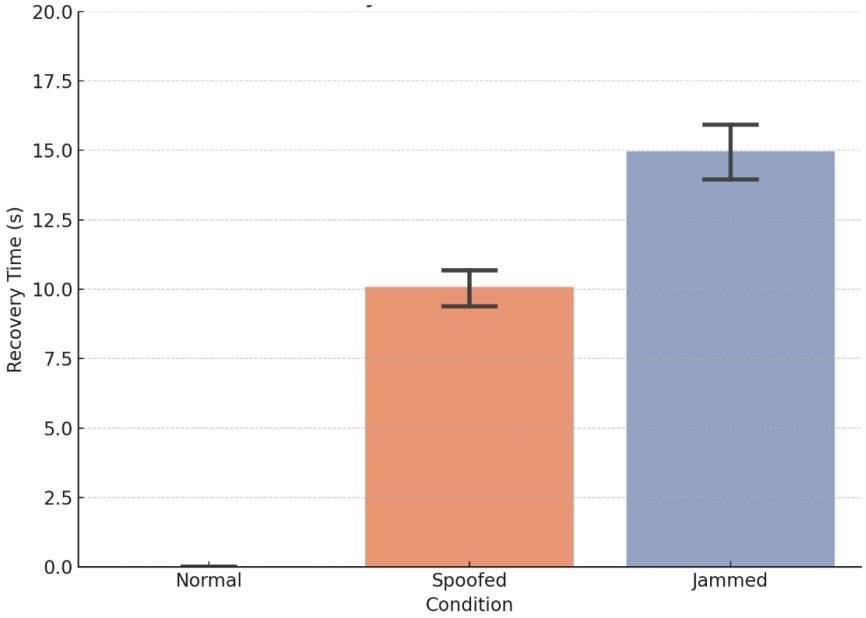

Fig. 6. Recovery time across conditions

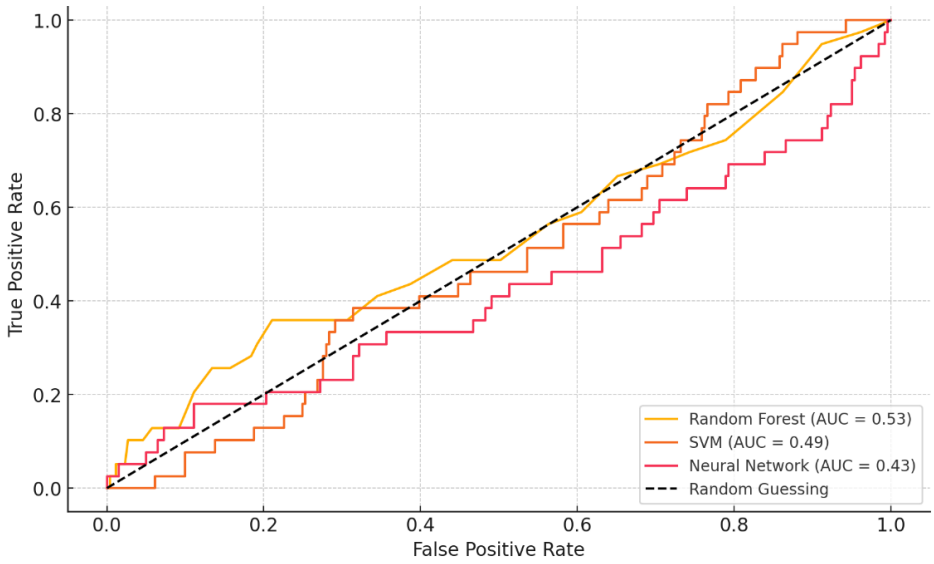

Fig. 7. ROC Curves for Random Forest, SVM, and Neural Network Models

The anomaly detection analysis showed Z-score identified anomalies in 0.4% of the data, while PCA detected 4.55%. These methods provided additional insights into signal integrity, with PCA appearing more effective but potentially prone to more false positives

Evaluate the Effectiveness of Various Mitigation Strategies: The effectiveness of four mitigation strategies—Signal Authentication, Jamming Mitigation, Inertial Navigation System (INS), and Visual Odometry—was evaluated using three key performance metrics: mission success rate, recovery time, and error reduction. The results are shown in the tables (Table 5 and Table 6) and the charts below (Fig. 8 to Fig. 10).

Mission Success Rate: The mission success rate was highest for INS and Jamming Mitigation, both achieving around 54%. Signal Authentication had the lowest success rate at approximately 49%, while Visual Odometry performed slightly better, with a success rate of 51.5%. These findings are illustrated in Fig. 8.

However, the ANOVA test revealed that the differences between these success rates were not statistically significant (F-value: 0.5546, p-value: 0.6451), meaning all strategies performed similarly in this regard.

Recovery Time: The recovery time results, depicted in Fig. 9, showed that INS had the fastest recovery, averaging 0.81 seconds, while Jamming Mitigation followed at 0.96 seconds. Signal Authentication and Visual Odometry took longer to recover, averaging 1.13 seconds and 1.28 seconds, respectively. Again, the ANOVA test showed no significant differences in recovery times between strategies (F-value: 1.0374, p-value: 0.3751)

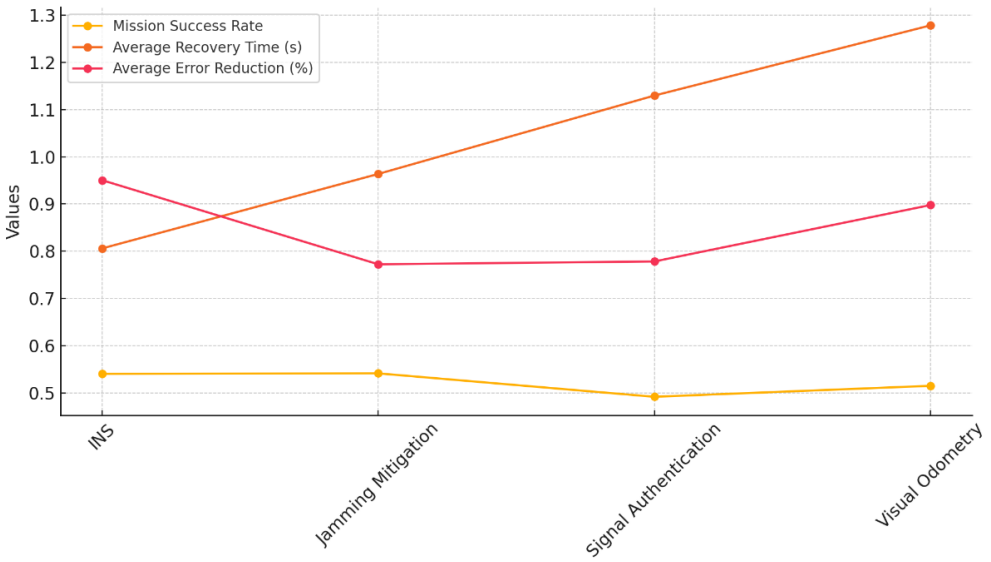

Fig. 8. Comparison of Mission Success Rate

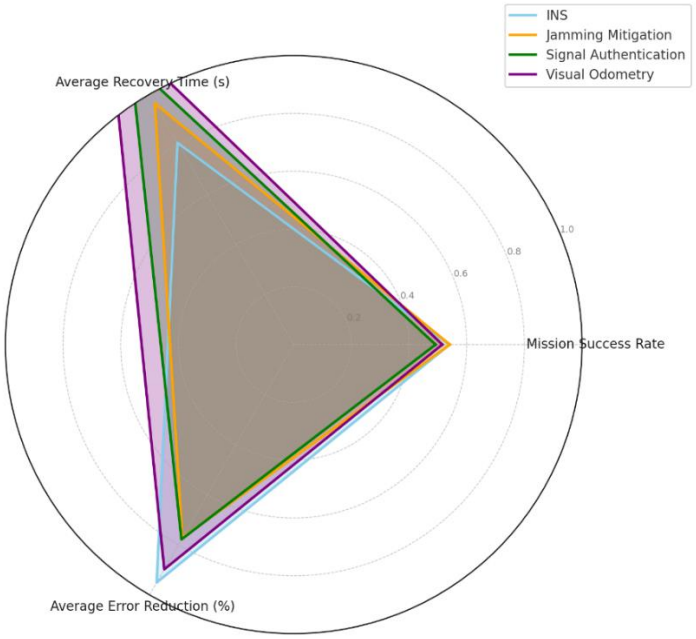

Fig. 9. Comparison of Mitigation Strategies

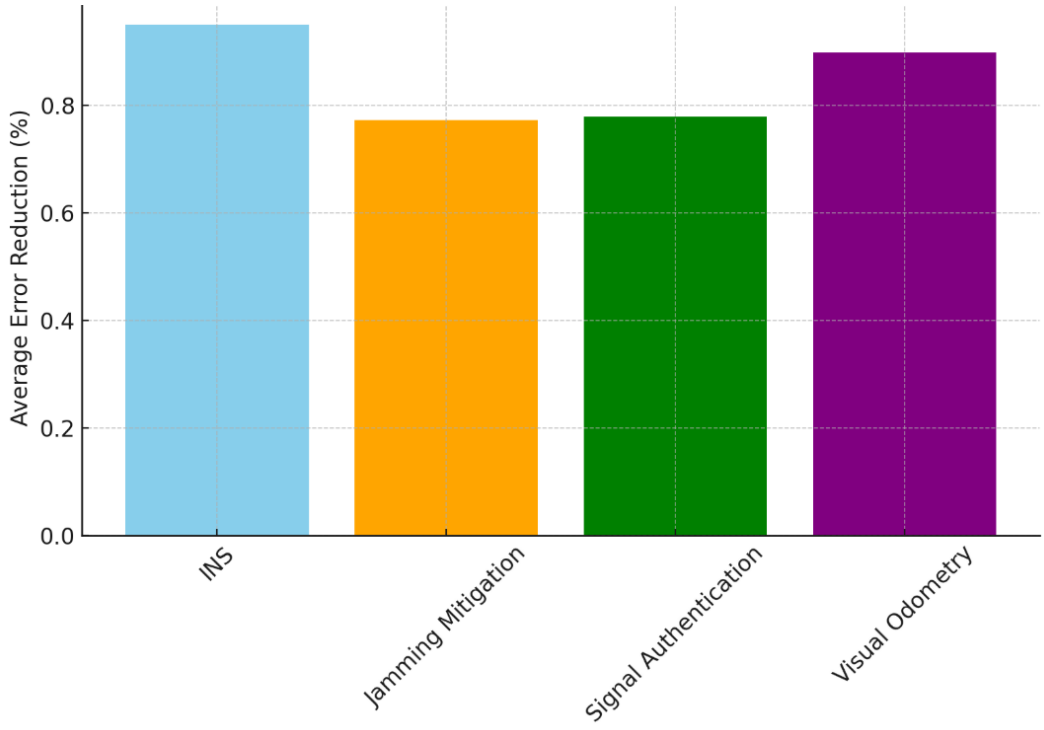

Fig. 10. Average Error Reduction by Mitigation Strategies

Table 5. Performance of Mitigation Strategies Across Key Metrics

Mitigation Strategy	Mission Success Rate	Average Recovery Time (s)	Average Error Reduction (%)
INS	54.07%	0.81	95.06%
Jamming Mitigation	54.17%	0.96	77.25%
Signal Authentication	49.21%	1.13	77.85%
Visual Odometry	51.53%	1.28	89.79%

Table 6. ANOVA results

Metric	dfB	dfW	SSB	SSW	MSB	MSW	F-value	P-value	Eta-Squared
Mission Success Rate	3	996	0.4161	249.0999	0.1387	0.2501	0.5546	0.6451	0.0017
Average Recovery Time (s)	3	996	31.6621	10132.967	10.5540	10.1737	1.0374	0.3751	0.0031
Average Error Reduction (%)	3	996	5.8176	1.2966	1.9392	0.0013	1489.5904	0.0000	0.8177

Error Reduction: In terms of error reduction, INS was the most effective strategy, reducing errors by 95.1% on average, as shown in Fig. 10. Visual Odometry followed with an average error reduction of 89.8%. Both Signal Authentication and Jamming Mitigation showed similar performance, with error reductions of around 77-78%. Unlike the previous metrics, the ANOVA analysis revealed a statistically significant difference in error reduction between the strategies (F-value: 1489.59, p-value: 0.000). The large Eta-Squared value (0.818) indicated that the choice of mitigation strategy had a substantial impact on error reduction.

The findings indicate that INS is the most effective strategy, offering the highest error reduction and fastest recovery time. Visual Odometry is also strong for error reduction but has slower recovery, while Jamming Mitigation

provides balanced performance with lower error reduction. **Signal Authentication** performed the weakest across all metric

5. DISCUSSION

The findings of this study reinforce the significant challenges that GPS spoofing and jamming pose to the safe operation of UAVs across both military and civilian sectors, a concern echoed by multiple researchers (e.g., Mohsan et al. [10]; Van den Bergh et al. [72]). As UAV reliance on GPS for navigation grows, the potential for interference to compromise mission success becomes increasingly critical. Real-world incidents, such as the disruption of UAV surveillance during the 2018 Venezuelan presidential election (Beene and Levin [2]), highlight the operational risks that UAVs face in GPS-compromised environments, which is consistent with the results showing significant positioning errors and mission failures under both spoofing and jamming conditions.

The qualitative analysis revealed that replay attacks and narrowband jamming are the most prevalent methods of GPS interference, with studies like those of Kassas et al. [70] and Ferreira et al. [71] highlighting how these methods severely degrade UAV performance. The positioning errors in this study, which increased to 15.11 meters under spoofing and 20.45 meters under jamming, are consistent with the findings of Gaspar et al. [78], who reported similar navigation drift under interference conditions. This further emphasizes the real-world applicability of the results, showing that UAVs are vulnerable to the exact types of interference described in the literature.

In terms of detection and mitigation strategies, this analysis demonstrates that machine learning algorithms can effectively detect interference, but trade-offs exist between accuracy and sensitivity. As noted by Ferreira et al. [71], multi-sensor fusion is one of the most promising techniques for detecting GPS interference, and this study found that SVM, while less accurate overall, exhibited better recall in detecting spoofed signals. This reinforces the importance of prioritizing sensitivity when developing detection systems for high-risk environments, such as those discussed in military settings by Lyu and Zhan [17].

Regarding mitigation strategies, the results show that Inertial Navigation Systems (INS) offer the highest error reduction (95.06%) and fastest recovery times, consistent with the work of Mohsan et al. [10], who highlighted the effectiveness of multi-sensor systems in maintaining UAV navigation in GPS-denied environments. However, the drift over time that occurs in INS was noted as a challenge in the literature, suggesting that while INS performs well in the short term, further research is needed to ensure its long-term accuracy.

The commercial sector faces unique challenges in adopting advanced anti-jamming techniques due to resource constraints. Studies such as those by Mohsan et al. [6] and Sadaf et al. [37] argue that while cryptographic methods and machine learning-based detection are highly effective, they remain costly and difficult to implement in commercial UAVs. This aligns with the finding that Signal Authentication was the weakest performer, likely due to its higher complexity and lower cost-effectiveness compared to other mitigation strategies, which are more suitable for high-budget military applications.

6. CONCLUSION AND RECOMMENDATION

This study analyzed GPS spoofing and jamming techniques and their impact on UAV performance, along with the effectiveness of various mitigation strategies. Replay attacks and narrowband jamming emerged as the most common interference methods. The analysis of GPS data showed that these attacks significantly increase positioning errors and reduce mission success rates, posing serious safety risks to UAV operations. Machine learning models, such as Random Forest, SVM, and Neural Networks, were assessed for detecting spoofed and jammed signals, with the SVM model demonstrating better sensitivity to spoofing despite lower overall accuracy. INS and Visual Odometry proved most effective in reducing navigation errors and maintaining mission success under interference, emphasizing the need for robust detection and mitigation strategies in GPS-reliant sectors. The study recommends the following:

1. **Adopt Multi-Sensor Fusion for Detection**: Prioritize using systems like INS and Visual Odometry in both civilian and military UAVs. These systems reduce

errors by over 90% and should be integrated to enhance UAV resilience in GPS-denied environments.

2. **Implement Machine Learning Detection**: Deploy machine learning algorithms, especially SVM models, in real-time UAV systems to improve detection sensitivity and quickly mitigate GPS spoofing and jamming.
3. **Develop Cost-Effective Anti-Jamming for Commercial UAVs**: Focus on affordable anti-jamming technologies, such as jamming-resistant antennas and frequency hopping, to enhance commercial UAV protection at a manageable cost.
4. **Strengthen GPS Signal Authentication**: Integrate cryptographic signal authentication into standard GPS protocols, particularly in critical civilian sectors like infrastructure monitoring, to prevent spoofing and ensure secure navigation.

DISCLAIMER (ARTIFICIAL INTELLIGENCE)

Author(s) hereby declare that NO generative AI technologies such as Large Language Models (ChatGPT, COPILOT, etc) and text-to-image generators have been used during writing or editing of this manuscript.

COMPETING INTERESTS

Authors have declared that no competing interests exist.

REFERENCES

1. Elmokadem T, Savkin AV. Towards fully autonomous UAVs: A survey. Sensors. 2021;21(18):6223. DOI:10.3390/s21186223.
2. Beene R, Levin A. Bloomberg - Are you a robot? Bloomberg.com; 2024. Available:https://www.bloomberg.com/politics/articles/2018-08-07/venezuela-attack-highlights-vulnerability-to-drone-assassins (accessed Sep 10, 2024).
3. Burbank J, Greene T, Kaabouch N. Detecting and mitigating attacks on GPS devices. Sensors. 2024;24(17):5529. DOI:10.3390/s24175529.
4. Felux M, Figuet B, Waltert M, Fol P, Strohmeier M, Olive X. Analysis of GNSS disruptions in European airspace. Ion.org. 2023:315–26. DOI:10.33012/2023.18626.
5. Wendt P, Voltes-Dorta A, Suau-Sanchez P. Estimating the costs for the airport operator and airlines of a drone-related shutdown: an application to Frankfurt International Airport. J Transp Secur. 2020;13(1–2):93–116. DOI:10.1007/s12198-020-00212-4.
6. Mohsan SAH, Othman NQH, Li Y, Alsharif MH, Khan MA. Unmanned aerial vehicles (UAVs): practical aspects, applications, open challenges, security issues, and future trends. Intell Serv Robot. 2023;16(1). DOI:10.1007/s11370-022-00452-4.
7. Aminifar F, Rahmatian F. Unmanned aerial vehicles in modern power systems: technologies, use cases, outlooks, and challenges. IEEE Electrific Mag. 2020;8(4):107–16. DOI:10.1109/mele.2020.3026505.
8. Shah IA. Privacy and security challenges in unmanned aerial vehicles (UAVs). Wiley Online Library. 2024:93–115. DOI:10.1002/9781394204472.ch5.
9. Couturier A, Akhloufi MA. A review on absolute visual localization for UAV. Robot Auton Syst. 2021;135:103666. DOI:10.1016/j.robot.2020.103666.
10. Mohsan SAH, Khan MA, Noor F, Ullah I, Alsharif MH. Towards the unmanned aerial vehicles (UAVs): a comprehensive review. Drones. 2022;6(6):147. DOI:10.3390/drones6060147.
11. Yu Z, Wang Z, Yu J, Liu D, Song H, Li Z. Cybersecurity of unmanned aerial vehicles: a survey. IEEE Aerosp Electron Syst Mag. 2023:1–25. DOI:10.1109/maes.2023.3318226.
12. Joseph SA. Balancing data privacy and compliance in blockchain-based financial systems. J Eng Res Rep. 2024;26(9):169–89. DOI:10.9734/jerr/2024/v26i91271.
13. Durlik I, Miller T, Kostecka E, Zwierzewicz Z, Łobodzińska A. Cybersecurity in autonomous vehicles—are we ready for the challenge? Electronics. 2024;13(13): 2654. DOI:10.3390/electronics13132654.
14. Pham M, Xiong K. A survey on security attacks and defense techniques for connected and autonomous vehicles. Comput Secur. 2021;109:102269. doi:10.1016/j.cose.2021.102269.
15. Osmani K, Schulz D. Comprehensive investigation of unmanned aerial vehicles

(UAVs): an in-depth analysis of avionics systems. Sensors. 2024;24(10):3064. DOI:10.3390/s24103064.

16. Okon SU, Olateju OO, Ogungbemi OS, Joseph SA, Olisa AO, Olaniyi OO. Incorporating privacy by design principles in the modification of AI systems in preventing breaches across multiple environments, including public cloud, private cloud, and on-prem. J Eng Res Rep. 2024;26(9):136–58. DOI:10.9734/jerr/2024/v26i91269.
17. Lyu C, Zhan R. Global analysis of active defense technologies for unmanned aerial vehicles. IEEE Aerosp Electron Syst Mag. 2022;37(1):6–31. DOI:10.1109/MAES.2021.3115205.
18. Arafat MY, Alam MM, Moh S. Vision-based navigation techniques for unmanned aerial vehicles: review and challenges. Drones. 2023;7(2):89. DOI:10.3390/drones7020089.
19. AL-Syouf RA, Bani-Hani RM, AL-Jarrah OY. Machine learning approaches to intrusion detection in unmanned aerial vehicles (UAVs). Neural Comput Appl. 2024. DOI:10.1007/s00521-024-10306-y.
20. Debie A, Samuel-Okon. Headlines to hard-lines: media intervention in managing bullying and cancel culture in the entertainment industry. Asian J Adv Res Rep. 2024;18(9):71–89. DOI:10.9734/ajarr/2024/v18i9736.
21. Giannaros A, et al. Autonomous vehicles: sophisticated attacks, safety issues, challenges, open topics, blockchain, and future directions. J Cybersecur Priv. 2023;3(3):493–543. DOI:10.3390/jcp3030025.
22. Alalwany E, Mahgoub I. Security and trust management in the Internet of Vehicles (IoV): challenges and machine learning solutions. Sensors. 2024;24(2): 368. DOI:10.3390/s24020368.
23. Che F, Ahmed QZ, Lazaridis PI, Sureephong P, Alade T. Indoor positioning system (IPS) using ultra-wide bandwidth (UWB)—for industrial Internet of Things (IIoT). Sensors. 2023;23(12):5710. DOI:10.3390/s23125710.
24. Wang X, Zhou Q. Analytical technique leveraging processing gain for evaluating the anti-jamming potential of underwater acoustic direct sequence spread spectrum communication systems. Symmetry. 2023;15(9):1710. DOI:10.3390/sym15091710.
25. John-Otumu AM, Ikerionwu C, Olaniyi OO, Dokun O, Eze UF, Nwokonkwo OC. Advancing COVID-19 prediction with deep learning models: a review. Int Conf Sci Eng Bus Driving Sustain Dev Goals. 2024:1–5. DOI:10.1109/seb4sdg60871.2024.10630186.
26. Samuel-Okon AD. Smart media or biased media: the impacts and challenges of AI and big data on the media industry. Asian J Res Comput Sci. 2024;17(7):128–44. DOI:10.9734/ajrcos/2024/v17i7484.
27. Radoš K, Brkić M, Begušić D. Recent advances on jamming and spoofing detection in GNSS. Sensors. 2024;24(13):4210. DOI:10.3390/s24134210.
28. Qu J, et al. Recent progress in advanced tactile sensing technologies for soft grippers. Adv Funct Mater. 2023;33(41). DOI:10.1002/adfm.202306249.
29. Salim S, Moustafa N, Reisslein M. Cybersecurity of satellite communications systems: a comprehensive survey of the space, ground, and links segments. IEEE Commun Surv Tutor. 2024:1. DOI:10.1109/comst.2024.3408277.
30. Khan SZ, Mohsin M, Iqbal W. On GPS spoofing of aerial platforms: a review of threats, challenges, methodologies, and future research directions. PeerJ Comput Sci. 2021;7 DOI:10.7717/peerj-cs.507.
31. Akinola OI. Adaptive location-based routing protocols for dynamic wireless sensor networks in urban cyber-physical systems. J Eng Res Rep. 2024 Jul;26(7):424–43. DOI: 10.9734/jerr/2024/v26i71220.
32. Abosata N, Al-Rubaye S, Inalhan G, Emmanouilidis C. Internet of things for system integrity: A comprehensive survey on security, attacks and countermeasures for industrial applications. Sensors (Basel). 2021 May;21(11):3654. DOI: 10.3390/s21113654.
33. Gonzalez-Jorge H, Aldao E, Fontenla-Carrera G, Veiga-López F, Balvís E, Ríos-Otero E. Counter drone technology: A review. Preprints. 2024 Feb 9. Available:https://www.preprints.org/manuscript/202402.0551 (accessed 2024 Sep 11).

34. Yaacoub J-P, Salman O. Security analysis of drones systems: Attacks, limitations, and recommendations. Internet Things. 2020 May;11:100218. DOI: 10.1016/j.iot.2020.100218.
35. Rejeb A, Rejeb K, Simske SJ, Treiblmaier H. Drones for supply chain management and logistics: A review and research agenda. Int J Logist Res Appl. 2021 Sep;26(6):1–24. DOI: 10.1080/13675567.2021.1981273.
36. Gamba MT, Polidori BD, Minetto A, Dovis F, Banfi E, Dominici F. GNSS radio frequency interference monitoring from LEO satellites: An in-laboratory prototype. Sensors. 2024 Jan;24(2):508. DOI: 10.3390/s24020508.
37. Sadaf M, et al. Connected and automated vehicles: Infrastructure, applications, security, critical challenges, and future aspects. Technologies. 2023 Oct;11(5):117. Available:https://www.mdpi.com/2227-7080/11/5/117 (accessed 2024 Sep 11).
38. AlRushood MA, Rahbar F, Selim SZ, Dweiri F. Accelerating use of drones and robotics in post-pandemic project supply chain. Drones. 2023 May;7(5):313. DOI:10.3390/drones7050313.
39. Omolara AE, Alawida M, Abiodun OI. Drone cybersecurity issues, solutions, trend insights and future perspectives: A survey. Neural Comput Appl. 2023 Aug;35. DOI:10.1007/s00521-023-08857-7.
40. Chamola V, Kotesh P, Agarwal N, Naren, Gupta N, Guizani M. A comprehensive review of unmanned aerial vehicle attacks and neutralization techniques. Ad Hoc Netw. 2021 Feb;111:102324. DOI: 10.1016/j.adhoc.2020.102324.
41. Amro A, Oruc A, Gkioulos V, Katsikas S. Navigation data anomaly analysis and detection. Information. 2022 Feb;13(3):104. DOI:10.3390/info13030104.
42. Olabanji SO, Oladoyinbo OB, Asonze CU, Oladoyinbo TO, Ajayi SA, Olaniyi OO. Effect of adopting AI to explore big data on personally identifiable information (PII) for financial and economic data transformation. Asian J Econ Bus Acc. 2024 Feb;24(4):106–25. DOI:10.9734/ajeba/2024/v24i41268.
43. Fascista A. Toward integrated large-scale environmental monitoring using WSN/UAV/crowdsensing: A review of applications, signal processing, and future perspectives. Sensors. 2022 Feb;22(5):1824. DOI: 10.3390/s22051824.
44. Bello HO, Ige AB, Ameyaw MN. Adaptive machine learning models: Concepts for real-time financial fraud prevention in dynamic environments. World J Adv Eng Technol Sci. 2024 Jul;12(2):21–34. DOI: 10.30574/wjaets.2024.12.2.0266.
45. Chen X, Luo R, Liu T, Yuan H, Wu H. Satellite navigation signal authentication in GNSS: A survey on technology evolution, status, and perspective for BDS. Remote Sens. 2023 Mar;15(5):1462. DOI: 10.3390/rs15051462.
46. Samuel-Okon AD, Olateju OO, Okon SU, Olaniyi OO, Igwenagu UT. Formulating global policies and strategies for combating criminal use and abuse of artificial intelligence. Arch Curr Res Int. 2024 Jun;24(5):612–29. DOI: 10.9734/acri/2024/v24i5735.
47. Hoffer J, De R, Kreuser P, Youssef T. Educational review: GPS applications and vulnerability implications. IEEE Xplore. 2020 Mar. DOI: 10.1109/southeastcon44009.2020.9249677.
48. Nankya M, Chataut R, Akl R. Securing industrial control systems: Components, cyber threats, and machine learning-driven defense strategies. Sensors. 2023 Jan;23(21):8840. DOI: 10.3390/s23218840.
49. Telli K, et al. A comprehensive review of recent research trends on unmanned aerial vehicles (UAVs). Systems. 2023 Aug;11(8):400. DOI: 10.3390/systems11080400.
50. Srivastava A, Prakash J. Internet of low-altitude UAVs (IoLoUA): A methodical modeling on integration of Internet of 'Things' with 'UAV' possibilities and tests. Artif Intell Rev. 2022 Jul;56. doi: 10.1007/s10462-022-10225-1.
51. Wu Z, Zhang Y, Yang Y, Liang C, Liu R. Spoofing and anti-spoofing technologies of global navigation satellite system: A survey. IEEE Access. 2020;8:165444–96. DOI: 10.1109/ACCESS.2020.3022294.
52. Serrano W. Big data in smart infrastructure. Adv Intell Syst Comput. 2020 Aug;703–32. DOI: 10.1007/978-3-030-55187-2_51.
53. Hsieh Y-H, Chao C-M, Lin C-Y, Yeh C-C. Anti-jamming low-latency channel hopping

protocol for cognitive radio networks. Electronics. 2023 Apr;12(8):1811.
DOI: 10.3390/electronics12081811.

54. Adigwe CS, Olaniyi OO, Olabanji SO, Okunleye OJ, Mayeke NR, Ajayi SA. Forecasting the future: The interplay of artificial intelligence, innovation, and competitiveness and its effect on the global economy. Asian J Econ Bus Acc. 2024 Feb;24(4):126–46.
DOI: 10.9734/ajeba/2024/v24i41269.
55. Felli L, Giuliano R, Negri AD, Terlizzi F, Mazzenga F, Vizzarri A. Maximal LoRa range for unmanned aerial vehicle fleet service in different environmental conditions. IoT. 2024 Jul;5(3):509–23.
DOI: 10.3390/iot5030023.
56. Castrillo VU, Manco A, Pascarella D, Gigante G. A review of counter-UAS technologies for cooperative defensive teams of drones. Drones. 2022 Mar;6(3):65.
DOI: 10.3390/drones6030065.
57. Lee J-C, Chen C-C, Shen C-T, Lai Y-C. Landmark-based scale estimation and correction of visual inertial odometry for VTOL UAVs in a GPS-denied environment. Sensors. 2022 Dec;22(24):9654.
DOI:10.3390/s22249654.
58. Xu C, Liu Z, Li Z. Robust visual-inertial navigation system for low precision sensors under indoor and outdoor environments. Remote Sens. 2021 Feb;13(4):772.
DOI:10.3390/rs13040772.
59. Olabanji SO. AI for identity and access management (IAM) in the cloud: Exploring the potential of artificial intelligence to improve user authentication, authorization, and access control within cloud-based systems. Asian J Res Comput Sci. 2024;17(3):38–56.
DOI:10.9734/ajrcos/2024/v17i3423.
60. Adnan MH, Zukarnain ZA, Harun NZ. Quantum key distribution for 5G networks: A review, state of art and future directions. Future Internet. 2022 Feb;14(3):73.
DOI:10.3390/fi14030073.
61. Hadi HJ, Cao Y, Nisa KU, Jamil AM, Ni Q. A comprehensive survey on security, privacy issues and emerging defence technologies for UAVs. J Network Comput Appl. 2023 Apr;213:103607.
DOI:10.1016/j.jnca.2023.103607.
62. Vikram A, Patel SK, Alsalman O. Measurement of optical fiber sensors for intrusion detection and warning systems fortified with intelligent false alarm suppression. Opt Quantum Electron. 2024 Apr;56(6).
DOI:10.1007/s11082-024-06797-7.
63. Olaniyi OO, Ugonnia JC, Olaniyi FG, Arigbabu AT, Adigwe CS. Digital Collaborative Tools, Strategic Communication, and Social Capital: Unveiling the Impact of Digital Transformation on Organizational Dynamics. Asian J Res Comput Sci. 2024 Mar;17(5):140–156.
DOI:10.9734/ajrcos/2024/v17i5444.
64. Michaelides-Mateou S. Challenges and Trends in the Aviation Industry: Integrating UAVs in Non-segregated Airspace. Springer eBooks; 2023 Jan. p. 377–409.
DOI:10.1007/978-3-031-32037-8_13.
65. Cromwell C, Giampaolo J, Hupy J, Miller Z, Chandrasekaran A. A Systematic Review of Best Practices for UAS Data Collection in Forestry-Related Applications. Forests. 2021 Jul;12(7):957.
DOI:10.3390/f12070957.
66. Behiry MH, Aly M. Cyberattack detection in wireless sensor networks using a hybrid feature reduction technique with AI and machine learning methods. J Big Data. 2024 Jan;11(1).
DOI:10.1186/s40537-023-00870-w.
67. Yanakiev Y, Bernal SL, Navajo AM, Stoianov N, Perez MG, Martin C. Approach to harmonisation of technological solutions, operating procedures, preparedness and cross-sectorial collaboration opportunities for first aid response in cross-border mass-casualty incidents. ACM Digital Library. 2023 Aug.
DOI: 10.1145/3600160.3605060.
68. Cheng Y, Li P. Technical thinking: how does e-land administration system promote the efficiency of cross-sectoral collaborative land governance in China? Surv Rev. 2023 Aug;56(397):348–366.
DOI:10.1080/00396265.2023.2247680.
69. Novák A, Kováčiková K, Kandera B, Novák Sedláčková A. Global Navigation Satellite Systems Signal Vulnerabilities in Unmanned Aerial Vehicle Operations: Impact of Affordable Software-Defined Radio. Drones. 2024 Mar;8(3):109.
DOI:10.3390/drones8030109.
70. Kassas ZM, Khalife J, Abdallah AA, Lee C. I am Not Afraid of the Jammer: Navigating with Signals of Opportunity in GPS-Denied Environments. Proceedings of the Satellite

Division's International Technical Meeting. 2020 Oct.
DOI:10.33012/2020.17737.

71. Ferreira R, Gaspar J, Sebastião P, Souto N. A Software Defined Radio Based Anti-UAV Mobile System with Jamming and Spoofing Capabilities. Sensors. 2022 Feb;22(4):1487.
DOI:10.3390/s22041487.
72. Van den Bergh B, Pollin S. Keeping UAVs Under Control During GPS Jamming. IEEE Syst J. 2019 Jun;13(2): 2010–2021.
DOI:10.1109/jsyst.2018.2882769.
73. Altaweel A, Mukkath H, Kamel I. GPS Spoofing Attacks in FANETs: A Systematic Literature Review. IEEE Access. 2023 Jan;11:55233–55280.
DOI:10.1109/access.2023.3281731.
74. Basan E, Basan A, Nekrasov A, Fidge C, Sushkin N, Peskova O. GPS-Spoofing Attack Detection Technology for UAVs Based on Kullback–Leibler Divergence. Drones. 2022 Jan;6(1):8.
DOI:10.3390/drones6010008.
75. Panice G, et al. A SVM-based detection approach for GPS spoofing attacks to UAV. In: Proceedings of the International Conference on Automation and Computing. 2017 Sep.
DOI:10.23919/iconac.2017.8081999.
76. He D, Chan S, Guizani M. Communication Security of Unmanned Aerial Vehicles. IEEE Wirel Commun. 2017 Aug;24(4):134–139.
DOI: 10.1109/mwc.2016.1600073.
77. Talaei Khoei T, Ismail S, Kaabouch N. Dynamic Selection Techniques for Detecting GPS Spoofing Attacks on UAVs. Sensors. 2022 Jan;22(2):662.
DOI:10.3390/s22020662.
78. Ferreira R, Gaspar J, Sebastião P, Souto N. Effective GPS Jamming Techniques for UAVs Using Low-Cost SDR Platforms. Wireless Personal Commun. 2020 Mar.
DOI:10.1007/s11277-020-07212-6.
79. Zheng X-C, Sun H-M. Hijacking Unmanned Aerial Vehicle by Exploiting Civil GPS Vulnerabilities Using Software-defined Radio. Sensors Mater. 2020 Aug;32(8):2729.
DOI: 10.18494/sam.2020.2783.
80. Ranyal E, Jain K. Unmanned Aerial Vehicle's Vulnerability to GPS Spoofing: A Review. J Indian Soc Remote Sens. 2020 Nov;49(3):585–591.
DOI: 10.1007/s12524-020-01225-1.
81. Di Pietro R, Oligeri G, Tedeschi P. JAM-ME: Exploiting Jamming to Accomplish Drone Mission. 2019 Jun.
DOI:10.1109/cns.2019.8802717.
82. Khan SZ, Mohsin M, Iqbal W. On GPS spoofing of aerial platforms: a review of threats, challenges, methodologies, and future research directions. PeerJ Comput Sci. 2021 May;7
DOI: 10.7717/peerj-cs.507.

Peer-review history:
The peer review history for this paper can be accessed here:
https://www.sdiarticle5.com/review-history/124341