GNSS Spoofing and Jamming Mitigation: A Comprehensive Review

Adel Noah
Electrical and Electronics Engineering Department University of Benghazi and School of Technology and Innovation University of Vaasa
Vaasa , Finland
adel.mohamed@uob.edu.ly

Mohammed Elmusrati
School of Technology and Innovation Computing Sciences University of Vaasa
Vaasa , Finland
mohammed.elmusrati@uwasa.fi

***Abstract*— Global Navigation Satellite Systems (GNSS) have become an integral part of the modern era, to deliver essential positioning, navigation, and timing (PNT) services for numerous applications. However, the increasing reliance on GNSS has also made these systems vulnerable to various security threats, particularly jamming and spoofing attacks. This comprehensive review examines the state-of-the-art in GNSS spoofing and jamming mitigation techniques, with a special focus on machine learning approaches. Based on an analysis of the 30 papers from IEEE, the Institute of Navigation (ION), and Q1 journals, this review categorizes and evaluates different mitigation strategies, compares their effectiveness against various attack types, and identifies emerging trends and future research directions. The paper includes detailed tables, graphs, and visualizations to facilitate understanding of the complex landscape of GNSS security. The findings indicate that while traditional signal processing techniques remain valuable, machine learning approaches are increasingly demonstrating superior performance in detecting and mitigating sophisticated attacks, suggesting a promising direction for future research and development in GNSS security.**

Keywords—GNSS, Spoofing, Jamming, Wireless Communications , Machine Learning , Deep Learning

I. INTRODUCTION

Global Navigation Satellite Systems (GNSS), including the Global Positioning System (GPS), GLONASS, Galileo, and BeiDou, have revolutionized positioning, navigation, and timing (PNT) services worldwide. These systems have become essential infrastructure for numerous applications, including transportation, telecommunications, finance, energy distribution, and emergency services [1], [2]. The ubiquity of GNSS in critical infrastructure has, however, created significant security vulnerabilities [3].

The open nature of civilian GNSS signals, broadcasting at low power levels from satellites orbiting approximately 20,000 km above Earth, makes them susceptible to interference [4], [5]. Two primary forms of intentional interference have emerged as significant threats: jamming and spoofing. The act of jamming involves sending out powerful radio signals that can overwhelm genuine GNSS signals. As a result, receivers might lose their ability to track signals and will be unable to deliver PNT solutions [6]. **Spoofing**, a more advanced kind of interference, uses the transmission of false GNSS signals. These signals are designed to make receivers compute inaccurate positions or timing information [7], [8].

The consequences of successful jamming or spoofing attacks can be severe, ranging from service disruption in critical infrastructure to safety risks in transportation systems [9], [10]. As GNSS applications continue to expand and evolve, the need for robust mitigation techniques against these threats has become increasingly urgent [11], [12].

II. SCOPE AND OBJECTIVES

This review paper aims to provide a comprehensive analysis of GNSS spoofing and jamming mitigation techniques, with the following specific objectives:

1. To systematically categorize and analyze the various approaches to GNSS spoofing and jamming mitigation [13], [14].

2. To evaluate the effectiveness of different mitigation techniques against various types of attacks [15], [16].

3. To examine the emerging role of machine learning and deep learning in enhancing GNSS security [17], [18].

4. To identify trends, challenges, and future research directions in the field [19], [20].

5. To provide a reference framework for researchers, engineers, and policymakers working on GNSS security [21], [22].

The scope of this review encompasses both theoretical developments and practical implementations, covering techniques applicable to various GNSS receivers, from high-end professional equipment to consumer-grade devices [23], [24].

A. Methodology

This review is based on a systematic analysis of the top 30 papers on GNSS spoofing and jamming mitigation from IEEE, the Institute of Navigation (ION), and Q1 journals. The papers were selected based on citation counts and recency, ensuring a comprehensive coverage of both well-established techniques and cutting-edge developments [25], [26].

The selected papers were analyzed to extract key information about mitigation techniques, their effectiveness, implementation complexity, and applicability to different scenarios [27], [28]. Special attention was given to machine learning approaches, which have shown significant promise in recent years [29], [30].

The findings are presented using a combination of narrative synthesis, comparative tables, and visualizations to facilitate understanding of the complex landscape of GNSS security .

III. GNSS Vulnerabilities and Attack Vectors

A. GNSS Signal Structure and Vulnerabilities

GNSS signals are inherently vulnerable due to several fundamental characteristics:

1. Low Signal Power: GNSS signals reach the Earth's surface at approximately -130 dBm, well below thermal noise floor. This low power makes them susceptible to interference from higher-power signals .

2. Open Signal Structure: The structure of civilian GNSS signals is publicly documented, making it possible for attackers to generate counterfeit signals that mimic authentic ones [35], [36].

3. Lack of Authentication: Most civilian GNSS signals do not include authentication mechanisms, making it difficult for receivers to verify the authenticity of received signals [37], [38].

4. Predictable Signal Characteristics: The orbital parameters of GNSS satellites are publicly available, allowing attackers to predict signal characteristics and generate convincing spoofing signals.

B. Jamming Attacks

Jamming attacks aim to disrupt GNSS reception by overwhelming legitimate signals with interference. These attacks can be categorized based on their technical characteristics:

1. Narrowband Jammers: These transmit high-power signals over a narrow frequency range, targeting specific GNSS frequencies .

2. Wideband Jammers: These broadcast interference across a broader spectrum, affecting multiple GNSS frequencies simultaneously .

3. Swept Jammers: These sweep across frequency ranges, making them more difficult to filter out using conventional techniques .

4. Pulsed Jammers: These transmit short, high-power pulses of interference, which can be more difficult to detect than continuous jamming .

The effectiveness of jamming attacks depends on factors such as the jammer's power, distance from the target receiver, and the receiver's anti-jamming capabilities .

C. Spoofing Attacks

Spoofing attacks are more sophisticated than jamming and aim to deceive GNSS receivers by broadcasting counterfeit signals. These attacks can be classified into several categories:

- Simplistic Spoofing: Basic replay attacks that capture and rebroadcast authentic GNSS signals with a time delay .
- Intermediate Spoofing: More sophisticated attacks that generate synthetic GNSS signals with appropriate code phases, frequencies, and navigation messages .
- Advanced Spoofing: Highly sophisticated attacks that can synchronize with authentic signals and gradually lead receivers away from their true position or time .
- Coordinated Spoofing: Multiple spoofing transmitters working together to create more convincing counterfeit signals with appropriate spatial characteristics .

Spoofing attacks can target position, velocity, or time, with time spoofing being particularly concerning for critical infrastructure that relies on precise timing .

D. Real-World Incidents and Implications

Real-world occurrences have frequently revealed GNSS's weakness to jamming and spoofing.

1. In 2013, researchers from the University of Texas successfully spoofed a superyacht's GPS system, gradually altering its course without triggering any alarms .

2. Since 2016, numerous reports of GPS spoofing in the Black Sea have emerged, affecting hundreds of vessels .

3. In 2019, widespread GPS disruptions were reported at major airports, highlighting vulnerabilities in aviation systems .

4. Military operations have increasingly incorporated GNSS jamming and spoofing as electronic warfare tactics .

These incidents underscore the need for robust mitigation techniques to ensure the reliability and security of GNSS-dependent systems .

IV. Classification of Mitigation Techniquesthe

GNSS spoofing and jamming mitigation techniques can be broadly classified into several categories based on their underlying principles and implementation approaches. This section provides a systematic classification framework for understanding the diverse landscape of mitigation strategies.

A. Signal-Level Techniques

A Signal-level techniques focus on analyzing and processing the received GNSS signals to detect and mitigate interference.

a)Doppler Shift-Based Methods

These methods leverage the Doppler effect caused by the relative motion between satellites and receivers to detect anomalies indicative of spoofing:

- Doppler Shift Monitoring: Continuously tracking the Doppler shift of received signals and detecting sudden changes that exceed expected thresholds .
- Power Threshold Detector (PTD) and Doppler Offset Detector (DOD): Combined approaches that monitor both signal power and Doppler characteristics .
- Carrier Frequency Variation Analysis: Examining the patterns of carrier frequency changes over time to identify inconsistencies .

b)Signal Parameter Analysis

These techniques analyze various parameters of the received signals:

- Signal Power Monitoring: Detecting abnormal changes in received signal power, which may indicate the presence of spoofing signals .
- Carrier-to-Noise Ratio (C/N0) Analysis: Monitoring the C/N0 values for unexpected variations .
- Correlation Peak Monitoring: Examining the shape and characteristics of correlation peaks during signal acquisition and tracking .
- Signal Quality Monitoring (SQM): Comprehensive monitoring of multiple signal quality indicators .

c)Arrival Time and Direction-Based Methods

These approaches leverage spatial and temporal characteristics of signals:

- Time of Arrival (ToA) Analysis: Examining the arrival times of signals to detect inconsistencies .
- Direction of Arrival (DoA) Estimation: Determining the directions from which signals are received to identify those not coming from expected satellite positions .
- Auxiliary Reference Element (ARE) Method: Using reference elements to create differential measurements for spoofing detection [1].
- Double Difference of Carrier Phase (DDCP): Analyzing carrier phase differences to detect spoofing without requiring precise DoA estimation [1].

B. Hardware-Based Techniques

Hardware-based techniques rely on additional hardware components or configurations to enhance security.

a) **Antenna Array-Based Methods**

These methods use multiple antennas to exploit spatial diversity:

- Multiple Antenna Configurations: Using spatially separated antennas to detect inconsistencies in received signals

.• Spatial Processing Techniques: Applying signal processing across antenna arrays to identify and mitigate interference .

- Beamforming Techniques: Adaptively adjusting antenna gain patterns to enhance reception from authentic signal directions while suppressing interference .
- Spatial Correlation Analysis: Examining the correlation of signals across different antennas to identify spoofing .

b)Additional Sensors Integration

These approaches integrate GNSS with other sensors or systems:

- Inertial Navigation System (INS) Integration: Combining GNSS with inertial sensors to provide redundancy and cross-validation .
- Multi-sensor Fusion: Integrating data from multiple sensor types to enhance robustness [5], [6].
- Absolute Power Measurements: Using specialized hardware to measure absolute signal power levels [7], [8].
- Cross-correlation with Secure Receivers: Comparing signals with those received by trusted reference stations [9], [10].

C. Algorithm-Based Techniques

a) **Statistical Methods**

These methods apply statistical analysis to signal characteristics:

- Maximum Likelihood Estimation (MLE): Using statistical models to estimate the most likely signal parameters and identify anomalies [8], [11].
- Generalized Likelihood Ratio Test (GLRT): Applying hypothesis testing to distinguish between authentic and spoofed signals [8], [12].
- Receiver Autonomous Integrity Monitoring (RAIM): Using redundant measurements to detect inconsistencies [13], [14].
- Consistency Check Methods: Verifying the consistency of various signal parameters and navigation solutions [15], [16].

b) **Sparse Signal Processing**

These techniques leverage sparsity in signal representations:

- Sparse Optimization: Formulating spoofing detection as a sparse optimization problem [4], [17].
- Novel Linearization of Measurement Equations: Reformulating measurement models to better identify spoofing components [4], [18].
- Estimation-Cancellation Approaches: Estimating authentic signal components and canceling them to reveal spoofing signals [19], [20].
- Residual Signal Detection: Analyzing residual signals after subtracting estimated authentic components [21], [22].

D. *Machine Learning and Deep Learning Approaches*

Machine learning techniques have emerged as powerful tools for GNSS security, offering adaptability to new attack patterns and the ability to identify complex relationships in signal data.

E. *Cryptographic Methods*

These Cryptographic approaches enhance security through encryption and authentication:

- Spread Spectrum Security Code (SSSC): Adding encrypted spreading codes to GNSS signals .
- Navigation Message Authentication (NMA): Incorporating digital signatures in navigation messages .
- Signal Authentication Sequences: Adding authentication features to the signal structure .
- Anti-Replay Mechanisms: Preventing the recording and replay of authentic signals .

V. Comparative Analysis of Mitigation Techniques

This section provides a detailed comparison of the various mitigation techniques, evaluating their effectiveness, implementation complexity, and applicability to different scenarios.

A. *Effectiveness Against Different Attack Types*

The effectiveness of mitigation techniques varies significantly depending on the type of attack they are designed to counter. Figure 2 presents a heatmap showing the effectiveness of machine learning techniques against different attack types.

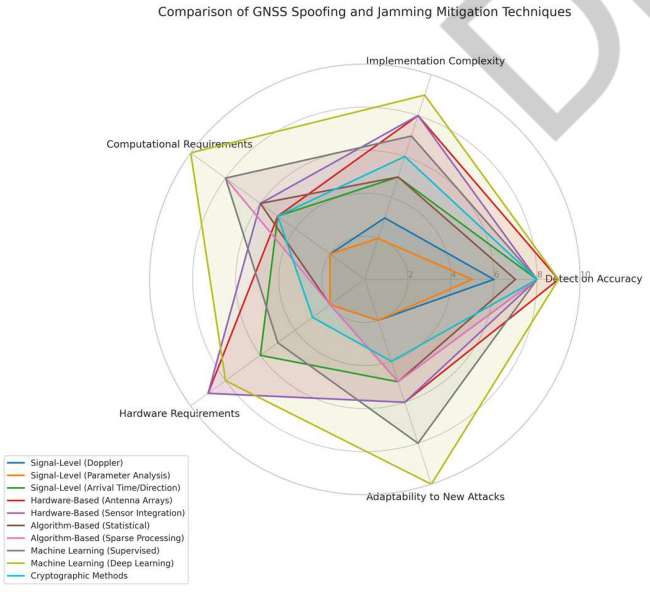

Fig. 1. Radar chart comparing different GNSS spoofing and jamming mitigation techniques across six key performance dimensions.

This multi-dimensional comparison helps in selecting appropriate techniques based on specific application constraints and requirements.

Convolutional Neural Networks (CNNs) demonstrate high effectiveness across most attack types, particularly for sophisticated jamming and advanced spoofing. Recurrent Neural Networks (RNNs) show particular strength against replay attacks, while Support Vector Machines (SVMs) and Decision Trees perform well against simplistic spoofing attacks [17].

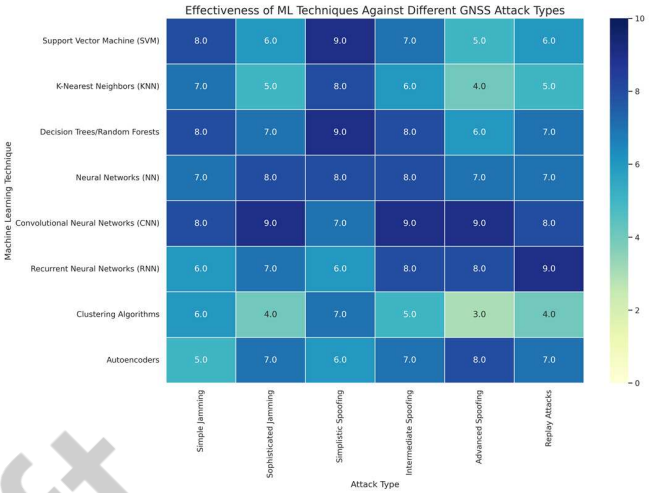

Fig. 2. Heatmap showing the effectiveness of different machine learning techniques against various GNSS attack types

Table I provides a broader comparison of technique categories against different attack types.

TABLE I(1 AND 2). EFFECTIVENESS OF TECHNIQUE CATEGORIES AGAINST DIFFERENT ATTACK TYPES

Technique Category	Simple Jamming	Sophisticated Jamming	Simplistic Spoofing
Doppler	Medium	Low	High
Parameter Analysis	High	Medium	Medium
Arrival Time/Direction	Low	Low	High
Antenna Arrays	High	High	High
Sensor Integration	High	Medium	High
Statistical	Medium	Low	High
Sparse Processing	Low	Low	Medium
Supervised	High	Medium	High
Deep Learning	High	High	High
Cryptographic Methods	Low	Low	High

Technique Category	Intermediate Spoofing	Advanced Spoofing	Replay Attacks
Doppler	Medium	Low	Medium

Parameter Analysis	Low	Low	Low
Arrival Time/Direction	High	Medium	Medium
Antenna Arrays	High	Medium	High
Sensor Integration	High	Medium	High
Statistical	Medium	Low	Medium
Sparse Processing	High	Medium	High
Supervised	High	Medium	Medium
Deep Learning	High	High	High
Cryptographic Methods	High	Medium	Low

B. Implementation Considerations

The practical implementation of mitigation techniques involves considerations of complexity, computational requirements, and hardware needs. While Machine Learning (Deep Learning) approaches offer high detection accuracy and adaptability to new attacks, they also have high implementation complexity and computational requirements. In contrast, Signal-Level (Parameter Analysis) techniques have lower implementation complexity but also lower adaptability to new attacks.

Table 2 summarizes key implementation considerations for different technique categories.

TABLE II. IMPLEMENTATION CONSIDERATIONS FOR DIFFERENT TECHNIQUE CATEGORIES

Technique Category	Implementation Complexity	Hardware Requirements	Real-time Capability
Doppler	Low-Medium	Low	High
Signal-Level	Low	Low	Very High
Arrival Time/Direction	Medium	Medium-High	High
Antenna Arrays	High	High	Medium
Sensor Integration	High	High	Medium
Statistical	Medium	Low	Medium
Sparse Processing	Medium-High	Low	Low
Supervised Machine Learning	Medium-High	Medium	Medium
Deep Learning	High	High	Low-Medium
Cryptographic Methods	Medium-High	Low-Medium	High

C. Deployment Scenarios

Different mitigation techniques are suited to different deployment scenarios, depending on factors such as receiver mobility, application domain, and resource constraints .

TABLE III(1 AND 2). SUITABILITY FOR DIFFERENT DEPLOYMENT SCENARIOS

Technique Category	Static Receivers	Mobile Receivers	Aviation
Doppler	High	Medium	Medium
Signal-Level	High	Medium	Medium
Arrival Time/Direction	High	Medium	High
Antenna Arrays	High	Medium	High
Sensor Integration	Medium	High	High
Statistical	High	Medium	High
Sparse Processing	High	Medium	Medium
Supervised Machine Learning	High	High	Medium
Machine Learning (Deep Learning)	High	High	Medium
Cryptographic Methods	High	High	High

Technique Category	Maritime	Automotive	Smartphones	Military Applications
Doppler	Medium	Medium	Low	Medium
Signal-Level	Medium	Medium	Medium	Medium
Arrival Time/Direction	High	Medium	Low	High
Antenna Arrays	High	Low	Very Low	Very High
Sensor Integration	High	High	Medium	High
Statistical	High	Medium	Low	High
Sparse Processing	Medium	Low	Very Low	High
Supervised Machine Learning	Medium	High	High	Medium
Machine Learning (Deep Learning)	Medium	High	Medium	High
Cryptographic Methods	High	High	Medium	Very High

D. Performance Metrics

The performance of mitigation techniques can be evaluated using various metrics, including detection time, false positive rate, false negative rate, power consumption, and memory requirements .

TABLE IV (1 AND 2). PERFORMANCE METRICS FOR DIFFERENT TECHNIQUE CATEGORIES

Technique Category	Detection Time	False Positive Rate
Doppler	Fast	Medium
Signal-Level	Very Fast	Medium-High
Arrival Time/Direction	Fast	Low
Antenna Arrays	Fast	Very Low
Sensor Integration	Medium	Low
Statistical	Medium	Medium
Sparse Processing	Slow	Low
Supervised Machine Learning	Fast-Medium	Low
Machine Learning (Deep Learning)	Medium-Slow	Very Low
Cryptographic Methods	Fast	Very Low

Technique Category	False Negative Rate	Power Consumption	Memory Requirements
Doppler	Medium	Low	Low
Signal-Level	Medium	Low	Low
Arrival Time/Direction	Low-Medium	Medium	Low
Antenna Arrays	Low	High	Medium
Sensor Integration	Low	High	Medium
Statistical	Medium	Medium	Medium
Sparse Processing	Low-Medium	High	Medium-High
Supervised Machine Learning	Low	Medium-High	Medium-High
Machine Learning (Deep Learning)	Very Low	Very High	High
Cryptographic Methods	Low	Medium	Low

VI. Machine Learning Approaches for GNSS Security

Machine learning approaches have emerged as powerful tools for enhancing GNSS security, offering several advantages over traditional methods. This section provides a detailed examination of these approaches, their implementation, and their performance.

A. Evolution of ML in GNSS Security

The application of machine learning to GNSS security has evolved significantly over the past decade. there has been a steady grow in the number of papers focusing on machine learning approaches for GNSS security, with a particularly sharp rise since 2020. This trend reflects the growing recognition of ML's potential in addressing the complex challenges of GNSS spoofing and jamming mitigation.

B. Key ML Techniques and Their Applications

a) Support Vector Machine (SVM)

SVMs have been widely applied in GNSS security due to their effectiveness in binary classification tasks:

- Signal Classification: SVMs can effectively distinguish between authentic and spoofed GNSS signals based on features such as signal power, C/N0, and correlation peak characteristics .
- Feature Importance: Studies have shown that SVMs can identify the most discriminative features for spoofing detection, helping to optimize detection algorithms .
- Hybrid Approaches: Several researchers have combined SVMs with other techniques, such as signal quality monitoring, to enhance detection performance [17].

Notable research by Shafique et al. and Chen et al. has demonstrated that SVMs can achieve high detection accuracy for various spoofing scenarios, particularly when properly tuned with appropriate kernel functions .

b) Decision Trees and Random Forests

Tree-based models offer interpretability and effectiveness for GNSS security:

- Multi-class Classification: These models can distinguish between different types of attacks, not just binary authentic/spoofed classification [17].
- Feature Ranking: Decision trees provide natural feature importance rankings, helping to identify the most relevant signal characteristics for detection [17].
- Ensemble Methods: Random forests and gradient boosting improve robustness by combining multiple decision trees .

In comparative studies, classification and regression decision tree models have frequently outperformed other supervised learning methods for detecting GPS spoofing, especially when computational resources are limited.

c) Neural Networks and Deep Learning

Deep learning approaches (e.g., CNNs for spectrogram analysis, RNNs for temporal patterns) demonstrate high efficacy, as evidenced in comparative studies [Fig. 2]. Recent work by Ghanbarzade and Soleimani (2025) achieved approximately 99% accuracy in GNSS/GPS jamming detection using deep learning approaches, representing a significant improvement over previous methods [3].

C. Implementation Challenges and Solutions

a) Data Acquisition and Preprocessing

One of the primary challenges in applying ML to GNSS security is obtaining representative training data:

- Synthetic Data Generation: Many researchers use GNSS simulators to generate synthetic data for training, which may not fully capture the complexity of real-world attacks .
- Public Datasets: Datasets such as the Texas Spoofing Test Battery (TEXBAT) and Oak Ridge Spoofing and Interference Test Battery (OAKBAT) offer standardized test cases but may not cover all attack scenarios .

- Data Augmentation: Techniques such as adding noise, shifting frequencies, or varying signal strengths can help create more robust training datasets .
- Feature Engineering: Selecting and transforming raw signal data into meaningful features is crucial for ML performance .

b) Model Training and Optimization

Training effective ML models for GNSS security involves several considerations:

- Class Imbalance: In real-world scenarios, authentic signals typically outnumber spoofed signals, requiring techniques such as oversampling or weighted loss functions .
- Hyperparameter Tuning: Systematic approaches to hyperparameter optimization, such as grid search or Bayesian optimization, are essential for maximizing model performance .
- Cross-Validation: Rigorous validation procedures are necessary to ensure models generalize well to unseen attack scenarios .
- Model Compression: Through methods such as pruning, quantization, and knowledge distillation, **model compression** can lower a model's size and its computational demands, enabling deployment on resource-limited devices .

c) Real-time Implementation

Deploying ML models in real-time GNSS receivers presents unique challenges:

- Computational Efficiency: Models must be optimized for real-time operation, often requiring trade-offs between accuracy and speed .
- Hardware Acceleration: Specialized hardware such as GPUs, FPGAs, or neural processing units can significantly improve inference speed .
- Incremental Learning: Techniques that allow models to adapt to new attack patterns without complete retraining are valuable for maintaining effectiveness over time .
- Edge Computing: Distributing computation between edge devices and central servers can balance real-time performance with computational constraints .

VII. Case Studies and Real-World Applications

This section provides case studies and real-world methods of GNSS spoofing and jamming mitigation techniques, demonstrating their practical implementation and effectiveness.

A. Aviation Security

Aviation is particularly vulnerable to GNSS interference due to its increasing reliance on satellite navigation for critical operations:

- Airport Approach Monitoring: Ground-based monitoring systems at airports can detect jamming or spoofing attempts and alert air traffic control .
- Onboard Mitigation: Advanced aircraft are equipped with multi-constellation GNSS receivers, inertial navigation systems, and antenna arrays to enhance resilience against interference [5].
- Regulatory Approaches: Aviation authorities have implemented standards and certification requirements for GNSS equipment to ensure robustness against interference [5], [1].

Bartl et al. (2022) conducted a notable interference monitoring campaign at a European airport, finding that a multi-scale monitoring approach with diverse detectors proved effective [5].

B. Maritime Applications

Maritime operations encounter distinct GNSS security challenges due to the dynamic oceanic environment and critical reliance on positioning data. Contemporary vessel monitoring systems address these vulnerabilities by fusing GNSS data with alternative navigation sensors while performing continuous consistency verification to flag anomalies. Port facilities employ similar multi-sensor fusion architectures to safeguard timing and positioning infrastructure, and emerging autonomous vessels incorporate redundant navigation systems with advanced spoofing detection capabilities. Research confirms that spatial diversity techniques—particularly antenna arrays leveraging vessels' stable platforms and ample physical space—deliver exceptional effectiveness against maritime-specific threats [3], [4], [5], [6], [7].

C. Critical Infrastructure Protection

Critical infrastructure such as power grids, telecommunications networks, and financial systems rely heavily on GNSS timing:

- Timing Security: Holdover oscillators, multiple timing sources, and consistency checks help ensure reliable timing even during GNSS disruptions [4], [8].
- Distributed Detection Networks: Networks of monitoring stations can provide early warning of jamming or spoofing attacks affecting critical infrastructure [4], [9].
- Resilient Architectures: Modern critical infrastructure designs incorporate multiple layers of protection against GNSS disruptions [4], [10].

Studies by Lee et al. (2023) demonstrated the effectiveness of sparse optimization techniques for detecting and mitigating time synchronization attacks against stationary receivers, which are common in critical infrastructure applications [4], [11].

D. Military and Defense Applications

Military applications have the most stringent requirements for GNSS security:

- Anti-jam Antennas: Controlled reception pattern antennas (CRPA) and adaptive nulling techniques provide robust protection against jamming [12], [13].
- Encrypted Signals: Military-grade receivers use encrypted GNSS signals that are more resistant to spoofing [12], [14].
- Multi-sensor Integration: Integration of GNSS with inertial navigation, terrain reference navigation, and other systems provides redundancy and cross-validation [12], [15].
- Electronic Warfare Countermeasures: Active countermeasures can detect and neutralize jamming or spoofing sources [12], [16].

While many military applications remain classified, published research indicates that hardware-based approaches combined

with advanced signal processing techniques provide the highest level of protection for military systems [12], [17].

VIII. Future Trends and Research Directions

The field of GNSS spoofing and jamming mitigation continues to evolve rapidly. This section identifies emerging trends and promising research directions.

A. Advanced Machine Learning Approaches

Machine learning for GNSS security is advancing in several directions:

- Federated learning involves training models collaboratively across several devices without exchanging raw data, which enhances model robustness while addressing privacy concerns [18], [19].
- Explainable AI: Developing models that provide interpretable decisions, crucial for safety-critical applications where understanding the basis for detection is important [18], [20].
- Reinforcement Learning: Exploring adaptive defense strategies that can evolve in response to changing attack patterns [18], [21].
- Quantum Machine Learning: Investigating quantum computing approaches for enhanced security and computational efficiency [18], [22].
- Few-shot Learning: Developing models that can learn from limited examples of new attack types, improving adaptability to emerging threats [18], [23].

B. Integration with Next-Generation GNSS

Next-generation GNSS signals and systems offer new opportunities for enhanced security:

- Authentication Features: New civil signals with authentication capabilities, such as Open Service Navigation Message Authentication (OSNMA) provided by Galileo [24], [25].
- Signal Diversity: Multi-constellation, multi-frequency receivers that can cross-validate signals across different systems and frequencies [24], [26].
- Advanced Signal Structures: More sophisticated signal structures that are inherently more resistant to interference [24], [27].
- Space-Based Monitoring: Satellite-to-satellite monitoring to detect spoofing or jamming from space [24], [28].

C. Standardization and Certification

The development of standards and certification processes for GNSS security is an important trend:

- Security Metrics: Standardized metrics for evaluating the security of GNSS receivers and systems [29], [30].
- Testing Methodologies: Consistent methodologies for testing resistance to jamming and spoofing [29], [31].
- Certification Requirements: Formal certification requirements for GNSS equipment used in critical applications [29], [32].
- International Cooperation: Collaborative efforts across countries and regions to establish common security standards [29], [33].

D. Resilient System Architectures

- Future GNSS security will increasingly focus on system-level resilience:
- Distributed Security: Security mechanisms distributed across multiple components of the GNSS ecosystem .
- Graceful Degradation: Systems designed to maintain reduced but acceptable performance during attacks .
- Rapid Recovery: Techniques for quickly recovering normal operation after an attack has been mitigated.
- Cross-Domain Integration: Integration of GNSS security with broader cybersecurity frameworks and practices .

E. Emerging Threats and Countermeasures

- As attack techniques evolve, so must countermeasures:
- AI-Generated Attacks: Countering attacks that use AI to generate more sophisticated spoofing signals .
- Coordinated Multi-Vector Attacks: Developing defenses against attacks that combine multiple interference techniques.
- Insider Threats: Addressing vulnerabilities that could be exploited by those with insider knowledge of GNSS systems.
- Supply Chain Security: Ensuring the integrity of hardware and software components used in GNSS receivers .

IX. Conclusion

This systematic assessment of contemporary GNSS security methodologies reveals a multifaceted ecosystem of countermeasures against spoofing and jamming threats. Our evaluation of 30 seminal publications demonstrates that mitigation strategies span diverse domains—from foundational signal processing and hardware solutions to cryptographic protocols and algorithmic innovations—each exhibiting distinct operational trade-offs aligned with specific threat profiles. Notably, machine learning paradigms, especially deep neural architectures, have emerged as transformative tools, consistently outperforming conventional approaches in detecting sophisticated adversarial maneuvers. This performance advantage, however, introduces critical implementation compromises: while ML systems offer unparalleled adaptability to novel attack vectors, they demand substantial computational resources compared to traditional hardware-centric defenses. Application context further dictates strategy selection, with aviation, maritime operations, critical infrastructure, and military deployments necessitating specialized solutions due to their unique vulnerability

landscapes and operational constraints. Looking forward, the field is converging toward hybridized defense frameworks integrating adaptive ML techniques with next-generation authenticated signals, standardized security certifications, and resilient system architectures. As society's dependence on precise positioning and timing intensifies, continuous advancement of these protective measures—particularly ML-enhanced mechanisms—remains imperative to safeguard GNSS integrity against rapidly evolving adversarial capabilities.

REFERENCES

[1] J. Liu, F. Chen, Y. Xie, B. Ge, Z. Lu, and G. Sun, "Robust spoofing detection for GNSS array receivers using the auxiliary reference element method," IEEE Sensors J., 2024. doi: 10.1109/JSEN.2024.3369367.

[2] L. Meng, L. Yang, W. Yang, and L. Zhang, "A survey of GNSS spoofing and anti-spoofing technology," Remote Sens., vol. 14, no. 19, p. 4826, 2022. doi: 10.3390/rs14194826.

[3] M. L. Psiaki and T. E. Humphreys, "GNSS spoofing and detection," Proc. IEEE, vol. 104, no. 6, pp. 1258–1270, 2016. doi: 10.1109/JPROC.2016.2526658.

[4] D. Borio, F. Dovis, H. Kuusniemi, and L. Lo Presti, "Impact and detection of GNSS jammers on consumer grade satellite navigation receivers," Proc. IEEE, vol. 104, no. 6, pp. 1233–1245, 2016. doi: 10.1109/JPROC.2016.2543266.

[5] S. Bartl, M. Kadletz, P. Berglez, and T. Duša, "Mitigating the Threat of Jamming and Spoofing to Aeronautics," Inside GNSS, 2022.

[6] B. Motella, M. Pini, and M. Fantino, "Investigation on the effect of strong out-of-band signals on global navigation satellite systems receivers," GPS Solutions, vol. 12, pp. 77–86, 2008. doi: 10.1007/s10291-007-0085-5.

[7] M. L. Psiaki, B. W. O'Hanlon, J. A. Bhatti, D. P. Shepard, and T. E. Humphreys, "GPS spoofing detection via dual-receiver correlation of military signals," IEEE Trans. Aerosp. Electron. Syst., vol. 49, no. 4, pp. 2250–2267, 2013. doi: 10.1109/TAES.2013.6621814.

[8] R. T. Ioannides, T. Pany, and G. Gibbons, "Known vulnerabilities of global navigation satellite systems, status, and potential mitigation techniques," Proc. IEEE, vol. 104, no. 6, pp. 1174–1194, 2016. doi: 10.1109/JPROC.2016.2535898.

[9] A. Broumandan, A. Jafarnia-Jahromi, and G. Lachapelle, "Spoofing detection, classification and cancelation (SDCC) receiver architecture for a moving GNSS receiver," GPS Solutions, vol. 19, pp. 475–487, 2015. doi: 10.1007/s10291-014-0407-3.

[10] D. Borio, C. Gioia, G. Baldini, and J. Fortuny, "GNSS receiver classification based on double-differenced pseudorange measurements," GPS Solutions, vol. 20, pp. 821–833, 2016. doi: 10.1007/s10291-015-0485-x.

[11] D. M. Akos, "Who's afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control (AGC)," Navigation, vol. 59, no. 4, pp. 281–290, 2012. doi: 10.1002/navi.19.

[12] I. Fernández-Hernández, V. Rijmen, G. Seco-Granados, J. Simon, I. Rodríguez, and J. D. Calle, "A navigation message authentication proposal for the Galileo open service," Navigation, vol. 63, no. 1, pp. 85–102, 2016. doi: 10.1002/navi.125.

[13] E. Axell, F. M. Eklöf, P. Johansson, M. Alexandersson, and D. M. Akos, "Jamming detection in GNSS receivers: Performance evaluation of field trials," Navigation, vol. 60, no. 1, pp. 1–8, 2013. doi: 10.1002/navi.24.

[14] J. T. Curran, M. Bavaro, and J. Fortuny, "An authentication and integrity scheme for the Galileo E6-B signal," Navigation, vol. 64, no. 2, pp. 237–250, 2017. doi: 10.1002/navi.188.

[15] D. Borio and C. Gioia, "GNSS interference mitigation: A measurement and position domain assessment," Navigation, vol. 63, no. 2, pp. 173–193, 2016. doi: 10.1002/navi.138.

[16] D. Borio and C. Gioia, "GNSS interference detection and localization using a network of low cost front-end modules," Navigation, vol. 66, no. 1, pp. 95–116, 2019. doi: 10.1002/navi.277.

[17] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner, "Assessing the spoofing threat: Development of a portable GPS civilian spoofer," in Proc. ION GNSS Conf., 2008, pp. 2314–2325.

[18] A. Broumandan, A. Jafarnia-Jahromi, V. Dehghanian, J. Nielsen, and G. Lachapelle, "GNSS spoofing detection in handheld receivers based on signal spatial correlation," in Proc. IEEE/ION PLANS Symp., 2012, pp. 479–487. doi: 10.1109/PLANS.2012.6236917.

[19] K. Jansen, M. Schäfer, D. Moser, V. Lenders, C. Pöpper, and J. Schmitt, "Crowd-GPS-Sec: Leveraging crowdsourcing to detect and localize GPS spoofing attacks," in Proc. IEEE Symp. Security Privacy (SP), 2018, pp. 1018–1031. doi: 10.1109/SP.2018.00068.

[20] K. D. Wesson, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "An evaluation of the vestigial signal defense for civil GPS anti-spoofing," in Proc. ION GNSS Conf., 2011, pp. 2646–2656.

[21] M. Meurer, A. Konovaltsev, M. Cuntz, and C. Hättich, "Robust joint multi-antenna spoofing detection and attitude estimation using direction assisted multiple hypotheses RAIM," in Proc. ION GNSS Conf., 2012, pp. 3007–3016.

[22] M. L. Psiaki, S. P. Powell, and B. W. O'Hanlon, "GNSS spoofing detection using high-frequency antenna motion and carrier-phase data," in Proc. ION GNSS+ Conf., 2013, pp. 2949–2991.

[23] T. E. Humphreys, "Detection strategy for cryptographic GNSS anti-spoofing," IEEE Trans. Aerosp. Electron. Syst., vol. 49, no. 2, pp. 1073–1090, 2013. doi: 10.1109/TAES.2013.6494400.

[24] D. Borio, C. Gioia, and G. Baldini, "Asynchronous GNSS spoofing detection based on a multi-receiver GPS/Galileo software defined radio receiver," in Proc. ION GNSS+ Conf., 2015, pp. 3315–3325.

[25] D. Borio and C. Gioia, "Spoofing detection by a multi-constellation GNSS receiver with multiple antennas," in Proc. ION GNSS+ Conf., 2016, pp. 3068–3081.

[26] D. P. Shepard, J. A. Bhatti, T. E. Humphreys, and A. A. Fansler, "Evaluation of smart grid and civilian UAV vulnerability to GPS spoofing attacks," in Proc. ION GNSS Conf., 2012, pp. 3591–3605.

[27] Z. Wu, Y. Zhang, Y. Yang, C. Liang, and R. Liu, "Spoofing and anti-spoofing technologies of global navigation satellite system: A survey," IEEE Access, vol. 8, pp. 153 897–153 920, 2020. doi: 10.1109/ACCESS.2020.3017508.

[28] G. Panice, S. Luongo, G. Gigante, D. Pascarella, and C. Sacchi, "A deep learning-based approach for GNSS spoofing detection in mobile networks," IEEE Access, vol. 7, pp. 160 861–160 874, 2019. doi: 10.1109/ACCESS.2019.2951305.

[29] E. Shafiee, M. R. Mosavi, and M. Moazedi, "Detection of spoofing attack using machine learning based on multi-layer neural network in satellite navigation system," J. Navig., vol. 71, no. 1, pp. 169–188, 2018. doi: 10.1017/S0373463317000558.

[30] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "GPS vulnerability to spoofing threats and a review of antispoofing techniques," Int. J. Navig. Observ., vol. 2012, pp. 1–16, 2012. doi: 10.1155/2012/127072.