

Deceptive signal countermeasures in GNSS: Survey of signal processing spoofing detection techniques

Ankita R. Prajapati¹, Dr. Tushar P. Dave², Sheetal N. Tanna³

¹ Student of Master of Engineering, Electronics & Communication Department, Dr S & S S Gandhi Engineering College, Surat

² Professor, Electronics & Communication Department, Dr S & S S Gandhi Engineering College, Surat

³ Ph.D. Student, Electronics & Communication Department, Sardar Vallabhbhai Patel National Institute of Technology, Surat

Date of Submission: 27-03-2026

Date of Acceptance: 06-04-2026

ABSTRACT: Global Navigation Satellite Systems (GNSS) have become integral to modern infrastructure, enabling precise positioning, navigation, and timing across numerous applications. However, the increasing reliance on these systems has exposed them to sophisticated security threats, particularly spoofing attacks that broadcast counterfeit signals to deceive receivers into calculating false positions or times. This paper presents a comprehensive survey of signal processing-based spoofing detection techniques, which form the foundation of GNSS anti-spoofing countermeasures. We examine the fundamental principles of GNSS spoofing, categorize various attack methodologies, and provide an in-depth analysis of signal processing detection approaches including correlation function monitoring, power-based methods, antenna array processing, and time-frequency analysis. The survey covers traditional detection techniques, recent advancements including machine learning-enhanced methods, and comparative performance evaluations using standardized datasets such as TEXBAT. Our analysis reveals that while signal processing techniques offer effective detection against many attack types, their performance varies significantly based on attack sophistication, implementation complexity, and environmental conditions. We conclude by identifying research gaps and future directions for robust spoofing detection in next-generation GNSS receivers.

KEYWORDS: GNSS, spoofing detection, signal processing, correlation monitoring, power detection, antenna array, machine learning, TEXBAT

I. INTRODUCTION

Global Navigation Satellite Systems (GNSS), including GPS (United States), Galileo (Europe), BeiDou (China), and GLONASS (Russia), provide essential positioning, navigation, and timing services worldwide [1]. These systems have become

deeply embedded in critical infrastructure, from aviation and maritime navigation to financial networks and telecommunications synchronization. Unmanned systems, including aerial (UAVs) and ground vehicles (UGVs), particularly rely on GNSS for accurate positioning and control [2].

Despite their ubiquity, civilian GNSS signals remain inherently vulnerable due to three fundamental weaknesses: 1. publicly disclosed signal structures and modulation formats, 2. openly available navigation data formats, and 3. unprotected broadcast channels with extremely low received power levels (-150 dBW to -160 dBW) [3]. These vulnerabilities make GNSS an attractive target for malicious interference, particularly spoofing attacks.

Spoofing involves transmitting counterfeit signals that mimic authentic GNSS transmissions, tricking victim receivers into computing false positions, velocities, or times [4]. Unlike jamming, which simply disrupts reception, spoofing is covert and potentially more dangerous, as victims remain unaware of the deception. The threat materialized dramatically in 2011 when Iran reportedly captured a US RQ-170 surveillance drone through GNSS spoofing, forcing it to land in Iranian territory [5]. Subsequent demonstrations have shown successful spoofing attacks against yachts, smartphones, and civilian UAVs [6].

In response, researchers have developed numerous anti-spoofing techniques. Among these, signal processing-based methods have emerged as particularly promising approaches, leveraging various characteristics of received signals to identify anomalies indicative of spoofing attacks [7]. These techniques examine signal power, correlation function shape, angle of arrival, and time-frequency properties to discriminate between authentic and counterfeit signals.

This paper provides a comprehensive survey of signal processing-based spoofing detection techniques. We examine the theoretical foundations

of GNSS spoofing, categorize attack methodologies, analyze various detection approaches, and review recent advancements including machine learning-enhanced methods. The remainder of this paper is organized as follows: Section 2 describes GNSS spoofing principles and attack classifications; Section 3 presents signal processing detection techniques categorized by their operational principles; Section 4 discusses machine learning-enhanced approaches; Section 5 examines performance evaluation and datasets; Section 6 explores future research directions; and Section 7 concludes the paper.

II. GNSS SPOOFING: PRINCIPLES AND ATTACK CLASSIFICATIONS

GNSS signal model

A typical GNSS signal can be mathematically represented as [4]:

$$y(t) = \text{Re} \left\{ \sum_{i=1}^N A_i D_i [t - \tau_i(t)] C_i [t - \tau_i(t)] e^{j[\omega_c t - \phi_i(t)]} \right\}$$

where N is the number of signals, A_i is the carrier amplitude, D_i represents the data bits, C_i is the spreading code (typically BPSK PRN code), $\tau_i(t)$ is the code phase, ω_c is the nominal carrier frequency, and $\phi_i(t)$ is the beat carrier phase.

A spoofer generates counterfeit signals with similar structure [8]:

$$y_s(t) = \text{Re} \left\{ \sum_{i=1}^{N_s} A_{si} \hat{D}_i [t - \tau_{si}(t)] C_i [t - \tau_{si}(t)] e^{j[\omega_c t - \phi_{si}(t)]} \right\}$$

Typically, $N_s = N$, and each spoofed signal uses the same spreading code $C_i(t)$ as the corresponding authentic signal. The spoofed amplitudes A_{si} , code phases $\tau_{si}(t)$, and carrier phases $\phi_{si}(t)$ are manipulated to achieve the attacker's objectives.

Spoofing attack classification

Based on implementation complexity and strategy, spoofing attacks can be classified into three categories [6, 9]:

Simplistic Attacks: Using commercial GNSS signal simulators, these attacks broadcast counterfeit signals without synchronization to authentic signals. They typically require higher power to overcome

authentic signals and are relatively easy to detect due to abrupt changes in signal characteristics.

Intermediate Attacks (Receiver-based): These sophisticated attacks combine a GNSS receiver and transmitter. The receiver component monitors authentic signals, enabling the spoofer to synchronize counterfeit signals with genuine transmissions. Attackers gradually increase counterfeit signal power while maintaining alignment, then slowly drag the victim receiver to false positions [10].

Sophisticated Attacks: Using multiple phase-locked transmitters, these attacks can defeat angle-of-arrival defenses by broadcasting from multiple directions. Such attacks require coordinated multiple transmitters and precise phase synchronization, making them expensive and complex to implement.

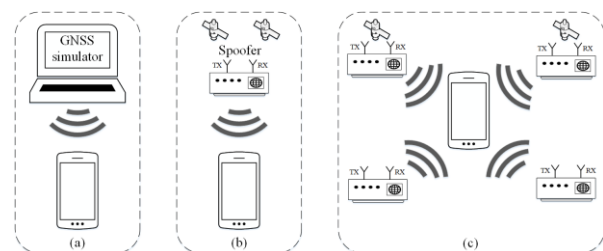


Figure 1: Types of spoofing attack: (a) simplistic, (b) intermediate, (c) sophisticated

Self-consistent spoofers design attacks to defeat legacy RAIM (Receiver Autonomous Integrity Monitoring) by synthesizing false code phases that induce desired false positions while maintaining small pseudo range residuals [4]. The attack sequence typically involves:

1. Initial alignment of spoofed signals with authentic signals at low power
2. Gradual power increase until capturing receiver tracking loops
3. Coordinated drag-off of code and carrier phases to false position

Alternative approaches include meaconing (record and replay) and SCER (Security Code Estimation and Replay) attacks, which handle unpredictable signal components [11].

III. SPOOFING DETECTION METHODS

GNSS signal spoofing detection methods have the primary goal of detecting spoofing attacks

Method	Type	Description
1. Signal Processing-Based	Correlation Function Monitoring	Examines distortion of the correlation function peak shape using various correlator outputs
	Power-Based Methods	Monitors absolute received power, AGC levels, and C/N ₀ for abnormal variations
	Antenna Array Processing	Uses multiple antennas to detect inconsistencies in signal direction and phase
	Time-Frequency Analysis	Analyzes signal timing and spectral characteristics to identify spoofing artifacts
2. Data Bit and Navigation Message	Data Bit Analysis	Monitors data bit streams for delays, unexpected sign changes, or authentication failures
	NMEA Message Analysis	Examines NMEA sentences (GSV, GGA, RMC) for inconsistencies in satellite data
3. Position Domain	Pseudorange Analysis	Verifies consistency among pseudorange measurements across different satellites
	Clock State Monitoring	Detects abnormal jumps or drift rates in receiver clock bias and timing
4. Drift Monitoring	Drift Monitoring	Compares GNSS-derived motion with IMU data and vehicle dynamic constraints
5. Encryption-Based	Encryption-Based Methods	Uses symmetric key encryption, spread spectrum security codes, and digital signatures
6. Machine Learning and Deep Learning	Supervised Learning	Applies SVM, KNN, decision trees, and XGBoost to classify spoofing using trained models
	Deep Learning	Employs CNN, GAN, LSTM, and MLP for automatic feature extraction and classification
	Features Used in ML Detection	Extracts signal power, correlation, pseudorange, and carrier phase features for ML models
7. Radio Frequency Fingerprinting (RFF)	Radio Frequency Fingerprinting (RFF)	Analyzes raw signal features before or after correlation to create unique transmitter fingerprints

Table 1: Categories of spoofing detection methods

to alert the receiver that its location and time data are not correct. It is necessary to understand the characteristics of different attacks to develop a good defense against the attack itself. A detailed categorization of spoofing detection methods is found below in Table 1.

1. Correlation function monitoring

During a spoofing attack, the total received signal includes both authentic and counterfeit components. The correlation function between the received signal and a local replica exhibits characteristic distortions [13]. When the spoofed

signal is aligned with or slightly offset from the authentic signal, the composite correlation peak becomes asymmetric or develops multiple peaks. Mathematically, the composite correlation function $R(\tau)$ can be expressed as:

$$R(\tau) = R_a(\tau) + R_s(\tau - \Delta\tau) + 2\sqrt{R_a(\tau)R_s(\tau - \Delta\tau)}\cos(\Delta\phi)$$

where $R_a(\tau)$ and $R_s(\tau)$ are the autocorrelation functions of authentic and spoofed signals respectively, $\Delta\tau$ is the code-phase offset between signals, and $\Delta\phi$ is the carrier phase difference. Correlation function monitoring can be further

classified into the different categories as suggested in Table 2.

Multi-Correlator Approaches: Modern receivers implement dozens of correlators at fine resolution, enabling detailed correlation function analysis. Turner et al. [16] demonstrated that increasing correlator outputs. This approach monitors the entire correlation function rather than discrete metrics, achieving superior detection sensitivity under various power conditions. Testing on TEXBAT scenarios showed accuracy improvement with low computational complexity.

Method	References
Signal Quality Monitoring (SQM)	Wesson et al., 2018; Fang et al., 2023
Multi-Correlator Techniques	Turner et al., 2020
Kolmogorov-Smirnov Test SQM	Zhou et al., 2024
Q-Channel Energy Detection	Wang et al., 2023
Ratio Metrics	Radoš et al., 2024
Delta Metric	Fang et al., 2023
Symmetric Difference	Fang et al., 2023

Table 2: Categories of Correlation function monitoring methods

Q-Channel Energy Detection: Wang et al. [15] developed a spoofing detection method based on abnormal quadrature (Q) channel energy. By estimating noise levels and monitoring Q-channel correlator outputs, their approach achieved at least 20% improvement in detection ratio compared to traditional SQM metrics when C/N_0 exceeded 32 dB-Hz. The Q energy detector performs particularly well against overpowered attacks.

Signal Quality Monitoring (SQM) Metrics: SQM employs various metrics to quantify correlation function distortion [14]:

1. Delta Metric: Compares early and late correlator outputs: $\Delta = (E - L)/(E + L)$
2. Ratio Metric: Examines ratio of prompt to early or late correlator values: $R\{E/P\} = E/P$, $R\{L/P\} = L/P$
3. Symmetric Difference Metric: Measures asymmetry about the prompt correlator: $S = (E - L)/P$

2. Power-Based Detection Methods

Power monitoring represents one of the simplest yet effective approaches for spoofing detection, based on the principle that spoofing signals typically require higher power to overcome authentic signals [3]. Power based detection method can be further classified into the different categories as suggested in Table 3.

Method	Key References
Received Power Monitoring (RPM)	Jafarnia-Jahromi et al., 2012; Broumandan et al., 2017
Automatic Gain Control (AGC) Analysis	Akos, 2012
Carrier-to-Noise Ratio (C/N_0) Monitoring	Jafarnia-Jahromi et al., 2012
Combined AGC & C/N_0 Detection	Radoš et al., 2024
Power-Distortion (PD) Detector	Wesson et al., 2018

Table 3: Categories of Power based detection methods

Received Power Monitoring (RPM): This technique examines total received power on an absolute scale by monitoring carrier amplitude values and Automatic Gain Control (AGC) settings [18]. A sudden power increase of more than 1-2 dB may indicate a spoofing attack, particularly when the spoofer requires substantial power advantage ($A_{si} \gg A_i$).

Carrier-to-Noise Ratio (C/N_0) Monitoring: Traditional spoofed signal detection based on C/N_0 compares measured values to expected ranges [19]. Jafarnia-Jahromi et al. demonstrated that absolute power tracking significantly reduces receiver vulnerability compared to techniques that only track relative C/N_0 variations.

AGC Analysis: Akos [20] showed that spoofing attacks cause high variations in receiver AGC gain levels. Monitoring AGC provides effective detection, particularly when combined with C/N_0 observations. As noted by Radoš et al. [12], if both AGC and C/N_0 decrease, jamming is more likely; if AGC decreases while C/N_0 remains constant or increases, spoofing is indicated.

Combined Power-Distortion Detection: Wesson et al. [13] developed power-distortion monitoring combining received power measurements with correlation function analysis. Their approach demonstrated effective detection against intermediate spoofing attacks but showed limitations

against highly overpowered attacks where distortion becomes minimal.

3. Antenna Array Processing

Multi-antenna techniques exploit spatial diversity to detect spoofing by examining signal direction of arrival [21]. Antenna array processing method can be further classified as suggested in Table 4.

Direction of Arrival (DoA) Estimation: Authentic GNSS signals arrive from different satellite directions distributed across the sky, while simplistic spoofers broadcast all signals from a single direction. DoA estimation using antenna arrays enables detection of this inconsistency [22].

Method	Key References
Direction of Arrival (DoA) Estimation	Magiera, 2019; Meurer et al., 2016
Carrier Phase Interferometry	Psiaki & Humphreys, 2016; Borio & Gioia, 2016
Controlled Reception Pattern Antenna (CRPA)	Meurer et al., 2016
Moving/Rotating Single Antenna	Chen et al., 2024
Coprime Array Processing	Zhao et al., 2022
Spatial Power Spectrum Estimation	Yang et al., 2023
Double-Differenced Carrier Phase	Yang et al., 2023

Table 4: Categories of Antenna array processing methods

Lee et al. [23] developed an antenna array-based method using compressed sensing for DoA estimation, successfully detecting sophisticated spoofing attacks. Yang et al. [24] proposed a six-array spoofing-interference-monitoring antenna that detects and identifies spoofing sources by monitoring correlation peaks and combining airspace-trapping algorithms.

Carrier Phase Interferometry: Using multiple antennas with known baselines, receivers can measure carrier phase differences to estimate signal arrival angles [25]. Psiaki et al. [4] demonstrated that a well-designed receiver can measure ϕ_i to approximately 1/40 cycle accuracy, enabling 3° direction accuracy with only 0.1 m baseline.

Moving Antenna Techniques: Chen et al. [26] proposed spoofing detection using the intersection angle between two directions of arrival (IA-DoA) with a single rotating antenna. This approach estimates IA-DoA between signal pairs using C/N₀ and Carrier Phase Single Difference (CPSD), proving effective while reducing hardware costs.

Coprime Array Processing: Zhao et al. [27] developed a coprime array-based method for spoofing detection with small time offset, achieving better DoA estimation accuracy without complex de-spreading operations by processing raw digital baseband signals.

4. Time-Frequency Analysis

Time-frequency techniques examine signal characteristics in joint domains to identify anomalies indicative of spoofing.

Time of Arrival (ToA) Analysis: GNSS positioning fundamentally relies on ToA ranging. Spoofed signals inherently have longer time of arrival than authentic signals due to processing delays [28]. Zhang and Zhan [29] developed a spoofing detection system based on Time Difference of Arrival Estimation (TDOAE) using two receivers. **Spectral Analysis:** Spoofing signals may introduce spectral artifacts detectable through Fourier or wavelet analysis. Morales Ferre et al. [30] used spectrogram analysis for jammer classification, achieving 94.90% accuracy with SVM methods.

Cross Ambiguity Function (CAF) Analysis: Borhani-Darian et al. [31] employed deep neural networks on CAF images for spoofing detection, achieving high success rates particularly at moderate to high signal-to-noise ratios.

IV. PERFORMANCE EVALUATION AND DATASETS

Standardized Test Datasets

Validating spoofing detection techniques requires standardized datasets with authentic and spoofed signals:

1. TEXBAT (Texas Spoofing Test Battery)

Developed by Humphreys et al. [44] at the University of Texas, TEXBAT provides eight spoofing scenarios with varying power levels, dynamics, and attack strategies. It has become the de facto standard for evaluating spoofing countermeasures.

2. OAKBAT (Oak Ridge Spoofing and Interference Test Battery)

Albright et al. [45] developed this complementary dataset containing GPS and Galileo spoofing scenarios, offering multiple test configurations for detection algorithm validation.

3. SatGrid Dataset

Foruhandeh et al. [46] provided real-time genuine and spoofing traces of GPS signals collected at different geographical locations, times, and environmental conditions.

Performance Metrics

Common metrics for evaluating signal processing detection include:

1. *Probability of Detection (PD)*: Likelihood of correctly identifying spoofing when present

2. *Probability of False Alarm (PFA)*: Likelihood of incorrectly declaring spoofing when absent

3. *Minimum Detectable Offset (MDO)*: Smallest code-phase offset reliably detectable

4. *Receiver Operating Characteristic (ROC)*: PD versus PFA across detection thresholds

5. *Computational Complexity*: Processing time, memory requirements, and power consumption

Comparative Analysis

Analysis of signal processing techniques using standardized datasets reveals [12, 17, 32]:

1. Traditional ratio metrics achieve $PD > 0.9$ for $\Delta\tau > 1$ chip but drop below 0.5 for $\Delta\tau < 0.5$ chips.
2. KS-test SQM maintains $PD > 0.85$ across all TEXTBAT scenarios.
3. Q-channel detection achieves 20% improvement over traditional methods in overpowered scenarios.
4. Antenna array methods provide robust detection against single-source attacks but require multiple antennas.
5. Multi-parameter fusion approaches outperform single-parameter methods by 15-25%

V. FUTURE RESEARCH DIRECTIONS

1. Multi-Technique Fusion

Combining complementary signal processing techniques offers enhanced robustness. Integration of correlation monitoring, power

analysis, antenna array processing, and machine learning classification can create layered defenses against sophisticated attacks [47]. Truong et al. [48] demonstrated that clock bias monitoring can complement signal processing techniques, particularly when the spoofer cannot perfectly synchronize with authentic signals.

2. Real-Time Implementation Challenges

Computational complexity remains a barrier for advanced signal processing techniques in resource-constrained receivers. Efficient algorithms for multi-correlator processing, optimized antenna array processing, and lightweight machine learning models are needed for practical deployment in mobile and embedded systems [12].

3. Next-Generation GNSS Signals

Modernized GNSS signals (GPS L1C, L5; Galileo E1, E5; BeiDou B1C, B2a) incorporate advanced modulation schemes (BOC, MBOC, AltBOC) that modify correlation function characteristics. Signal processing techniques must adapt to these new signal structures while maintaining detection effectiveness [49].

4. Standardized Evaluation Frameworks

The research community would benefit from standardized evaluation frameworks enabling fair comparison of detection techniques. This includes common datasets, performance metrics, testing protocols, and benchmark implementations [44].

5. Cognitive and Adaptive Receivers

Future receivers may incorporate cognitive capabilities that dynamically adapt signal processing strategies based on observed threat levels and environmental conditions. Machine learning enables receivers to learn and recognize new attack patterns over time [31].

VI. CONCLUSION

Signal processing techniques form the foundation of GNSS spoofing detection, offering diverse approaches to identify counterfeit signals by examining their distinctive characteristics. This survey has examined the theoretical foundations of GNSS spoofing, categorized attack methodologies, and provided comprehensive analysis of signal processing detection techniques including correlation function monitoring, power-based methods, antenna array processing, time-frequency analysis, and machine learning-enhanced approaches.

Correlation monitoring techniques, particularly enhanced SQM methods like KS-test monitoring and Q-channel energy detection, provide effective detection across a wide range of attack conditions. Power-based methods offer simplicity and computational efficiency but may struggle against sophisticated low-power attacks. Antenna array processing provides robust spatial discrimination but requires additional hardware. Machine learning approaches achieve high detection accuracy but require representative training data and careful validation.

The evolution of spoofing attacks continues to challenge detection capabilities, driving ongoing research into more sophisticated countermeasures. Future work should focus on multi-technique fusion, real-time implementation optimization, adaptation to next-generation GNSS signals, and standardized evaluation frameworks. As GNSS dependency grows across critical infrastructure, robust signal processing-based spoofing detection remains essential for ensuring reliable positioning, navigation, and timing services in an increasingly contested electromagnetic environment.

REFERENCES

- [1] L. Meng, L. Yang, W. Yang, and L. Zhang, "A survey of GNSS spoofing and anti-spoofing technology," *Remote Sensing*, vol. 14, no. 19, p. 4826, 2022.
- [2] 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. 165444-165496, 2020.
- [3] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "GPS vulnerability to spoofing threats and a review of antispoofing techniques," *International Journal of Navigation and Observation*, vol. 2012, 2012.
- [4] M. L. Psiaki and T. E. Humphreys, "GNSS spoofing and detection," *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1258-1270, 2016.
- [5] D. P. Shepard, T. E. Humphreys, and A. A. Fansler, "Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks," *International Journal of Critical Infrastructure Protection*, vol. 5, no. 3-4, pp. 146-153, 2012.
- [6] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner Jr, "Assessing the spoofing threat: Development of a portable GPS civilian spoofer," in *Proceedings of the 21st International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2008)*, 2008, pp. 2314-2325.
- [7] L. Huang, "Anti-spoofing techniques for GNSS receiver," *Geomatics and Information Science of Wuhan University*, vol. 36, no. 11, pp. 1344-1347, 2011.
- [8] L. Huang, H. Gong, X. Zhu, and F. Wang, "Research of re-radiating spoofing technique to GNSS timing receiver," *Journal of National University of Defense Technology*, vol. 35, no. 4, pp. 93-96, 2013.
- [9] E. Garbin Manfredini, "Signal processing techniques for GNSS anti-spoofing algorithms," Ph.D. dissertation, Polytechnic University of Turin, 2017.
- [10] T. E. Humphreys, "Detection strategy for cryptographic GNSS anti-spoofing," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 49, no. 2, pp. 1073-1090, 2013.
- [11] F. Gallardo and A. P. Yuste, "SCER spoofing attacks on the Galileo open service and machine learning techniques for end-user protection," *IEEE Access*, vol. 8, pp. 85515-85532, 2020.
- [12] K. Radoš, M. Brkić, and D. Begušić, "Recent advances on jamming and spoofing detection in GNSS," *Sensors*, vol. 24, no. 13, p. 4210, 2024.
- [13] K. D. Wesson, J. N. Gross, T. E. Humphreys, and B. L. Evans, "GNSS signal authentication via power and distortion monitoring," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 54, no. 2, pp. 739-754, 2018.
- [14] J. Fang, J. Yue, B. Xu, and L.-T. Hsu, "A post-correlation graphical way for continuous GNSS spoofing detection," *Measurement*, vol. 216, p. 112974, 2023.
- [15] J. Wang, X. Tang, P. Ma, J. Wu, C. Ma, and G. Sun, "GNSS spoofing detection using Q channel energy," *Remote Sensing*, vol. 15, no. 21, p. 5337, 2023.
- [16] M. Turner, S. Wimbush, C. Enneking, and A. Konovaltsev, "Spoofing detection by distortion of the correlation function," in **2020 IEEE/ION Position, Location and Navigation Symposium (PLANS)**, 2020, pp. 566-574.
- [17] W. Zhou, Z. Lv, G. Li, B. Jiao, and W. Wu, "Detection of spoofing attacks on global navigation satellite systems using Kolmogorov-Smirnov test-based signal quality monitoring method," *IEEE Sensors Journal*, vol. 24, no. 7, pp. 10474-10490, 2024.
- [18] A. Broumandan, R. Siddakatte, and G. Lachapelle, "An approach to detect GNSS spoofing," *IEEE Aerospace and Electronic Systems Magazine*, vol. 32, no. 8, pp. 64-75, 2017.
- [19] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "GPS spoofer

- countermeasure effectiveness based on using signal strength noise power and C/N_0 observables," *International Journal of Satellite Communications and Networking*, vol. 30, no. 4, pp. 181-191, 2012.
- [20] 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.
- [21] J. Magiera, "A multi-antenna scheme for early detection and mitigation of intermediate GNSS spoofing," *Sensors*, vol. 19, no. 10, p. 2411, 2019.
- [22] M. Meurer, A. Konovaltsev, M. Appel, and M. Cuntz, "Direction-of-arrival assisted sequential spoofing detection and mitigation," in *Proceedings of the 2016 International Technical Meeting of the Institute of Navigation*, 2016, pp. 536-546.
- [23] Y.-S. Lee, J. S. Yeom, and B. C. Jung, "A novel array antenna-based GNSS spoofing detection and mitigation technique," in *2023 IEEE 20th Consumer Communications & Networking Conference (CCNC)*, 2023, pp. 489-492.
- [24] H. Yang, R. Jin, W. Xu, L. Che, and W. Zhen, "Satellite navigation spoofing interference detection and direction finding based on array antenna," *Sensors*, vol. 23, no. 3, p. 1604, 2023.
- [25] D. Borio and C. Gioia, "A sum-of-squares approach to GNSS spoofing detection," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 52, no. 4, pp. 1756-1768, 2016.
- [26] S. Chen, S. Ni, T. Lei, L. Cheng, and X. Song, "GNSS spoofing detection via the intersection angle between two directions of arrival in a single rotating antenna," *Sensors*, vol. 24, no. 4, p. 1116, 2024.
- [27] Y. Zhao, F. Shen, D. Xu, and Z. Meng, "A coprime array-based technique for spoofing detection and DoA estimation in GNSS," *IEEE Sensors Journal*, vol. 22, no. 22, pp. 22828-22835, 2022.
- [28] V. Truong, A. Vervisch-Picois, J. Rubio Hernan, and N. Samama, "Characterization of the ability of low-cost GNSS receiver to detect spoofing using clock bias," *Sensors*, vol. 23, no. 5, p. 2735, 2023.
- [29] Z. Zhang and X. Zhan, "Statistical analysis of spoofing detection based on TDOA," *IEEE Transactions on Electrical and Electronic Engineering*, vol. 13, no. 6, pp. 840-850, 2018.
- [30] R. Morales Ferre, A. de la Fuente, and E. S. Lohan, "Jammer classification in GNSS bands via machine learning algorithms," *Sensors*, vol. 19, no. 22, p. 4841, 2019.
- [31] P. Borhani-Darian, H. Li, P. Wu, and P. Closas, "Detecting GNSS spoofing using deep learning," *EURASIP Journal on Advances in Signal Processing*, vol. 2024, no. 1, p. 14, 2024.
- [32] Z. Chen, J. Li, J. Li, X. Zhu, and C. Li, "GNSS multi-parameter spoofing detection method based on support vector machine," *IEEE Sensors Journal*, vol. 22, no. 18, pp. 17864-17874, 2022.
- [33] S. Semajski, L. Semajski, W. De Wilde, and S. Gautama, "Use of supervised machine learning for GNSS signal spoofing detection with validation on real-world meaconing and spoofing data—Part II," *Sensors*, vol. 20, no. 7, p. 1806, 2020.
- [34] T. T. Khoei, A. Gasimova, M. A. Ahajjam, K. A. Shamaileh, V. Devabhaktuni, and N. Kaabouch, "A comparative analysis of supervised and unsupervised models for detecting GPS spoofing attack on UAVs," in *2022 IEEE International Conference on Electro Information Technology (eIT)*, 2022, pp. 279-284.
- [35] J. Li, W. Li, S. He, Z. Dai, and Q. Fu, "Research on detection of spoofing signal with small delay based on KNN," in *2020 IEEE 3rd International Conference on Electronics Technology (ICET)*, 2020, pp. 625-629.
- [36] A. Elango, S. Ujan, and L. Ruotsalainen, "Disruptive GNSS signal detection and classification at different power levels using advanced deep-learning approach," in *2022 International Conference on Localization and GNSS (ICL-GNSS)**, 2022, pp. 1-7.
- [37] Z. Wu, Y. Zhao, Z. Yin, and H. Luo, "Jamming signals classification using convolutional neural network," in *2017 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT)*, 2017, pp. 62-67.
- [38] J. Li, X. Zhu, M. Ouyang, W. Li, Z. Chen, and Q. Fu, "GNSS spoofing jamming detection based on generative adversarial network," *IEEE Sensors Journal*, vol. 21, no. 20, pp. 22823-22832, 2021.
- [39] E. Shafiee, M. R. Mosavi, and M. Moazedi, "Detection of spoofing attack using machine learning based on multi-layer neural network in single-frequency GPS receivers," *Journal of Navigation*, vol. 71, no. 1, pp. 169-188, 2018.
- [40] M. Marchand, A. Toumi, G. Seco-Granados, and J. A. López-Salcedo, "Machine learning assessment of anti-spoofing techniques for GNSS receivers," in **WIPHAL 2023: Work-in-Progress in Hardware and Software for Location Computation**, CEUR Workshop Proceedings, 2023.
- [41] D. R. Kartchner, R. Palmer, and S. K. Jayaweera, "Satellite navigation anti-spoofing using deep learning on a receiver network," in *2021 IEEE Cognitive Communications for Aerospace Applications Workshop*, 2021, pp. 1-5.
- [42] A. Siemuri, K. Selvan, H. Kuusniemi, P. Valisuo, and M. S. Elmusrati, "A systematic review of machine learning techniques for GNSS use cases," *IEEE Transactions on Aerospace and*

Electronic Systems, vol. 58, no. 6, pp. 5043-5077, 2022.

[43] B. Pardhasaradhi, R. R. Yakkati, and L. R. Cenkeramaddi, "Machine learning-based screening and measurement to measurement association for navigation in GNSS spoofing environment," *IEEE Sensors Journal*, vol. 22, no. 23, pp. 23423-23435, 2022.

[44] T. E. Humphreys, J. A. Bhatti, D. P. Shepard, and K. D. Wesson, "The Texas spoofing test battery: Toward a standard for evaluating GPS signal authentication techniques," in *Proceedings of the 25th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2012)*, 2012, pp. 3569-3583.

[45] A. Albright, S. Powers, J. Bonior, and F. Combs, "Oak Ridge Spoofing and Interference Test Battery (OAKBAT)—GPS," Oak Ridge National Laboratory (ORNL), 2020.

[46] M. Foruhandeh, A. Z. Mohammed, G. Kildow, R. Gerdes, and R. Berges, "SatGrid dataset, realtime genuine and spoofing traces of GPS signals collected at different geographical locations, times and environmental conditions," University Libraries, Virginia Tech, 2020.

[47] K. Liu, W. Wu, Z. Wu, L. He, and K. Tang, "Spoofing detection algorithm based on pseudorange differences," *Sensors*, vol. 18, no. 9, p. 3197, 2018.

[48] V. Truong, A. Vervisch-Picois, J. Rubio Hernan, and N. Samama, "Characterization of the ability of low-cost GNSS receiver to detect spoofing using clock bias," *Sensors*, vol. 23, no. 5, p. 2735, 2023.

[49] J. T. Curran, M. Navarro, M. Anghileri, P. Closas, and S. Pfletschinger, "Coding aspects of secure GNSS receivers," *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1271-1287, 2016.