Empirical Evaluation of GNSS Timing Spoofing and Detection Using Machine Learning

Empirical Evaluation of GNSS Timing Spoofing and Detection Using Machine Learning

Muhammad Safi[1 2], Heidi Kuusniemi[1 2 3], Mahmoud Elsanhoury[2], Petri Välisuo[2]
[1] *Department of Electrical Engineering, Tampere University*, Tampere, Finland
[2] *School of Technology and Innovations ,University of Vaasa* ,Vaasa, Finland
[3] *Finnish Geospatial Research Institute, National Land Survey*, Espoo Finland
msafi60k@gmail.com, heidi.kuusniemi@tuni.fi, mahmoud.elsanhoury@uwasa.fi, petri.valisuo@uwasa.fi

***Abstract*— This paper presents an empirical analysis of GNSS timing spoofing detection using data from Jammertest 2024. While positioning spoofing has been extensively studied, timing spoofing presents unique threats to critical infrastructure including power grids, telecommunications, and financial systems. Our analysis reveals that position parameters become compromised at lower spoofing power levels (20-25 dBm) compared to timing parameters (30 dBm), creating potential for early warning systems. Traditional carrier-to-noise ratio methods proved unreliable, while validity flags in NMEA messages showed strong but incomplete detection capability. To address detection gaps, we implemented an unsupervised Isolation Forest algorithm achieving perfect recall (100%) and high specificity (99.96%) without requiring extensive labeled examples. A combined approach leveraging both validity flags and machine learning is able to offer robust protection with minimal computational overhead. Our findings demonstrate practical robustness measures for timing-dependent critical infrastructure and how it can be implemented.**

Keywords*— *GNSS, GPS, Machine Learning (ML), Unsupervised, Timing Spoofing, Time synchronization

I. INTRODUCTION

Global Navigation Satellite Systems (GNSS) provide critical timing synchronization services essential for modern infrastructure including power grids, telecommunications networks, financial systems, and transportation [1]. These systems rely on precise timing with nanosecond-level accuracy for coordinated operations across geographically dispersed components [2]. In Finland alone, where electricity generation is projected to reach 15 TWh by 2035 [3], the energy sector's dependence on precise timing synchronization creates significant vulnerability to GNSS disruptions.

Recent incidents highlight the growing threat landscape. Commercial aircraft have experienced loss of onboard digital communication systems due to timing spoofing [4], while critical infrastructure including power grids and financial networks face increasing risks from sophisticated attacks targeting their timing dependencies [5], [6]. The European Union has identified GNSS timing as a critical vulnerability, with spoofing incidents in the Baltic region rising by 35% in the past year [7].

Despite increased awareness of these vulnerabilities, effective real-time detection and mitigation of timing spoofing attacks remain challenging. Current approaches primarily focus on theoretical models or laboratory settings, with limited field testing under realistic conditions [8]. While various detection methods have been proposed, from signal processing techniques to machine learning approaches, their effectiveness against real-world timing spoofing specifically (as opposed to positioning spoofing) lacks comprehensive empirical validation [9].

This paper addresses this gap by analyzing empirical data from Jammertest 2024, focusing specifically on GNSS timing spoofing detection.

II. RELATED WORK

A. Timing Spoofing Attack Vectors

GNSS timing spoofing methods include production spoofing (falsified signals maintaining position accuracy) [10], forwarding spoofing (delayed authentic signals) [11], and gradual self-synchronization spoofing (covert timing control) [12]. [13] categorized spoofing algorithms as pseudorange modification, satellite position modification, and combined approaches. Timing attacks can cause errors exceeding 36.5μs with minimal location displacement (<248.6m), violating IEEE C37.118 standards [14] and potentially causing power grid blackouts through timing synchronization attacks [15].

B. Traditional Detection Approaches

Detection methods include signal processing, data bit, and positioning analyses [16]. Signal processing examines C/N_0 [17], with AGC providing more reliable early detection [18]. [19] implemented a jitter detection system using an oscillator that activates when jitter exceeds 0.2μs. Additional methods include antenna arrays and correlation peak monitoring [16].

Data bit approaches analyze navigation message content. [20] identified timing discrepancies in NMEA messages (GGA, RMC, VTG), while [21] developed NMEA-based Anomaly detection (MANA) for anomaly detection without hardware modifications. Time of Arrival (ToA) and Direction of Arrival (DoA) techniques also detect spoofing [16].

Positioning methods analyze derived measurements. [22] achieved 99.99% detection using pseudorange double-differences between dual receivers, while [23] presented Separate Clock Drift Matched Filter (SCD-MF) for analyzing synchronicity patterns with minimal computational requirements.

C. AI-Based Detection Methods

ML or Machine learning approaches have shown promising results. [24] found Classification and Regression Trees (CART) most effective among nine ML models, similar to [25] who applied statistical runs tests to GPS signal Power Spectral Density (PSD) data (>95% detection on CART). [26] extracted seven features from GPS receivers, achieving >99% accuracy for power grid timing attacks.

Deep learning implementations include Long Short-Term Memory (LSTM) networks for NTP attack detection [27] and neural networks with correlation coefficient screening [28], achieving F1 scores >99% with <10μs response times. For reinforcement learning, [29] developed DQN-based detection

with near-perfect accuracy, though not for timing but for location spoofing.

D. Research Gap

Despite significant advances, several gaps remain in GNSS timing spoofing detection research. Most studies rely on simulated data or laboratory environments rather than field-collected data from real spoofing events [30]. The focus has predominantly been on positioning spoofing, with timing spoofing receiving comparatively less attention despite its critical infrastructure implications [31]. Additionally, unsupervised learning approaches remain underexplored for timing spoofing specifically, despite their potential advantage in detecting novel and genuine attack patterns without prior examples [32].

This research addresses these gaps by analyzing actual field data from Jammertest 2024, focusing specifically on timing spoofing detection, and implementing an unsupervised Isolation Forest algorithm, which hasn't been used in timing spoofing context to identify anomalous timing behavior without requiring extensive labeled training examples.

III. Jammertest 2024 Dataset

Jammertest is an annual event held in Andøya, Norway that serves as the world's largest open test for PNT/GNSS resilience against real-world interference [33]. The event is organized in collaboration with Norwegian national agencies including the Public Roads Administration, Communications Authority, and Defense Research Establishment.

The data for this study was collected during Jammertest 2024 using a u-blox ZED-F9P-00b-02 GNSS receiver, which can process signals from multiple satellite constellations across various frequency bands [34]. While the receiver includes anti-spoofing capabilities such as Galileo Open Service Navigation Message Authentication (OSNMA), these features were disabled during testing to evaluate baseline vulnerability.

Our analysis focuses specifically on Event 2.4.2 from Jammertest, which targeted GNSS timing with systematically increasing spoofing power. The test employed a cigarette-type GNSS spoofer positioned 34.91 meters from the receiver, targeting multiple GNSS bands (L1, L2, L5, E1, E5a, and E5b). The data spans 1 hour, 27 minutes (07:17-08:45 UTC), with the timing spoofing segment occurring from 07:04 UTC to 07:32 UTC. The total amount of time spoofed data was approximately 28 minutes on which various tests and analysis were conducted.

During the spoofing test, the spoofer implemented a 15-minute (900 seconds) time offset from actual time, with transmission power incrementing by 5 dBm every two minutes, starting at -35 dBm and increasing to 30 dBm. The spoofed signals successfully maintained the receiver's position fix while manipulating timing information, a sophisticated approach that makes detection particularly challenging. Table I summarizes the experimental parameters for the critical time spoofing segment.

TABLE I. Parameters of Timing Spoofing Event

Parameter	Value
Receiver	u-blox ZED-F9P-00b-02
Spoofer Type	stationary
Distance to Receiver	34.91 meters
Spoofing Duration	28 minutes (07:04-07:32 UTC)
Spoofing Power Range	-35 dBm to 30 dBm (5 dBm steps)
Time Offset Magnitude	15 minutes ahead
Targeted GNSS Bands	L1, L2, L5, E1, E5a, E5b

IV. Parameter Analysis During Spoofing

We analyzed the u-blox receiver data using the pyubx2 library [37] to extract and examine key GNSS parameters during the timing spoofing event. This analysis focused on both navigation-level data (NMEA messages) and raw measurements to identify distinctive signatures of timing attacks that could inform detection strategies.

A. Timing and Power Threshold Analysis

The primary indicator of timing spoofing was observed in the GNRMC (Required Minimum Specific) NMEA messages [38], which contain essential navigation data including time, position, and velocity. By establishing a baseline of expected timestamp progression and comparing it against the receiver's reported time, we identified a significant time jump during the attack period as shown in figure 1.

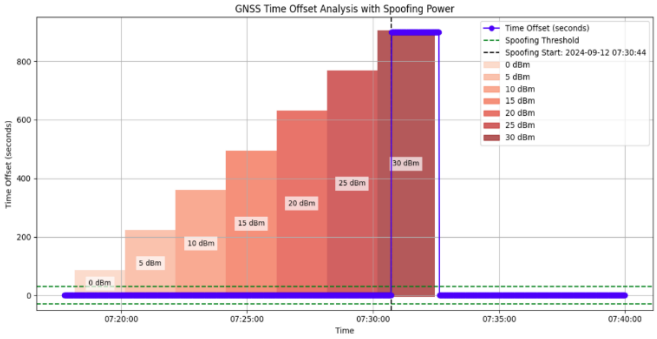

Fig. 1. Graph showing different spoofing power effects

Figure 1 shows that timing spoofing occurred between 07:30:44 UTC and 07:32:37 UTC, lasting approximately 1.88 minutes. This corresponds precisely with the period when the spoofer reached maximum power (30 dBm), demonstrating the receiver's significant resilience to lower-power spoofing attempts. The receiver required approximately 34 seconds of exposure to the 30 dBm signal before accepting the spoofed time and returned to normal timing approximately 10 seconds after the spoofing ended.

B. Position and Speed Effects

An unexpected finding was that position and speed parameters were compromised before timing synchronization was affected. We converted latitude and longitude data to local north-east coordinates to better visualize subtle position shifts in meters.

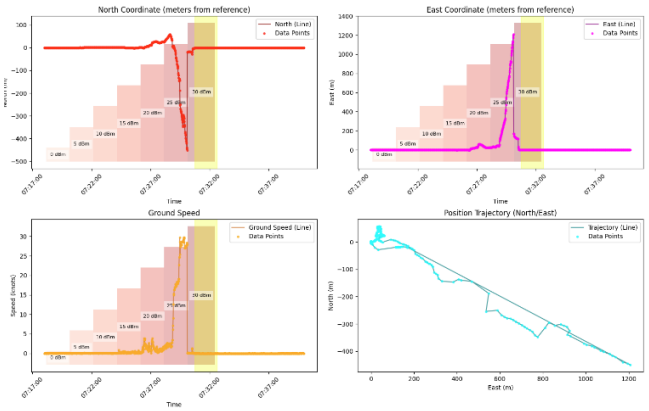

Fig. 2. Location parameters change during the spoofing event

Figure 2 shows that position spoofing began when the spoofer transmitted at 20-25 dBm, significantly before the 30 dBm required for timing manipulation. The yellow area is when the time of receiver was spoofed. During this period, the receiver reported physically impossible movements, appearing to travel approximately 1200 meters east and 400 meters south within one minute, reaching speeds up to 30 knots before abruptly stopping. Horizontal Dilution of Precision (HDOP) which is a measure of satellite geometry [39] also spiked during the spoofing event.

C. *Raw Measurement Analysis*

The most revealing insights came from analyzing raw measurements contained in RXM-RAWX messages, particularly pseudorange (C1C), carrier-to-noise ratio (S1C), and Doppler shift (D1C). We created a RINEX (Receiver Independent Exchange Format) file from the .ubx data to systematically analyze these parameters across different satellite constellations (GPS/G, Galileo/E, GLONASS/R, and BeiDou/C).

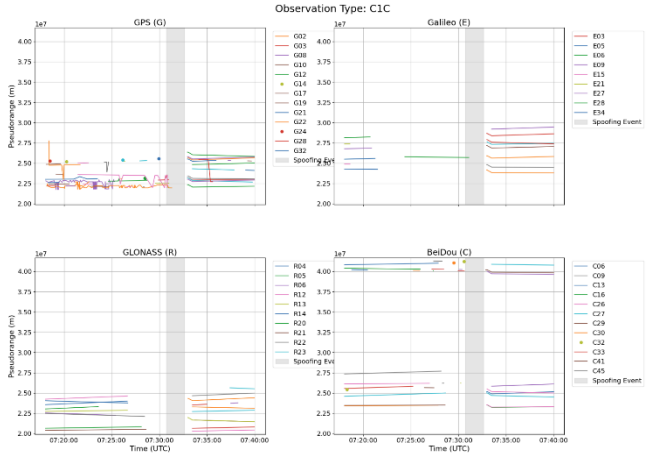

Fig. 3. Pseudoranges during the spoofing event.

Pseudoranges observations revealed a critical signature: during the timing spoofing window, the receiver recorded almost no valid raw measurement data. GLONASS signals disappeared several minutes before the time jump, followed by BeiDou, while only minimal GPS and Galileo measurements were intermittently available. Within 10 seconds after spoofing ceased, all constellations became visible again. This pattern of raw data suppression provides a distinctive attack signature.

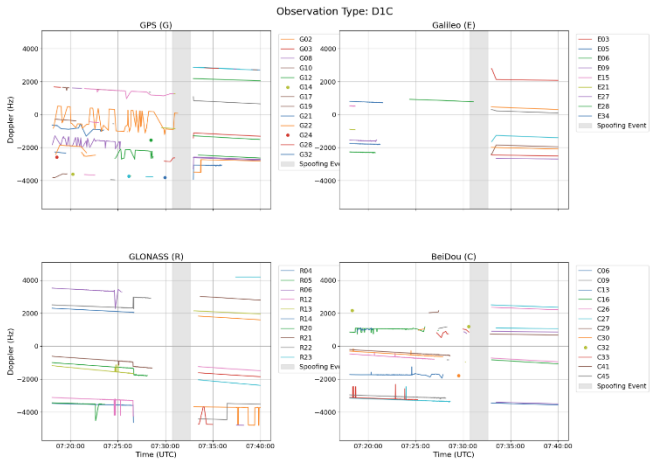

Fig. 4. Doppler Shift during the spoofing event

Doppler shift analysis revealed oscillating patterns in GPS signals prior to the attack, indicating changing relative satellite velocities, while Galileo showed more stable measurements. GLONASS and BeiDou exhibited abrupt changes and unusual patterns with rapid fluctuations before signal loss, providing potential early indicators of spoofing activity.

V. Spoofing Detection and Evaluation

The timing spoofing was detected using both traditional and AI methods.

A. *Traditional Detection*

Firstly, the signal-based detection method was utilized. Signal-based detection we used analyzes carrier-to-noise ratio (C/N_0) measurements to identify anomalous signal strength patterns. While previous research suggests C/N_0 typically increases during spoofing [10], our analysis revealed inconsistent behavior.

Fig. 5. C/N_0 during the spoofing period

During spoofing, most satellites exhibited signal loss rather than strength increases. While satellite G03 briefly showed elevated C/N_0 values, the sparse measurement availability during the attack period complicated pattern recognition. The inconsistent C/N_0 behavior across constellations (GPS maintaining stronger signals than GLONASS or BeiDou) rendered this approach unreliable for timing spoofing detection in our scenario

The positioning approach examined pseudorange RMS errors extracted from RXM-MEASX messages. These errors represent statistical deviations between expected and actual signal readings, which typically increase during spoofing events [40], [41].

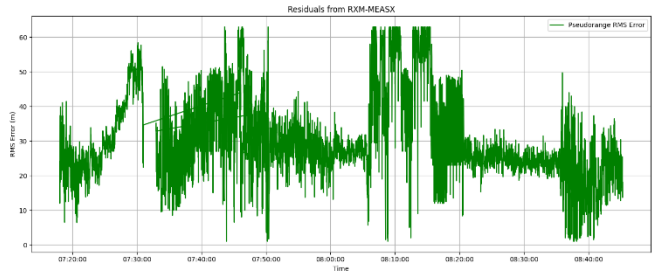

Fig. 6. Pseudorange RMS errors

Our analysis revealed distinctive straight-line patterns during spoofing periods, caused by measurement unavailability rather than elevated errors. While not designed explicitly for spoofing detection, these patterns provide clear anomaly signatures that successfully identified the timing attack window.

Lastly, the most effective traditional approach leveraged the validity flag bit in GNRMC (Recommended Minimum Specific GNSS Data) NMEA messages. In these messages, "A" indicates an Autonomous valid solution while "V" signifies an invalid solution.

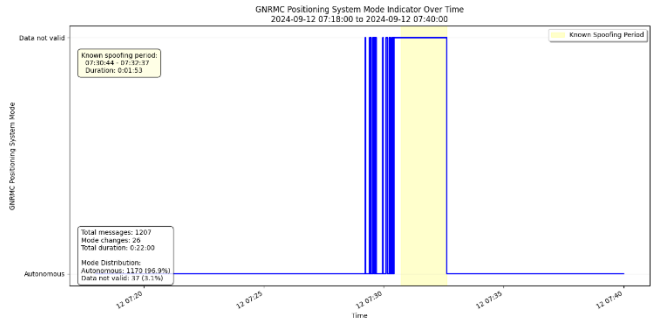

Fig. 7. GNRMC message status

The validity flag correctly identified the entire spoofing region, marking all affected messages as invalid. Notably, the receiver began flagging messages as invalid before timing was compromised, providing early warning when position data was affected. During evaluation, this approach achieved perfect detection of spoofing periods where NMEA messages were available.

The primary limitation was data availability, during approximately two minutes of the most intense spoofing, very few NMEA messages were generated, creating a detection gap that necessitated our machine learning approach

B. *AI Detection*

To address the limitations of traditional methods, we implemented an Isolation Forest algorithm, an unsupervised anomaly detection technique particularly suited for spoofing detection where labeled attack data is scarce [43]. We selected it for several key advantages: unsupervised operation without requiring extensive labeled examples, linear time complexity with minimal memory requirements, and demonstrated superior performance in related GNSS applications. In literature, [42] reported 95.85% accuracy in UAV GPS spoofing detection using similar approaches.

We constructed a dataset with 15 potential features extracted from RINEX and UBX files, focusing on raw signal characteristics and their derivatives as these manifest the earliest signs of spoofing. The validity flag was intentionally excluded to prevent data leakage and ensure independence from the internal detector.

The dataset was split into training (60%), validation (20%), and testing (20%) datasets, with outlier removal using Z-score filtering [44] to preserve the limited anomaly samples while eliminating extreme values.

We employed grid search to optimize key hyperparameters as shown in (1).

$$\Theta^* = \{t^*, \psi^*, \lambda^*, \alpha^*, \beta^*\} = \text{argmax}_\Theta \text{F1}\left(y_V, f_\Theta(X_V)\right) \quad (1)$$

Where,

- n_estimators (t): 100 trees
- max_samples (ψ): 0.7 (70% of data sampled per tree)
- max_features (λ): 0.9 (90% of features considered per split)
- contamination (α): 0.005 (expected proportion of anomalies)
- bootstrap (β): False (sampling without replacement)

C. *Results of AI based detection*

The Isolation Forest algorithm achieved exceptional performance when evaluated on the test dataset:

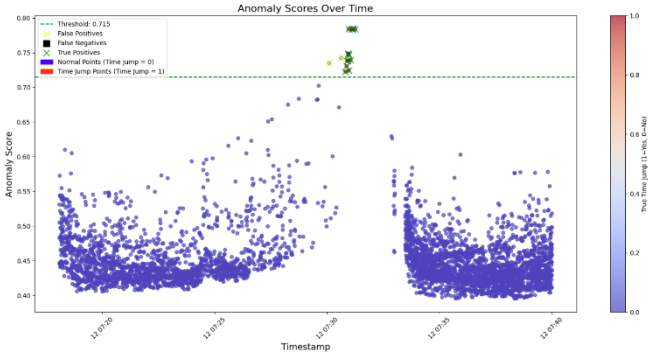

Fig. 8. Anomaly score distribution

TABLE II. RESULT METRICS OF ISOLATION FOREST

Metric	Value
Precision	0.8750
Recall	1.0000
F1-score	0.9333
Specificity	0.9996
False Positive Rate	0.0004
Accuracy	0.9996

The confusion matrix shows:

TABLE III. CONFUSIION MATRIX

	Predicted Normal	Predicted Spoofing
Actual Normal	4693	2
Actual Spoofing	0	14

The algorithm successfully identified all 14 spoofing instances (100% recall) while generating only 2 false positives from 4,695 normal samples (99.96% specificity). This perfect recall is particularly significant for security applications, where missed detections carry higher operational risks than false alarms [45]. [44] reported 95.85% accuracy for UAV spoofing detection using Isolation Forest, while our implementation achieved 99.96%, although the conditions may vary.

While both the validity flag and Isolation Forest methods independently demonstrated strong performance, each had complementary strengths. The validity flag excelled during moderate spoofing but failed during peak spoofing when NMEA messages were unavailable. Conversely, the Isolation Forest maintained detection capability throughout by leveraging raw measurement data, even when only one or two satellites remained visible. A combined system is proposed where validity flag provides primary detection with early warning capability, while the Isolation Forest algorithm fills detection gaps during periods of message unavailability.

VI. IMPLEMENTATION CONSIDERATIONS AND APPLICATIONS

Our detection methodologies present both significant potential and practical challenges for critical infrastructure protection. The Isolation Forest algorithm demonstrated efficient performance with minimal overhead, requiring approximately 22 MB of storage, suitable for almost all modern micro-controllers, though may require some adjustment if it is to be implemented directly on the receivers. For resource-constrained environments, we propose a tiered implementation where the low-cost validity flag serves as an initial trigger for machine learning analysis only when suspicious conditions are detected.

Despite the algorithm's high specificity (99.96%), real-world deployment must include protocols for managing false positives without compromising normal operations. This is especially critical in timing-sensitive applications where service interruptions can have cascading effects.

This work offers valuable protection for four critical sectors: Telecommunications networks, particularly 5G infrastructure with complex synchronization requirements [46]; Power grid systems where phasor measurement units rely on precise timing for grid stability [47]; Financial services where microsecond-level timing accuracy ensures transaction integrity [48]; and Transportation systems facing increasing spoofing threats in regions like the Baltic Sea [49].

The implementation costs must be considered against the potential impacts of successful attacks. With reports suggesting that a single successful attack could cause economic damage in billions [50], the value proposition for deployment is compelling, particularly for our combined approach that leverages existing receiver capabilities with minimal additional resources.

VII. CONCLUSION AND FUTURE WORK

Our analysis of GNSS timing spoofing data from Jammertest 2024 yielded several observations. We identified a progressive attack sequence where position/speed parameters were compromised at lower power levels (20-25 dBm) than timing (30 dBm), which may inform early warning system development. Our evaluation suggested that traditional C/N_0-based detection offers limited reliability while validity flags provide partial protection. The Isolation Forest algorithm showed promising performance (100% recall, 99.96% specificity) without requiring extensive labeled examples. By combining validity flag monitoring with machine learning verification, we created a robust framework leveraging complementary strengths of both methodologies.

These findings indicate that multi-layered strategies have potential to enhance GNSS timing security. However, the dataset was limited (only 1.88 minutes of spoofed reception out of 28 minutes of spoofer activity), and results should be interpreted with caution. Future work should expand the dataset, investigate reinforcement learning techniques for adapting to evolving threats, optimize implementation for resource-constrained systems through TinyML etc., and examine integration of detection with automated mitigation strategies like holdover oscillator switching to support comprehensive protective approaches for timing-dependent critical infrastructure.

REFERENCES

[1] GPS.gov, "Timing applications," 2022. [Online]. Available: https://www.gps.gov/applications/timing/

[2] E. Falletti, D. Margaria, G. Marucco, B. Motella, M. Nicola, and M. Pini, "Synchronization of critical infrastructures dependent upon GNSS: Current vulnerabilities and protection provided by new signals," IEEE Systems Journal, vol. 13, no. 3, pp. 2118-2129, 2018.

[3] Fingrid, "Prospects for future electricity production and consumption: Fingrid's forecast Q3/2024," 2024. [Online]. Available: https://www.fingrid.fi/globalassets/dokumentit/en/news/prospects-for-future-electricity-prodution-and-consumption.-fingrids-forecast-q3-2024.pdf

[4] J. Pearson, "GPS spoofers 'hack time' on commercial airlines, researchers say," Reuters, Aug. 11, 2024. [Online]. Available: https://www.reuters.com/technology/cybersecurity/gps-spoofers-hack-time-commercial-airlines-researchers-say-2024-08-10/

[5] Advanced Navigation, "Navigating the rising threat of GNSS spoofing in critical industries," Feb. 14, 2024. [Online]. Available: https://www.advancednavigation.com/tech-articles/navigating-the-rising-threat-of-gnss-spoofing-in-critical-industries/

[6] GPSPATRON, "The power grid's vulnerability to GPS spoofing attacks," Apr. 23, 2019. [Online]. Available: https://gpspatron.com/power-grid-spoofing/

[7] A. Kauranen, "Finland detects satellite navigation jamming and spoofing in Baltic Sea," Reuters, Oct. 31, 2024. [Online]. Available: https://www.reuters.com/world/europe/finland-detects-satellite-navigation-jamming-spoofing-baltic-sea-2024-10-31/

[8] M. L. Psiaki and T. E. Humphreys, "GNSS spoofing and detection," Proceedings of the IEEE, vol. 104, no. 6, pp. 1258-1270, 2016.

[9] 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.

[10] K. Radoš, M. Brkić, and D. Begušić, "Recent advances on jamming and spoofing detection in GNSS," Sensors, vol. 24, no. 13, p. 4210, 2024.

[11] X. Wei and B. Sikdar, "Impact of GPS time spoofing attacks on cyber physical systems," in 2019 IEEE International Conference on Industrial Technology (ICIT), 2019, pp. 1155-1160.

[12] Y. Gao and G. Li, "Three time spoofing algorithms for GNSS timing receivers and performance evaluation," GPS Solutions, vol. 26, no. 87, 2022.

[13] Y. Gao and G. Li, "Three time spoofing algorithms for GNSS timing receivers and performance evaluation," GPS Solutions, vol. 26, no. 87, 2022.

[14] X. Wei and B. Sikdar, "Impact of GPS time spoofing attacks on cyber physical systems," in 2019 IEEE International Conference on Industrial Technology (ICIT), 2019, pp. 1155-1160.

[15] H. Zhang, S. Peng, L. Liu, S. Su, and Y. Cao, "Review on GPS spoofing-based time synchronisation attack on power system," IET Generation, Transmission & Distribution, vol. 14, no. 20, pp. 4301-4309, 2020.

[16] K. Radoš, M. Brkić, and D. Begušić, "Recent advances on jamming and spoofing detection in GNSS," Sensors, vol. 24, no. 13, p. 4210, 2024.

[17] A. Rustamov, N. Gogoi, A. Minetto, and F. Dovis, "Assessment of the vulnerability to spoofing attacks of GNSS receivers integrated in consumer devices," in 2020 International Conference on Localization and GNSS (ICL-GNSS), 2020, pp. 1-6.

[18] S. Honkala et al., "Performance of EGNSS-based timing in various threat conditions," IEEE Transactions on Instrumentation and Measurement, vol. 69, no. 5, pp. 2287–2299, 2020.

[19] B. Qian, Z. Cai, Y. Xiao, L. Hong, and S. Su, "GPS spoofing-based time synchronisation attack in advanced metering infrastructure and its protection," The Journal of Engineering, vol. 2020, no. 9, pp. 809-815, 2020.

[20] D. Lee, D. Miralles, D. Akos, A. Konovaltsev, L. Kurz, S. Lo, and F. Nedelkov, "Detection of GNSS spoofing using NMEA messages," in 2020 European Navigation Conference (ENC), 2020, pp. 1-10.

[21] J. Spravil, C. Hemminghaus, M. von Rechenberg, E. Padilla, and J. Bauer, "Detecting maritime GPS spoofing attacks based on NMEA sentence integrity monitoring," Journal of Marine Science and Engineering, vol. 11, no. 5, p. 928, 2023.

[22] L. Xiao, X. Li, and G. Wang, "GNSS spoofing detection using pseudo-range double differences between two receivers," in 2019 IEEE 7th International Conference on Computer Science and Network Technology (ICCSNT), 2019, pp. 498-502.

[23] W. Gao, H. Li, M. Zhong, and M. Lu, "The separate clock drift matched filter to detect time synchronization attacks toward global navigation satellite systems," IEEE Transactions on Industrial Electronics, vol. 70, no. 6, pp. 6305-6315, 2022.

[24] T. T. Khoei et al., "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.

[25] X. Wei, M. N. Aman, and B. Sikdar, "Exploiting correlation among GPS signals to detect GPS spoofing in power grids," IEEE Transactions on Industry Applications, vol. 58, no. 1, pp. 697-708, 2022.

[26] A. Iqbal, M. N. Aman, and B. Sikdar, "Machine learning based time synchronization attack detection for synchrophasors," in GLOBECOM 2023 - 2023 IEEE Global Communications Conference, 2023, pp. 2251-2256.

[27] A.-G. Romaniuc, V.-C. Vasile, M.-E. Borda, and B. Alexandru, "NTP spoofing attack detection on time servers with GNSS sensors based on Long Short-Term Memory algorithm," in 2024 15th International Conference on Communications (COMM), 2024, pp. 1-6.

[28] J. Li et al., "A real-time GNSS time spoofing detection framework based on feature processing," GPS Solutions, vol. 29, no. 45, 2025.

[29] S. Dasgupta, T. Ghosh, and M. Rahman, "A reinforcement learning approach for global navigation satellite system spoofing attack detection in autonomous vehicles," Transportation Research Record, vol. 2676, no. 12, pp. 318-330, 2022.

[30] 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.

[31] J. Lee, E. Schmidt, N. Gatsis, and D. Akopian, "Detection and mitigation of spoofing attacks against time synchronization and positioning," IEEE Access, vol. 11, pp. 138986-139003, 2023.

[32] A. Iqbal, M. N. Aman, and B. Sikdar, "Representation learning based time synchronization attack detection for synchrophasors," in 2023 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), 2023, pp. 1-6.

[33] Jammertest, "About Jammertest," 2025. [Online]. Available: https://jammertest.no/about/

[34] u-blox, "ZED-F9P-02B data sheet," 2024. [Online]. Available: https://www.mouser.fi/datasheet/2/1025/ZED_F9P_02B_DataSheet_UBX_21023276-3180703.pdf

[35] Jammertest, "Test logs from Jammertest 2024," 2024. [Online]. Available: https://jammertest.no/content/files/2025/02/Logg_Jammertest_2024_v1.xlsx

[36] Jammertest, "Jammertest 2024 Test Catalog," 2024. [Online]. Available: https://jammertest.no/content/files/2025/02/Testcatalog.pdf

[37] semuadmin, "pyubx2 - PyPI," PyPI, 2025. [Online]. Available: https://pypi.org/project/pyubx2/

[38] NovAtel, "GPRMC – GPS specific information," NovAtel. [Online]. Available: https://docs.novatel.com/OEM7/Content/Logs/GPRMC.htm

[39] E. D. Kaplan and C. J. Hegarty, Understanding GPS: Principles and applications, 2nd ed. Artech House, 2006, pp. 327-328.

[40] X. Shang, F. Sun, L. Zhang, Q. Zhang, X. Tang, and C. Gao, "Detection and mitigation of GNSS spoofing via the pseudorange difference between epochs in a multicorrelator receiver," GPS Solutions, vol. 26, no. 2, p. 37, 2022.

[41] A. Angrisano, S. Gaglione, C. Gioia, D. Borio, and J. Fortuny-Guasch, "Testing the test satellites: The Galileo IOV measurement accuracy," in 2013 International Conference on Localization and GNSS (ICL-GNSS), 2013, pp. 1-6.

[42] A. B. Mohammed, L. C. Fourati, and A. M. Fakhrudeen, "Isolation Forest algorithm against UAV's GPS spoofing attack," in 2024 IEEE International Conferences on Internet of Things (iThings) and IEEE Green Computing & Communications (GreenCom) and IEEE Cyber, Physical & Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics, 2024, pp. 459-463.

[43] F. T. Liu, K. M. Ting, and Z.-H. Zhou, "Isolation forest," in 2008 Eighth IEEE International Conference on Data Mining, 2008, pp. 413–422.

[44] V. Aggarwal, V. Gupta, P. Singh, K. Sharma, and N. Sharma, "Detection of spatial outlier by using improved Z-score test," in 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), 2019, pp. 788-790.

[45] Google Developer, "Classification: Accuracy, recall, precision, and related metrics," Google for Developers, Mar. 3, 2025. [Online]. Available: https://developers.google.com/machine-learning/crash-course/classification/accuracy-precision-recall

[46] Inside GNSS, "Timing sources for wireless carriers, critical infrastructure bolstered against GNSS jamming and spoofing," Jun. 24, 2021. [Online]. Available: https://insidegnss.com/timing-sources-for-wireless-carriers-critical-infrastructure-bolstered-against-gnss-jamming-and-spoofing/

[47] W. Syam, "GNSS spoofing: a fatal attack on GNSS system that is difficult to detect," WASY Research, Jul. 18, 2022. [Online]. Available: https://www.wasyresearch.com/gnss-spoofing-a-fatal-attack-on-gnss-system-that-is-difficult-to-detect/

[48] Quartz, "The GPS/GNSS system behind finance, telecommunications and transportation networks is vulnerable to terrorist jamming and criminal spoofing," 2017. [Online]. Available: https://qz.com/1106064/the-entire-global-financial-system-depends-on-gps-and-its-shockingly-vulnerable-to-attack

[49] A. Kauranen, "Finland detects satellite navigation jamming and spoofing in Baltic Sea," Reuters, Oct. 31, 2024. [Online]. Available: https://www.reuters.com/world/europe/finland-detects-satellite-navigation-jamming-spoofing-baltic-sea-2024-10-31/

[50] GPS World, "Going up against time: The power grid's vulnerability to GPS spoofing attacks," Aug. 1, 2012. [Online]. Available: https://www.gpsworld.com/wirelessinfrastructuregoing-against-time-13278/