engineering proceedings

MDPI

Proceeding Paper

Enhanced GNSS Threat Detection: On-Edge Statistical Approach with Crowdsourced Measurements and Fuzzy Logic Decision-Making †

Eustachio Roberto Matera *, Olivier Lagrange and Maxime Olivier

Thales Services Numériques, 78140 Vélizy-Villacoublay, France; olivier.lagrange@thalesgroup.com (O.L.)
* Correspondence: eustachio-roberto.matera@thalesgroup.com
† Presented at the European Navigation Conference 2025 (ENC 2025), Wrocław, Poland, 21–23 May 2025.

Abstract

Global Navigation Satellite Systems are vulnerable to jamming and spoofing threats, compromising several critical applications. Existing detection methods based on hardware solutions (antenna array, spectrogram) are low-latency and accurate but require expensive hardware, while machine learning solutions are the most effective but require extensive training and lack adaptability. This work proposes an edge-based, statistical threat detector using crowdsourced GNSS data and fuzzy logic to integrate multiple anomaly indicators. A key feature is a C-/N_0-based crowdsourcing metric. Experiments show detection precision up to 88% for jamming and 97% for spoofing, with false positive rates around 1–2% and an average detection time of 10 s.

Keywords: GNSS; jamming; spoofing; crowdsourcing; fuzzy logic

1. Introduction

Global Navigation Satellite Systems (GNSSs) are vital for precise positioning and timing across various applications, like transportation (aviation, maritime, land, unmanned aerial vehicles) and critical infrastructures (financial services, telecommunications). However, GNSS has major inherent vulnerabilities which are exposed to malicious attacks, resulting in inaccurate positioning, navigation errors, or service disruptions, jeopardizing safety, efficiency, and security [1]. GNSS signals are weak and Open Service, therefore susceptible to interferences and easily accessible to malicious actors' manipulations. These vulnerabilities are deeply investigated in the literature [2,3]. Main threats are represented by jamming and spoofing attacks. Today, these attacks are becoming more frequent and affordable to execute. Detecting and mitigating these threats is essential to safeguard GNSS applications.

Authors in [3] analyzed different detection methodologies, such as machine learning (ML) methods, antenna array-based and signal processing methods, ranking them by their detection capabilities and complexity. ML techniques result in being the most effective for detection capabilities, although they require extensive data training and struggle with adaptability and responsiveness to new threats [2], as well as poorly interpretable internal setup parameters. Antenna array-based methods have highest performances in real-time applications but need tailored and expensive hardware and complex signal processing. Signal strength-based techniques are simpler and easier to be integrated in the receiver platforms since they do not need any dedicated hardware, being a valid alternative to

Check for updates

Academic Editor: Tomasz Hadaś

Published: 24 February 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

the more complex methods presented above but suffer low detection capabilities and limited classification between threats and unintentional variations. A common and heavily exploited approach compares the measured Carrier-to-Noise-density ratio (C/N_0) and the Automatic Gain Control (AGC) to expected values to detect possible threats [3]. In [4] the detection capacity of the approach mentioned above is improved by exploiting the C/N_0 correlation properties of synchronized measurements to detect common measurement variations. This type of approach could balance the need for real-time detection with low implementation costs and no dedicated hardware, although the detection power and the probability of false alarms need to be investigated further.

This work presents a methodology for jamming and spoofing detection aimed at local detectors, focusing on low-latency alerts and minimal computational requirements. It is designed to be integrated into any receiver platform using standard output data from commercially available receivers. As a result, the solution is independent of the hardware of the source GNSS receivers, enabling seamless use with any data source. The threat detector processes GNSS receivers' output data to generate anomaly indicators that identify unexpected variations in the selected features compared to nominal dynamics. The core solution uses a crowdsourcing-based C/N_0 metric [5], leveraging C/N_0 data correlation to generate the anomaly indicator. To improve detection reliability, multiple independent anomaly indicators are generated from different signal features, addressing direct receiver and satellite navigation parameter attacks. These anomaly indicators are subsequently integrated using a fuzzy logic approach for more refined detection of jamming and spoofing events, improving upon traditional decision threshold methods. This approach allows for clear and explainable parametrization of the decision logic based on statistical methods, rather than relying on the poorly interpretable parameters of machine learning models.

2. Context

Jamming attacks interfere with authentic satellite signals, preventing receivers from collecting and tracking them by transmitting high-power signals at the desired frequency [6]. On the contrary, spoofing attacks involve transmitting fake signals that mimic authentic ones at higher power, deceiving receivers into tracking these false signals and falsifying their location [7]. Detecting these attacks is essential to prevent harmful outcomes. Understanding the characteristics of different attacks is crucial for developing effective defenses. Scientific works, such as [3,7], provide comprehensive analyses of various jamming/spoofing attack spectrums and examine detection methods applied at different GNSS stages: Radio Frequency (RF) processing, Signal Processing, and Data Processing. In Table 1 we summarized the principles, advantages, and disadvantages of the most common techniques. RF processing methods provide accurate and low-latency detection, ideal for real-time applications, but require expensive hardware and the integration in the receiver's signal processing chain, posing scalability challenges. Signal processing-based detection characteristics vary by method. Correlation peak monitoring and code-carrier monitoring have good detection capabilities, but they are computationally demanding, and require integration in the receiver signal processing chain. In the other hand, signal power monitoring, analyzing the dynamic of C/N_0 metric, is a low-latency approach, which can be used either in an integrated way in the receiver processing chain, or externally by accessing directly to the data in the receiver output. However, it is less precise than other techniques, very sensitive to variations, and has many difficulties in discriminating against jamming and spoofing attacks from other types of variations. Data processing detection methods offer top performance, usually independent of the receiver, but necessitate extensive data analysis with high computational costs and latency. ML solutions in the data processing stage are the leading approach for detecting GNSS jamming and spoofing attacks, offering

https://doi.org/10.3390/engproc2026126018

superior detection and classification of jamming and spoofing. However, ML face significant challenges, including extensive data training requirements, adaptability issues, and limited responsiveness to threats.

Table 1. Summary of GNSS jamming and spoofing detection methodologies.

Area of Interest	Method	Advantage	Disadvantage
RF Processing	Antenna Array	Low latency, high responsiveness	Requires expensive hardware
	RF Spectrogram	Accurate spoofing detection	Time consuming, resource-intensive
	AGC	Low latency, low-complex	Hard to discriminate threats from other environmental factors
Signal Processing	Signal Power	Low latency, low-complex	
	Correlation Peak	Less sensible to signal variations	Computationally expensive
	Code and Carrier Phase	High accuracy	
Data Processing	Direction of Arrival	Accurate spoofing detection	Complex and expensive implementation
	Time of Arrival	Accurate spoofing detection	Requires precise time synchronization
	Multi-Receiver Differential approach	High accuracy	Time consuming, resource-intensive approach, high cost and complexity
	Machine Learning	High accuracy global detection	Computationally expensive. Requires extensive data training.

The objective of this work is to develop a low-complexity detection method tailored to the current ecosystem of GNSS receivers and operational use cases. The proposed solution is designed for seamless integration into existing heterogeneous static receiver platforms, without requiring additional hardware or external network support. It aims to accurately distinguish abnormal signal behavior from nominal environmental variations, ensuring adaptability to diverse deployment conditions.

In this study, we focus on an edge-based, statistical threat detection approach that operates locally using crowdsourced GNSS data. The detector is embedded within a single receiver and exploits signal power monitoring, relying on the correlation properties of the C/N_0 metric as the primary indicator for jamming and spoofing detection. To mitigate the limitations of signal power monitoring in differentiating intentional interference from natural signal fluctuations, an anomaly detection algorithm based on the data-processing monitoring family is incorporated. Subsequently, indicator fusion combines the outputs of both detection modules, enabling the generation of a unified and reliable anomaly alert.

It is important to note that crowdsourcing can be interpreted in both local and networked contexts. The approach presented here focuses on the multi-satellite (local) perspective, leveraging simultaneous observations from different satellites within a single receiver to detect local interference. This is complementary to the multi-receiver (networked) approach, where information from multiple receivers is jointly analyzed to characterize satellite-specific attacks. Our broader research addresses the two approaches, which are designed to remain independent yet ultimately integrable within a unified jamming and spoofing detection framework. However, the local, edge-based solution offers fast data processing, requires no external synchronization, and can be implemented on existing platforms, key advantages that motivated our decision to focus this paper on this component.

3. Methodology

The On-Edge Threat detection high-level scheme is depicted in Figure 1.



Figure 1. On-Edge Threat detection block diagram.

The first module acquires the local GNSS receiver output data (PVT and ephemeris, pseudorange, carrier phase, Doppler frequency, C/N_0), coming from a single receiver platform, and additional information, such as the receiver's reference position and GNSS orbital elements (Two-Line element files, TLE), if the applicable solution can periodically receive external data from a server, as long as real-time operation and detection are maintained locally. In the second module, the raw GNSS data are processed in order to generate uniform and normalized independent features (i.e., removing unwanted trends in the data, such as those in the C/N_0 time series caused by satellite and receiver mutual dynamics). These features are subsequently used in the third module for the elaboration of the corresponding anomaly indicators, which distinguish between normal dynamics of the measurement's time series and anomalies caused by unwanted events. The selected indicators include receiver-focused metrics like position variation and clock bias variation, as well as satellite navigation parameters like ephemeris and satellite clock bias.

The ensemble of the anomaly indicators is acquired by decision logic to generate jamming and spoofing alarm indicators. A common decision logic usually applied for this purpose is based on binary hypothesis estimated through Neymann–Pearson statistical tests [8]. However, the interactions between the binary decision threshold are limited to some determined and discontinuous cases, strongly limiting the ability to represent these types of phenomena.

To avoid decision discontinuities, we implemented fuzzy logic, which enables flexible classification through partial membership in multiple categories, ideal for detecting jamming and spoofing. The Fuzzy Logic Threat Detection system consists of three stages. First, we select the most effective anomaly indicators by removing redundancies. Second, we define fuzzy membership functions, assigning degrees of membership (0 to 1) to linguistic categories like "low" and "high" based on the input probability density function (PDF). For example, "low" has full membership with no interference and none with interference; "high" is the inverse. Thresholds are determined using nominal and interference data, with the 95th percentile guiding the bending points. In the final stage, we establish fuzzy decision rules, such as "If CN0 is High and Position Error is High, then Spoofing is detected to classify the jamming and spoofing alerts." The output consists of two smooth probabilistic threat scores: one for jamming and one for spoofing.

C/N_0 fluctuations are crucial for detecting threat interferences and fundamental to apply the Signal Power Monitoring solution. This versatile metric can detect local threats by correlating C/N_0 time series from different satellites for a single receiver and regional threats by correlating C/N_0 time series from multiple receivers for a single satellite. Thus, the C/N_0 anomaly indicator is essential to our detection strategy. The proposed C/N_0 anomaly indicator is obtained applying the operations described in Figure 2.

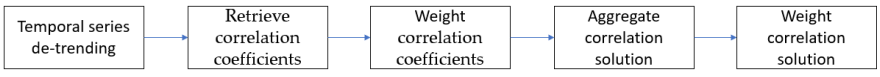


Figure 2. Diagram of crowdsourcing-based indicators using the C/N_0 metric.

The first step involves detrending C/N_0 temporal series using polynomial regression to decorrelate measurements from elevation [4]. The second step is based on the cross-

correlation methodology of the C/N_0 temporal series provided in [8]. At a given epoch n, we approximate the Pearson correlation coefficients of two C/N_0 temporal series X_a and X_b, $\rho(X_a, X_b) = \frac{Cov(X_a, X_b)}{(\sigma_a \sigma_b)}$, between any pair of C/N_0 time series over a specific sliding window, T_n. By performing an exhaustive computation, we define a squared Pearson matrix P of size N, which includes correlation information about any pair of tracked GNSS signals, with N equal to the number of tracked signals for which C/N_0 time series are available. Further, we propose an aggregated metric to quantify the severity of the attack by gathering all the pairwise information equal to the median of the strict upper triangular part of the calculated Pearson matrix, A, $\mu_\rho^{(N)} = med(A)$. The methodology proposed in [8] does not take into account possible weighting schemes to enhance these correlation properties. In this work, then, we propose to apply two different weighting parameters. The first one is directly applied to the Pearson correlation coefficients, $\rho(X_a, X_b)$, and corresponds to a weighting parameter based on the probability value, p, derived from the following correlation index hypothesis test: probability that the correlation index is significantly different from 0, assuming that no correlation between the temporal series exists (H_0 hypothesis). Therefore, if the value of p is low, H_0 is almost certainly rejected since there is a relationship between the series. Hence, it is here proposed to weigh the Pearson correlation coefficient by

$$\widetilde{\rho}(X_a, X_b) = \rho(X_a, X_b)(1 - p) \tag{1}$$

We observed that our weighting coefficient is maximum during the correlation peaks (great chance that H_0 will be rejected) and lower the rest of the time. This weighting is able to separate the correlation peaks from the other minor variations, allowing a better detection of anomalies. We observed also that the size of the correlation matrix, N, is not taken into account in any weighting scheme, even if we observed that increasing the number of correlated series improves detection accuracy and reduces the risk of false detection. Thus, a second weight factor applied to the $\mu_\rho^{(N)}$ parameter is proposed as follows:

$$\mu_p^{(N)} = \mu_\rho^{(N)} \frac{N_{avail}}{\widetilde{N}} \tag{2}$$

where N_{avail} is the number of correlated series at epoch of the calculation of the feature, and $\widetilde{N}$ is the expected number of correlated series over the observation window, experimentally observed via a statistical analysis over a real dataset.

4. Experimental Results

This section aims to evaluate the effectiveness of the proposed methodology using a real dataset. In the first step, we evaluated various indicators using real GNSS datasets with jamming and spoofing to identify the most effective ones for low-latency threat detection. This analysis eliminated redundant indicators and optimized model performance. The evaluation used 1 Hz GPS L1 C/A data from a static receiver, with both nominal (interference-free) and mixed interference scenarios from the JammerTest 2023 event [9]. The anomaly indicators analysis is summarized in Table 2. The anomaly indicators are computed from a combination of navigation data, TLE orbital information, and receiver observables. Each indicator quantifies the deviation between measured parameters and their theoretical or reference counterparts, providing a diagnostic signature of potential anomalies in the GNSS signal or receiver behavior:

The satellite visibility indicator compares the number of satellites tracked by the receiver with the theoretical visibility derived from TLE propagation for the receiver's position and elevation mask. Deviations indicate possible signal obstruction or loss of lock.

The satellite orbit indicator evaluates the difference between satellite positions obtained from broadcast ephemerides and those predicted from TLE orbits, allowing the detection of inconsistencies or manipulation in the navigation message. The PVT Solution Anomaly is determined by comparing the estimated receiver position with a known reference. Significant position or clock deviations denote possible spoofing or local degradation. The Azimuth–Elevation Error is obtained by contrasting theoretical satellite angles computed from TLE data with those derived from broadcast ephemerides; systematic angular offsets may reveal orbit or ephemeris anomalies. The Doppler Frequency Error measures the difference between observed and theoretical Doppler shifts derived from satellite–receiver relative motion. Large residuals are typically associated with spoofing or oscillator instability. The Code–Phase Coherence indicator assesses the agreement between code and carrier-phase ranges; a loss of coherence could indicate interference. Signal quality is further examined through the C/N_0 Correlation indicator, obtained by cross-correlating C/N_0 time series from different satellites. High correlations reveal common-mode disturbances such as jamming or propagation effects. Finally, the Receiver Clock Bias indicator monitors the temporal evolution of the receiver clock offset and drift. Abrupt variations or abnormal trends suggest possible timing manipulation or internal instability.

Table 2. Summary of anomaly indicator analysis.

Features	Anomaly	Procedure	Advantages	Disadvantages	Redundancy	Priority
1-Nav, 2-TLE files	Satellite visibility	Difference between observed and theoretical number of satellites	Effective to retrieve satellite loss-of-lock and re-tracking	Low sensitivity	No	Medium
1-Nav, 2-TLE files	Satellite orbit	Difference between observed and theoretical orbit	Effective against nav. message manipulation	Poor sensitivity in case of changes in raw measures	With satellite visibility	Low
1-PVT, 2-Ref. Pos.	PVT Solution Anomaly	Difference between estimated and reference coordinates	Very Effective against spoofing attacks	Precise reference position required	No	High
1-Nav, 2-TLE, 3-Ref. Pos.	Azimut–Elevation Error	Difference between observed and theoretical values	Effective against nav. message manipulation	Accuracy dependent on theoretical estimation	With satellite visibility	Low
1-Doppler frequency, 2-TLE, 3-Ref. Pos.	Doppler Frequency Error	Difference between observed and theoretical Doppler frequency	Effective against spoofing attacks	Accuracy dependent on theoretical estimation	With Code-Phase Coherence	Low
1-Code, 2-Carrier Phase	Code–Phase Coherence	Difference between phase variation and code variation	Detects the beginning of interference activities	High sensitivity to noise	No	High
1-C/N_0	C/N_0 correlation	Cross-correlation of C/N_0 temporal series	Effective against jamming and spoofing	High sensitivity to noise	No	High
1-Receiver clock bias	Receiver clock drift variation	Analysis of anomalous receiver clock drift dynamic	Effective against receiver clock manipulations	High sensitivity to noise	No	Medium

https://doi.org/10.3390/engproc2026126018

Based on accuracy and adaptability, the following three high-priority indicators were selected: Crowdsourced C/N_0 Correlation, PVT Solution Error, and Code-Phase Coherence. Two medium-priority indicators, Receiver Clock Bias Anomaly and Satellite Availability Anomaly, were also chosen for their unique spoofing and signal disruption detection capabilities. Figure 3 illustrates the behaviors of the five high and medium priority anomaly indicators on a specific dataset, the JammerTest DS01.23 scenario. The scenario is characterized by five different temporal phases which are identified by colored squares inside the C/N_0 temporal series plot (Figure 3a): two nominal sections (green squares) interspersed with a section where the receiver was reset due to configuration changes (violet square), followed by a jamming attack section (yellow square), and a spoofing attack section (red square).

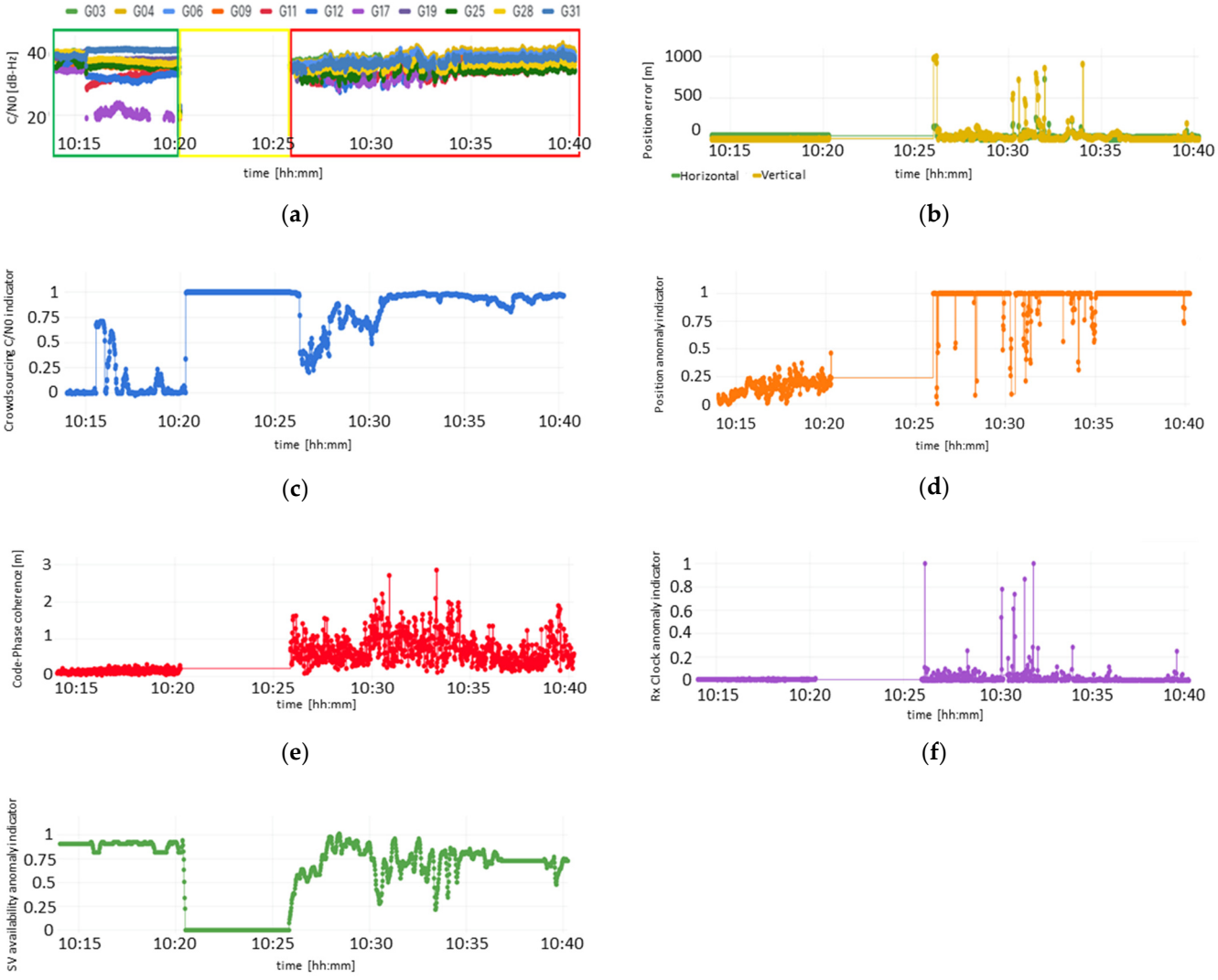
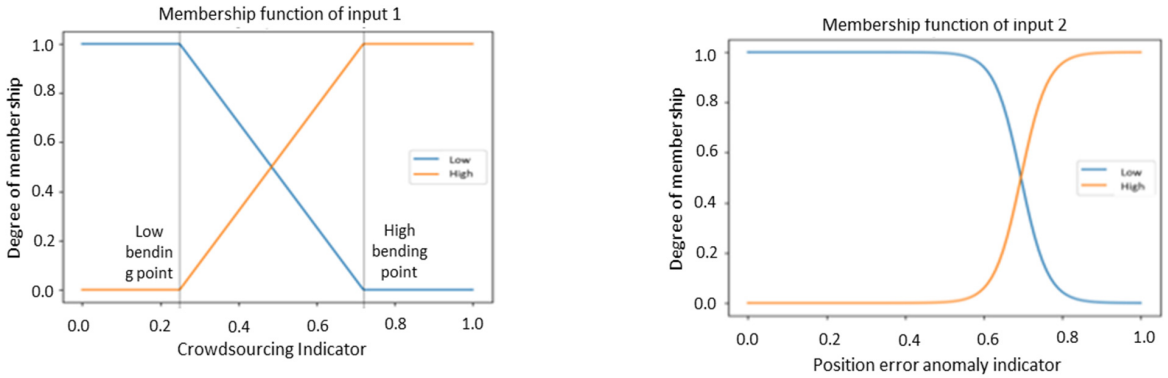


Figure 3. Anomaly indicators obtained from JammerTest DS01.23 scenario. (**a**) C/N_0 de-trended time series, (**b**) horizontal and vertical position error, (**c**) crowdsourcing C/N_0 anomaly indicator, (**d**) position anomaly indicator, (**e**) code–phase coherence indicator, (**f**) clock receiver anomaly indicator, (**g**) satellite availability anomaly indicator (in this case the figure should be read as 1: nominal, 0: anomaly).

After identifying the most effective anomaly indicators, we defined a baseline solution using the minimal essential set of indicators. Crowdsourced C/N_0 anomaly indicator was found to be the most practical and reliable metric for interference detection. Although

Code–Carrier Phase Coherence provides valuable insights, its reliance on pseudorange and carrier phase measurement processing limits its real-time applicability. PVT anomaly indicator, despite requiring full solution computation, proved effective for distinguishing real threats from normal variations. Thus, we decided the baseline fuzzy logic model to integrate only Crowdsourced C/N_0 and PVT anomaly indicators. Since the modular design of the proposed solution could easily support the integration of more indicators, an advanced configuration using all five priority indicators will be used for performance comparison. However, a full analysis of the five-indicator model is left for future work due to space constraint in this article. Fuzzy membership functions were successively defined, with Figure 4 showing the "Low" and "High" subsets for anomaly detection based on Crowdsourcing C/N_0 anomaly indicator and PVT anomaly indicator.



(**a**) (**b**)

Figure 4. Membership functions of baseline fuzzy logic solution. (**a**) Degree of membership of Crowdsourcing indicator; (**b**) degree of membership of position error indicator.

Consequently, the rules of fuzzy logic have been defined. For the system with only two input parameters, a basic decision matrix can be defined as follows (Table 3):

Table 3. Fuzzy logic decision rules.

Anomaly Indicators	**C/N_0**		
	Fuzzy Subsets	**Low**	**High**
Position Error	Low	Nothing	Jamming
	High	Nothing	Spoofing

Finally, we tested the proposed methodology on the real dataset to verify the current performance of the baseline detector. The jamming and spoofing alert indicators obtained from the JammerTest DS01.23 scenario are depicted in Figure 5. The detector is able to clearly identify and classify the jamming and spoofing events. Also, the non-binary and continuous nature of the alert indicators better characterize the real dynamic of the anomaly events. Finally, we could see how the receiver reset anomaly (10:16 in the figure) is identified as a jamming alert, meaning that, with this baseline configuration, the solution is not able to discriminate other types of anomalies from jamming/spoofing threats. This issue could be reduced by the use of a larger number of indicators and a more complex decision logic, which will be able to identify different types of anomalies.

To assess the overall detection performances of the proposed solution, an experimental test has been initiated, using a real dataset obtained from the JammerTest 2023 Event [9]. The GNSS receiver utilized for this test was a Septentrio MOSAIC-H_SN4832, configured to receive signals from the GPS L1 C/A constellation with a data rate of 1 s. The details can be

found in Table 4. Independently, the behavior of the detector in presence of nominal data has been tested using a nominal real dataset obtained from French National Space Agency.

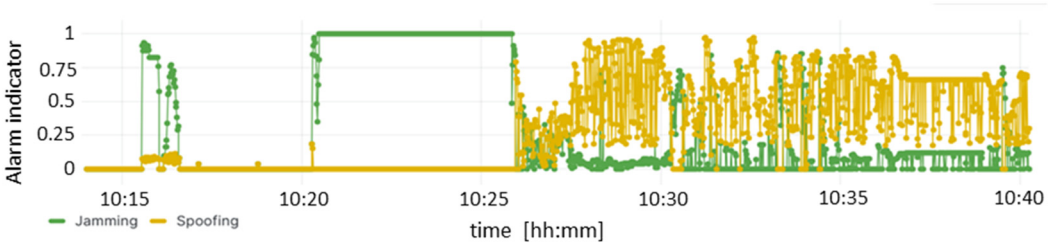


Figure 5. Output jamming (green) and spoofing (yellow) alarm indicators of baseline solution applied to JammerTest DS01.23 scenario.

Table 4. Summary of datasets used for experimental tests.

Scenario Name	Event	Description
DS01.5	Jamming L1 modulation	Jamming power ramp
DS01.12	Stationary meaconing	Initial jamming followed by continuous spoofing
DS01.14	Incoherent spoofing using synthetic ephemerides	Gradually increasing spoofing signal strength
DS01.22	Coherent spoofing using true ephemerides	Initial Jamming and continuous spoofing
DS01.23	Coherent spoofing using true ephemerides	Continuous Jamming plus continuous spoofing

The alarm indicators were evaluated against labeled data using a confusion matrix and standard metrics, such as Power of Detection, False Alarm Probability and Precision. Detection time was also measured as the delay between the labeled anomaly and its detection. Moreover, the performances of baseline solution have been compared with the advanced solution, tested with the same dataset. The detector's performances in case of nominal situations are satisfactory with a very low false positive rate, tending to zero. Also, Table 5 summarizes results for both the baseline (two indicators) and advanced (five indicators) solutions across the datasets presented in Table 4. The baseline achieved high precision rates (~0.75 for jamming, ~0.95 for spoofing) with low false alarm rates (~0.1 for jamming, ~0.02 for spoofing) and an average detection time of roughly 10 s, highlighting the baseline's robustness, especially the effectiveness of the crowdsourced C/N_0 indicator. On the other hand, the advanced solution showed improved precision and faster detection, combined with the ability to detect all types of events within the analyzed scenarios. However, the limited dataset may underrepresent more diverse attack scenarios, potentially favoring the advanced model's broader scope.

Table 5. Summary of the experimental results.

Solution	Det. Time [s]				Probability False Alarm				Precision			
	Jamming		Spoofing		Jamming		Spoofing		Jamming		Spoofing	
	Mean	Std	Mean	Std	Mean	Std	Mean	Std	Mean	Std	Mean	Std
Baseline	10	4.58	25	8.32	0.10	0.06	0.02	0.04	0.75	0.18	0.95	0.06
Advanced	10.8	10.9	23	5.19	0.03	0.02	0.03	0.02	0.88	0.06	0.97	0.04

5. Conclusions

This study introduces a low-complexity on-edge detector for analyzing local GNSS metrics such as C/N_0 trends and PVT consistency to identify jamming or spoofing anoma-

lies in near real-time. It integrates easily into various receiver platforms without requiring expensive hardware, making it suitable for current GNSS ecosystems. The detector processes GNSS metrics to generate anomaly indicators, which are then synthesized using fuzzy logic for jamming/spoofing alarms. The key solution, the Crowdsourcing C/N_0 anomaly indicator, refines detection through weighted Pearson correlation matrices, prioritizing significant signal correlations and adjusting confidence levels based on data availability. Other anomaly indicators based on data measurement analysis are used as feedback solution to cope with C/N_0 anomaly indicator limitations. The different indicators are integrated together through a Fuzzy Decision Logic approach to finally detect and classify the jamming and spoofing alerts. This approach reduces false alarms and adapts to complex attack scenarios, improving threat assessment amidst real-world GNSS uncertainties.

Author Contributions: Conceptualization, E.R.M., O.L. and M.O.; methodology, E.R.M., O.L. and M.O.; software, E.R.M., O.L. and M.O.; validation, E.R.M., O.L. and M.O.; formal analysis, E.R.M., O.L. and M.O.; investigation, E.R.M., O.L. and M.O.; resources, E.R.M., O.L. and M.O.; data curation, E.R.M., O.L. and M.O.; writing—original draft preparation, E.R.M. and O.L.; writing—review and editing, E.R.M. and O.L.; visualization, E.R.M. and O.L.; supervision, E.R.M. and O.L.; project administration, O.L.; funding acquisition, O.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study were collected during the Jammer Test 2023 campaign (information available at https://jammertest.no). The datasets consist of RINEX observation files and receiver-native format data corresponding to specific test scenarios provided by CNES (French Space Centre), which directly participated in the campaign. The data are not publicly available due to ownership and usage restrictions. Data are available from the authors upon reasonable request and subject to authorization by the data owner.

Conflicts of Interest: Authors E.R.M. and O.L. are employees of the company Thales Services Numériques, Author M.O. was employed by the company Thales Services Numériques. All authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

GNSS	Global Navigation Satellite System
C/N_0	Carrier-to-Noise-density ratio
ML	Machine Learning
TLE	Two-Line element files
PDF	Probability Density Function

References

1. Ieropoulos, V. The Impact of GPS Interference in the Middle East. In Proceedings of the 2024 IEEE International Conference on Cyber Security and Resilience, CSR 2024, London, UK, 2–4 September 2024; Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, USA, 2024; pp. 732–736. [CrossRef]
2. Ghanbarzade, A.; Soleimani, H. GNSS/GPS Spoofing and Jamming Identification Using Machine Learning and Deep Learning. *arXiv* **2025**. Available online: http://arxiv.org/abs/2501.02352 (accessed on 1 March 2025). [CrossRef]
3. Radoš, K.; Brkić, M.; Begušić, D. Recent Advances on Jamming and Spoofing Detection in GNSS. *Sensors* **2024**, *24*, 4210. [CrossRef]

4. Minetto, A.; Rustamov, A.; Dovis, F. Detecting single-antenna spoofing attacks by correlation in time series of raw measurements. In Proceedings of the 36th International Technical Meeting of the Satellite Division of the Institute of Navigation, ION GNSS+ 2023, Denver, CO, USA, 11–15 September 2023; Institute of Navigation: Manassas, VA, USA, 2023; pp. 73–84. [CrossRef]
5. Olsson, G.K.; Nilsson, S.; Axell, E.; Larsson, E.G.; Papadimitratos, P. Using Mobile Phones for Participatory Detection and Localization of a GNSS Jammer. *arXiv* **2023**. Available online: http://arxiv.org/abs/2305.02038 (accessed on 1 January 2025). [CrossRef]
6. Kuusniemi, H.; Zahidul, M.; Bhuiyan, H.; Airos, E.; Kröger, T. Effects of GNSS Jammers on Consumer Grade Satellite Navigation Receivers. 2012. Available online: https://www.researchgate.net/publication/230555697 (accessed on 1 January 2025).
7. Psiaki, M.L.; Humphreys, T.E. GNSS Spoofing and Detection. *Proc. IEEE* **2016**, *104*, 1258–1270. [CrossRef]
8. Rustamov, A.; Minetto, A.; Dovis, F. Improving GNSS Spoofing Awareness in Smartphones via Statistical Processing of Raw Measurements. *IEEE Open J. Commun. Soc.* **2023**, *4*, 873–891. [CrossRef]
9. Jammertest-2023. Available online: https://jammertest.no/content/files/2024/03/Jammertest-2023---Testplan.pdf (accessed on 5 May 2025).

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.