18th International Conference on Space Operations, Montreal, Canada, 26 - 30 May 2025.

SpaceOps-2025, ID # 434

Advanced Protection Strategies for GNSS Enhancing System Resilience to Spoofing and Jamming Threats

David Sánchez-Heredero Martínez[a], Francisco Gallardo López[a], Narayan Dhital[a]

[a] DLR GfR, Weßling Bavaria, Germany

Abstract

In recent years, Global Navigation Satellite Systems (GNSS) services have experienced significant growth, enabling users to integrate these services into increasingly sophisticated applications. However, the increased reliance on GNSS solutions has raised critical discussions about the system's robustness and reliability. These concerns are further amplified by political situations that have led to a GNSS environment where, military grade, jamming and spoofing attacks are becoming more common and impacting several markets. Addressing this vulnerability promptly is essential. To mitigate these threats, the Galileo GNSS has incorporated Navigation Message Authentication (NMA). Nevertheless, Secure Code Estimation and Replay (SCER) spoofing attacks can surpass these protection mechanisms, indicating the need for more advanced systems. This paper proposes a complementary detection method for end-user receivers, assuming the use of NMA, to defend against SCER attacks by processing satellite-recorded data.
Keywords: (maximum 6 keywords)
GNSS, Spoofing, Jamming, Machine Learning, Satellites, LEO

Acronyms/Abbreviations

ACRONYM	MEANING
GNSS	Global Navigation Satellite System
NMA	Navigation Message Authentication
SCER	Secure Code Estimation and Replay
OSNMA	Open Service Navigation Message Authentication
GPS	Global Positioning System
MEO	Medium Earth Orbit

1. Introduction

From humanity's earliest days, accurately determining one's location has been a fundamental challenge. By the 16th century, navigation required extensive skills and a broad range of instruments. According to Bowditch, Ferdinand Magellan's 1519 expedition relied on "sea charts, a terrestrial globe, wooden and metal theodolites, wooden and wood-and-bronze quadrants, compasses, magnetic needles, hour glasses and 'timepieces', and a log to be towed astern" [1]. All this equipment took Magellan in his trip in 1519 to estimate the latitude, the speed and the position of the ship. However, the longitude couldn't be measured. It wasn't until 250 years later that there was any update on this issue [2]. An improvement of clocks where still neded and the costs of it made the solution implementation to lead to a not accurate solution.

Within the context of World War II, radionavigation solutions started to be evaluated and implemented. Great Britain deployed *Gee* to guide aircraft and the US developed *Loran* (Long-range radio aid to navigation). However, global solutions where still needed. This set the bases for the began of a new set of solutions of navigation.

Around 1957 the Soviet Union launched *Sputnik I,* the world's first artificial satellite. This episode marked the beginning of the space age and the "space race" starring between the US and the USSR. It took 8 years to see the first operational satellite navigation system in 1964, *Transit* [3]. After the big success of this system, more ambitious solutions where aimed. A set of Medium Earth Orbit (MEO) satellites began to be launched populating what we call today GNSS constellations. Declared operational in 1995, the Global Positioning System (GPS) was the first one to be

deployed. Other systems were subsequently deployed: the Russian GLONASS (1976), the Chinese BeiDou (2000), and the European Galileo (declaration of Initial Services) (2016) [2].

The implications of GNSS solutions are not narrowed to navigation solutions, but clock solutions are as well a significant improvement that allows the user to obtain a precise timing from a low-cost device. The remarkable success of GNSS has allowed significant improvements in security and operational capabilities across many sectors. In maritime operations, GNSS underpins safe navigation and port management. Similarly, in aviation, highly accurate GNSS signals are crucial for flight safety and air traffic management. Furthermore, unmanned applications such as drones, autonomous ground vehicles, and autonomous ships are prime examples of this technology's widespread adoption and reliance [4].

Emerging Threats to GNSS Integrity

Because critical infrastructures and some safety-of-life services depend on GNSS to some extent, disruptions from Radio Frequency Interference (RFI) can pose significant threats. Jamming and spoofing attacks in particular have gained attention due to recent high-profile incidents. One such incident occurred in December 2019 at the Port of Shanghai, where Automatic Identification System (AIS) data from nearby vessels formed an anomalous circular pattern over land [5]. Similarly, in December 2022, the Dallas/Fort Worth International Airport experienced a major service interruption due to spoofed signals, forcing aircraft to rely on outdated flight routes [6]. These examples reflect the importance of the vulnerability in the maritime and aviation sectors to malicious interference, highlighting the need for rapid and reliable detection solutions.

An ESA-funded project led by DLR GfR mbH resulted in the development of **RESIST** (RF analytical Evaluation of Signal In Space Threats), a system that leverages data from both Low Earth Orbit (LEO) satellites and ground station antennas. At the core of RESIST is the **CMCU** (Combined ML-based Cross-layering Unit) algorithm, jointly created by DLR GfR mbH and the Technical University of Madrid (UPM) [7] [8]. Building on this foundation, a new, lighter, and more cost-effective solution has now been introduced and is presented within this paper. Its main algorithm, significantly streamlines the detection of jamming and spoofing events, enabling faster response times and more robust interference mitigation.

GNSS has become indispensable to modern society, from defence applications to commercial sectors, particularly maritime and aviation. Recent interference incidents demonstrate the urgent need for robust, fast-response mitigation strategies. The system addresses this challenge by combining innovative ML algorithms with the advantages of LEO constellations, providing enhanced security and availability for critical GNSS services.

2. Material and methods

A variety of solutions exist to detect jamming and spoofing events in Global Navigation Satellite Systems (GNSS). However, many of these solutions remain at the theoretical or prototype stage, largely due to implementation complexity or unfavourable cost-effectiveness. Currently, one of the most accessible options for any stakeholder concerned with Radio Frequency Interference (RFI) in GNSS is the **Automatic Dependent Surveillance–Broadcast (ADS-B)**. Through ADS-B, aircraft broadcast real-time position, velocity, and timing (PNT) information that can be monitored to infer the presence of interference. While ADS-B data are invaluable for analysing the effects of jamming or spoofing on operational assets, reliance on these broadcasts alone does not necessarily provide a proactive mechanism to prevent or mitigate interference incidents. Similarly, Automatic Identification System (AIS), reports ship's positions, information broadcast by vessels and ships is a source of information for the detection of radio frequency interferences.

To address these challenges, we propose a LEO-based solution. This method focuses on early detection and geo-localization of interference sources. The system processes from both spaceborne (LEO satellites) and terrestrial stations. The data inputs from the satellite are then fed into the main algorithm. It then, performs advanced signal and data analysis to identify anomalies indicative of jamming or spoofing activities. By leveraging a mixture of measurements and other parameters. By doing so, we can rapidly characterize interference events in a given region.

A key advantage of this method is its ability to deliver **early** detection and geo-localization of jamming or spoofing attacks. This high speed stems from combining data from multiple vantage points, LEO satellites in orbit and ground-

based stations, thereby reducing reliance on a single dataset or technology. Moreover, the solution is designed to be more cost-effective and straightforward to implement than many existing GNSS RFI detection systems, aiming to facilitate broader adoption across both government and commercial sectors.

In developing and validating of the system, we have utilized satellite data provided by **existing LEO missions**. This dataset includes high-resolution observations encompassing various orbital geometries, temporal spans, and signal conditions, which allowed us to test the robustness and adaptability of the core algorithm under different interference scenarios. Ground stations co-located with DLR's facilities provided supplemental measurement data on local atmospheric conditions, signal noise levels, and potential terrestrial interference sources.

A series of **controlled jamming and spoofing tests** was also conducted to evaluate system performance. In these tests, known RFI sources were introduced in a controlled environment to measure how promptly and accurately the system could detect and localize the interference.

2.1 Methodological Workflow

1. **Data Acquisition**
   - Collect raw data via LEO satellites and ground station antennas.
   - Store the data in indexed archives for standardized processing.
2. **Preprocessing and Filtering**
   - Perform time synchronization across data sources.
   - Filter out known noise artifacts and remove incomplete or corrupted data sets.
3. **Algorithmic Analysis (Core algorithm)**
   - Extract signal metrics from the archive.
   - Perform calibration to noise the sources.
   - Apply machine learning and statistical methods to detect anomalies that may signal jamming or spoofing events.
4. **Localization and Notification**
   - Combine multi-source data to triangulate the location of the identified RFI source.
   - Trigger alerts or notifications to system operators and relevant stakeholders for rapid intervention.
5. **Performance Assessment**
   - Evaluate detection accuracy, latency, and overall system reliability using ground-truth reference data and controlled interference scenarios.

Compare the obtained results with existing solutions such as ADS-B to measure improvement in terms of precision, speed, and cost-effectiveness.

3. Results

A major outcome of this project is the successful integration of the core algorithm of the system into a comprehensive service monitoring platform. This platform synthesizes data from Low Earth Orbit (LEO) satellites, ground station antennas, and other GNSS data sources , then runs the algorithm in near real-time to identify potential jamming or spoofing incidents. The monitoring platform offers a user-friendly interface for visualization and alert management, shown in Figure 1.

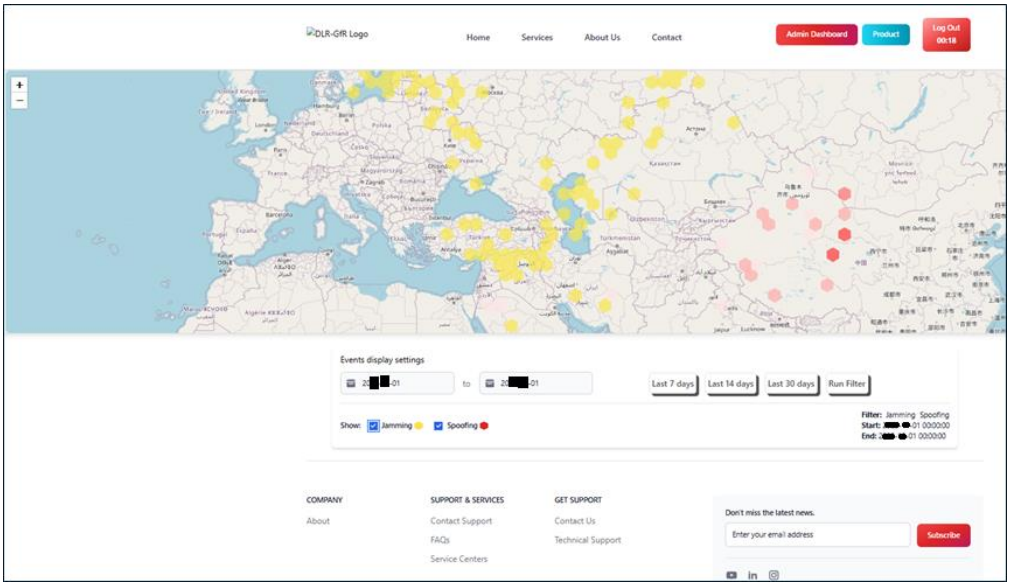

Figure 1 – System´s map interface ilustration

Preliminary evaluations suggest that the algorithm reliably identifies anomalous GNSS signal patterns and triggers alerts in a timeframe sufficient to mitigate potential interference. Positioning accuracy depends primarily on signal strength, while detection latency can vary based on interference conditions and other operational factors. These findings highlight the system's capacity for prompt and dependable alerts, which is essential for reducing the impact of RFI events.

3.1 User Interface and Operational Feedback

The newly developed map-based interface (Figure 1) offers interactive visualization of potential interference zones. Key interface features include:

- **Real-Time Alerts**: Color-coded markers and pop-up notifications indicate active or historical jamming/spoofing incidents.
- **Layered Geographic Information**: Users can toggle layers to review critical infrastructure, shipping lanes, or flight corridors affected by interference.
- **Incident Logs**: A historical record of detected events is available for further analysis, enabling operators to identify recurring patterns or hotspots.

Early feedback from technical operators and end users suggests that the interface is intuitive and facilitates rapid situational awareness. Users have particularly appreciated the overlay of system health data (e.g., satellite coverage, signal-to-noise ratio) to better contextualize the alerts.

3.2 System Scalability

In terms of scalability, initial load-testing indicates that the system monitoring platform can handle **a large** simultaneous data streams without noticeable performance degradation. This capacity allows the system to be scaled up for larger GNSS networks or expanded to cover additional geographical regions, providing 24/7 coverage in a quick and scalable way.

5. Discussion

The validation of the system demonstrates that a proactive, LEO-based approach to GNSS jamming and spoofing detection is both feasible and ready for operational testing. By integrating advanced algorithms and leveraging satellite data, the system improves interference detection reliability and achieves shorter detection latencies compared to conventional methods. This early success underlines the potential impact on critical sectors such as aviation, maritime, and other GNSS-dependent industries.

A key milestone will be the test service provided with a major airline in the coming months. This pilot phase offers an opportunity to gather real-world feedback, refine the data processing workflows, and adapt the system to dynamic

operational needs. By cooperating directly with an end user, the solution stands to accelerate its transition from a research-focused platform to a fully deployed commercial service.

Table 1 provides an overview of the planned rollout:

Start	Service	Duration	
15.04.2025	Testing Commercial service operations	3 Months	Major European Airline
01.07.2025	Early Commercial service	12 Months	4 hour delay for data availability **< 1 revisit per day**
01.07.2026	Commercial service		Commercial mapping **MVP: 1 revisit per day**
Payload deployment			
From 2029	Real Time Service		< 30 minutes delay for data availability

The phased approach is designed to balance immediate user needs with the complexity of scaling satellite infrastructure and refining algorithms. Early stages allow for incremental improvements in accuracy and data throughput, while long-term goals target near-real-time performance. Achieving less than a 30-minute delay will be especially crucial for highly time-sensitive applications, further solidifying the system´s position as a front-line defense against GNSS interference in both civil and commercial contexts.

Overall, the roadmap highlights how lessons learned from the testing and early service phases will pave the way toward a robust, real-time, and globally accessible RFI detection platform. By directly engaging with a major European Airline, the project ensures that system enhancements remain practical, ultimately helping to safeguard GNSS-reliant ecosystems worldwide.

6. Conclusions

The system presented provides a promising, cost-effective approach to GNSS jamming and spoofing detection by leveraging a LEO-based infrastructure and advanced algorithms, with ground assets. Initial validation efforts, including controlled interference scenarios, have demonstrated the system´s capability to detect and localize threats more rapidly than traditional methods. These successes are bolstered by the upcoming trial with an European Airline, which will allow real-world operational testing and iterative refinement of both the hardware and software components.

The phased roadmap, moving from early service pilots to near-real-time global coverage, highlights a clear path toward broader deployment across the aviation sector and other GNSS-dependent domains. In the long run, the proposed system´s ability to deliver timely, accurate, and actionable interference alerts will be instrumental in safeguarding critical infrastructure, enhancing safety-of-life services, and ensuring reliable global navigation services. Continued collaboration with industry partners and ongoing technical enhancements will ensure that the solution remains at the forefront of GNSS security solutions.

References

[1] N. Bowditch, The American Practical Navigator, Washintong, DC: Defense Mapping Agency Hydrographic Office, 1984.

[2] Pratap Misra, Per Enge, Global Positioning System. Signals, Measurements and Performance, Lincoln, Massachusetts: Ganga-Jamuna Press, 2012.

[3] T. A. Stansell, "The TRANSIT Navigation Satellite System," *Magnavox Technical Report,* pp. R-5933A, 1973.

[4] D. Hassan, "ISO/TC 20/SC 16. Uncrewed aircraft system," ISO, [Online]. Available: https://www.iso.org/committee/5336224.html. [Accessed 01 04 2025].

[5] "Sinister Spoofing in Shanghai," Inside, 10 December 2019.

[6] Alan Levin and Mary Schlangenstein, "Runway at DFW Airport temporarily closes while FAA looks into faulty GPS signals," The Dallas Morning News, Dallas, Oct. 18, 2022.

[7] 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. pp. 85515-85532, 2020, 2020.

[8] F. Gallardo and A. P. Yuste, "Operational Deployment of GNSS Anti-spoofing System for Road Vehicles," *Lecture Notes in Computer Science,* vol. 13120, pp. pp.15-26, 2021.