Evaluation of NovAtel's Jamming and Spoofing Detection and Mitigation Capabilities During Jammertest2024

Ali Broumandan, Ali Pirsiavash, Isabelle Tremblay, and Sandy Kennedy
Hexagon | NovAtel

Biographies:

Ali Broumandan received his Ph.D. degree from the Geomatics Engineering Department at the University of Calgary in 2009. He has about 20 years of experience in signal processing focusing on positioning, navigation and timing applications. Currently, he is with Hexagon's Autonomy & Positioning division as a principal research associate. He leads the resilient PNT team in the applied research group focusing on improving GNSS receiver performance in challenged operational environments.

Ali Pirsiavash is a research associate at Hexagon's Autonomy & Positioning division and has over 10 years of academic and industrial experience in GNSS and telecommunications signal processing and system design. He received his Ph.D. in Geomatics Engineering from the University of Calgary in 2019, with a specialization in positioning, navigation, and wireless location. Ali's current research interests include signal processing and receiver design for precise and resilient GNSS applications.

Isabelle Tremblay holds a B.A.Sc. in Geomatics from Laval University (1996). She is currently working with Hexagon's Autonomy & Positioning division as a geomatics designer and has more than 20 years of experience working in the GNSS industry.

Sandy Kennedy is vice president of innovation at Hexagon's Autonomy and Positioning division. She is responsible for directing applied research activities to support the vision of: *Autonomy and Positioning – Assured.* She completed both her B.Sc. and M.Sc. degrees in Geomatics Engineering at the University of Calgary, in 2000 and 2002 respectively. She has spent over 20 years in R&D at NovAtel and A&P, developing leading-edge positioning technology and working with a diverse, global customer base.

Abstract — In September 2024, the annual Jammertest event was conducted in Bleik, Norway, serving as a comprehensive testing ground for GNSS technologies under real-world interference conditions. The event, held on the island of Andøya, was designed to evaluate the performance and resilience of GNSS systems by broadcasting a variety of jamming and spoofing signals. These controlled tests simulated sophisticated hostile environments to assess the reliability and mitigation strategies of civilian GNSS signals and receiver technologies. This paper focuses on the performance of Hexagon │ NovAtel's OEM7 receivers, specifically their ability to detect and mitigate the effects of these intentional interferences. Leveraging data collected during Jammertest, the evaluation highlights the role of NovAtel's GNSS Resilience and Integrity Technology (GRIT) platform. GRIT is shown to provide advanced situational awareness and robust tools for identifying and mitigating interference across all GNSS frequency bands. This technology demonstrates efficacy under a range of challenging conditions, including multi-frequency and multi-band jamming, as well as spoofing attacks designed to mislead navigation solutions. Additionally, the paper presents results from the Galileo OSNMA feature. OSNMA, a cryptographic authentication service, adds an extra layer of security by validating the authenticity of GNSS data. The findings from Jammertest highlight the critical advancements in anti-jamming and anti-spoofing technologies. They emphasize the need for continuous innovation in GNSS receiver design to meet the challenges posed by evolving interference threats while ensuring reliable and secure navigation for civilian users.

1 INTRODUCTION

Civilian Global Navigation Satellite Systems (GNSS) play a crucial role in critical infrastructure and safety-critical applications. A wide range of civilian applications, from aviation, maritime, and vehicular navigation to smart-phone applications and wearable devices, rely on GNSS for their positioning and timing solutions, the disruption of which can interfere with every-day-life or critical operations, and even jeopardize human safety. GNSS signals are vulnerable to jamming and counterfeit spoofing signals, due to their low reception power and publicly available signal structure. The risk of GNSS spoofing has grown in recent years, given the conflicts around the world and particularly with the advancement of software defined radio technologies.

Several types of spoofing attacks have been presented and discussed in the literature, a review of which can be found in Jafarnia-Jahromi et al., 2012a. In a basic scenario, a GNSS repeater can be used to carry out a meaconing attack. A repeater system includes a GNSS antenna that captures real GNSS signals, an amplifier that boosts signal strength, and a transmitting antenna that propagates high-power signals, potentially overpowering authentic signals at the target receiver. The encrypted ranging code and navigation messages are not immune to this type of attack. In a signal simulator scenario, simulated spoofing signals are paired with a radio transmitter, where generated spoofing signals are not necessarily synchronized to the authentic signals. A more complicated type of spoofing attack consists of a GNSS receiver coupled with a spoofing transmitter. By approximating the target receiver's location, the spoofer can synchronize its signals with the authentic ones, extract time and navigation information, and generate counterfeit signals that match both the code and frequency of the legitimate signals. This type of spoofing attack is challenging to detect as the spoofing signals are synchronized with those coming down from actual satellites, and such attacks can be carried out using readily available software-defined radios (Curran et al., 2018). To combat this, various spoofing detection techniques have been proposed that leverage unique characteristics of counterfeit signals to distinguish them from genuine GNSS signals. These methods are implemented on both single-antenna (Bhatti & Humphreys, 2017; Pirsiavash et al., 2016; Psiaki & Humphreys, 2016) and multi-antenna receiver platforms (Borio & Gioia, 2015; Vagle et al., 2018). For single-antenna systems, spoofing detection metrics are applied in either the pre-despreading or post-despreading stages of the GNSS receiver. These metrics are most effective when both spoofed and authentic signals are present. Pre-despreading techniques focus on detecting excessive power in GNSS bands, under the assumption that spoofed signals are stronger than legitimate ones (Jafarnia-Jahromi et al., 2014, 2012b). Post-despreading methods, on the other hand, analyze abnormal signal behavior caused by spoofing after whipping off the spreading code (e.g., Jafarnia-Jahromi et al., 2013; Pirsiavash et al., 2017; Broumandan & Curran 2017; Wesson et al., 2017; Pirsiavash 2019).

Given the above introduction and to tackle the increasing challenges and security concerns surrounding GNSS systems, NovAtel OEM7 receivers include cutting-edge technologies, designed to effectively detect and counteract GNSS-related threats. **FIGURE 1** provides an overview of NovAtel's GNSS resilience solutions and technologies. The GNSS Resilience and Integrity Technology (GRIT) platform enhances situational awareness and provides robust tools for detecting and mitigating interference across a wide range of applications and environments. Key components include the Interference Toolkit (ITK), Spoofing Detection Toolkit (SK), and Robust Dual-Antenna Receiver (RoDAR), which utilize a variety of countermeasures, ranging from advanced jamming detection and analysis to spoofing detection and prevention, ensuring the integrity and reliability of GNSS solutions (Broumandan et al., 2020). Additionally, the recently introduced Galileo Open Service Navigation Message Authentication (OSNMA) module adds an extra layer of security by verifying the authenticity of navigation messages from Galileo E1 signals. In September 2024, the Jammertest event took place in Bleik, Norway, where various interference attacks were simulated to disrupt GNSS signals. This paper evaluates the performance of NovAtel's OEM7 receivers in identifying and mitigating jamming and spoofing threats, using real-world data collected during the event. Through comprehensive spectrum monitoring and jamming analysis across all GNSS bands, NovAtel receivers were able to effectively detect and characterize jamming activities. Furthermore, the performance of GRIT's anti-jamming and anti-spoofing capabilities was validated through complex test scenarios involving both spoofing and jamming attacks. The OSNMA results are also presented, highlighting its role as a complementary layer of protection, working synergistically with other monitoring techniques toward a more resilient solution.

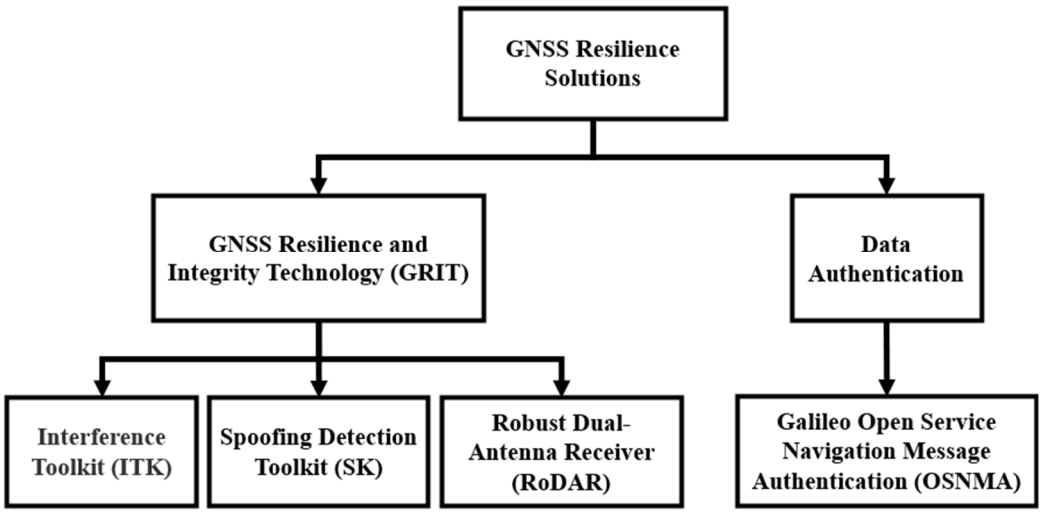

FIGURE 1 Overview of NovAtel's GNSS resilience solutions and technologies

2 GNSS RESILIENCE AND INTEGRITY TECHNOLOGY (GRIT)

GRIT is a NovAtel OEM7 firmware suite that delivers situational awareness and advanced interference mitigation tools including interference detection and characterization, spoofing detection, time-tagged digital snapshots spatial processing, and null-steering.

2.1 Interference Toolkit (ITK)

NovAtel receivers are designed to track signals across multiple frequencies, delivering the high precision and performance they are renowned for. As the radio frequency (RF) spectrum becomes increasingly congested, electronic devices can unintentionally interfere with GNSS signal bands. To address this, NovAtel has developed the ITK technology for its OEM7 receivers. ITK measures GNSS RF spectrum levels and applies advanced mitigation techniques to protect signal and measurement quality, ensuring reliable multi-frequency, multi-constellation positioning performance even under congested and challenging environments. ITK identifies interference occurrence and characterizes the detected jammer in time and frequency domains. Mitigation strategies include the use of notch filters to eliminate interference at specific frequencies, along with a High Dynamic Range (HDR) mode to counteract the effect of wideband interference.

2.2 Spoofing Detection Toolkit (SK)

A real-time SK, available in NovAtel's OEM7 receivers, employs a selection of the most effective spoofing detection metrics over a multi-frequency, multi-constellation platform, covering all the civilian GNSS signals and frequency bands. The detection outputs derived from different metrics are fed to an onboard central unit, where the ultimate decision is made whether the receiver is under spoofing attack or not. The goal is to minimize the likelihood of false alarms caused by jamming and multipath signals, while ensuring high-confidence detection of spoofing attacks. The implemented spoofing detection has gone through extensive tests, showing a successful performance in almost all spoofing scenarios, detailed information on which can be found in Broumandan et al., (2020, 2024).

2.3 Robust Dual-Antenna Receiver (RoDAR)

RoDAR is an active anti-jamming tool that uses spatial processing to defend against different types of interference and spoofing scenarios. In this solution, RF signals from two antennas are passed to the null-steering weight calculation unit after down conversion and digitization. The second antenna signal is processed through phase rotation and gain compensation based on the calculated array weights and is removed from the first antenna signal. The cleaned, jamming- and spoofing-free signal samples are then forwarded to the tracking and data processing modules for a resilient navigation solution. RoDAR provides up to 30 dB of nominal protection compared to an unprotected receiver and is classified as commercial good for export control purposes. The OEM7 multi-constellation and multi-frequency capabilities offer resiliency through frequency diversity. In high-threat conditions, RoDAR steps in, providing active anti-jamming across two GNSS bands.

3 DATA AUTHENTICATION AND OSNMA

Implementing robust data authentication mechanisms is a key focus in the continued development of GNSS resiliency in NovAtel receivers, with the OSNMA module serving as a prime example. OSNMA provides Galileo users with cryptologic protection by exploiting authentication information to ensure the navigation data received from Galileo is from the system itself and has not been altered. The process is based on the Timed Efficient Stream Loss-tolerant Authentication (TESLA) protocol where the authenticating key is broadcast with delays for all satellites, enabling auto- and cross-authentication of data from different satellites. The OSNMA data is broadcast within the reserved bits embedded in the odd page parts of a nominal Galileo E1B I/NAV message, to include an 8-bit Header and Root Key (HKROOT), and a 32-bit Message Authentication Code and Key (MACK). During a nominal sub-frame, 15 pages are transmitted every 30 seconds to build up a set of 120-bit HKROOT and 480-bit MACK messages. HKROOT provides a Digital Signature Message (DSM) over a sequence of blocks comprising the public and root key information. MACK includes the TESLA chain key, and the authentication tags and related information, used to verify the authenticity of the navigation data (Galileo OSNMA SIS ICD 2022; Galileo OSNMA Receiver Guidelines 2024). In the receiver, the authentication process is initialized by retrieving and verifying the public key (retrieved from space or directly from the OSNMA server) and root key depending on the stored information available at the receiver's start. Once the root key is verified, the TESLA chain key and navigation message authentication stage is set. The verified key takes the navigation data and replicates the authentication tags to be matched with those received from space and decides about the authenticity of the navigation message, commencing by bootstrapping the TESLA chain key verification by the root key, leading to a steady state where the chain key is authenticated by its predecessor verified in the preceding subframe (Pirsiavash et al., 2024).

4 JAMMERTEST 2024

This section details the outcomes from Jammertest 2024, a comprehensive five-day, over-the-air broadcast jamming and spoofing test event. This event was conducted in September 2024 by the Norwegian Public Roads Administration in collaboration with the Norwegian Communications Authority, the Norwegian Metrology Service, and the Norwegian Space Agency. The testing took place at Bleik, located on Andøya Island, a location known for its suitability for such specialized experiments.

The performance of the NovAtel OEM7 GNSS receiver technology integrated into PwrPak7 enclosures was evaluated. These state-of-the-art devices were subjected to rigorous testing scenarios designed to simulate real-world jamming and spoofing conditions. For specific jamming test series, NovAtel's RoDAR capability, implemented on OEM718D receiver cards, was employed. These cards were connected to Hexagon | Antcom - antennas, and the entire setup was mounted on a dedicated test vehicle. The PwrPak7 and a competitor receivers were connected to a geodetic-grade GNSS-850 antenna, as illustrated in **FIGURE 3**.

During the experiments, the PwrPak7 receiver served dual purposes: it was used to monitor the spectrum environment and to provide situational awareness, particularly for detecting and analyzing jamming and spoofing events. Comprehensive data logs, including NovAtel's ITK and SK logs, were collected throughout the test. These logs allowed for in-depth analysis of jamming and spoofing incidents, both in real-time and during post-processing. This approach facilitated the validation of the receiver's resilience and capabilities under hostile signal conditions.

The PwrPak7 receiver was configured to operate with multi-frequency and multi-constellation capabilities, allowing it to track all available GNSS signals during the test scenarios. This configuration provided comprehensive coverage and robustness in diverse signal environments. In the following sections, the detailed outcomes from the tests, focusing on the receiver's behavior when subjected to jamming and spoofing events are provided. Key findings demonstrate the effectiveness of detection and mitigation strategies, leveraging NovAtel's GRIT under selected test scenarios. GRIT's performance highlights the receiver's ability to adapt to hostile signal conditions while maintaining integrity and reliability. Signal quality was evaluated using the average carrier-to-noise density ratio (C/N_0). The impact of jamming and spoofing on the receiver's positional accuracy was also analyzed, comparing performance metrics between the RoDAR-equipped system and the single-antenna PwrPak7 configuration. These analyses reveal the robustness of the technologies under attack conditions.

Additional insights are provided by the receiver's power monitoring capabilities, as reported through ITK logs. Real-time spoofing detection results were also captured and analyzed using the SK logs. These tools provided critical data for understanding and mitigating the effects of interference and spoofing.

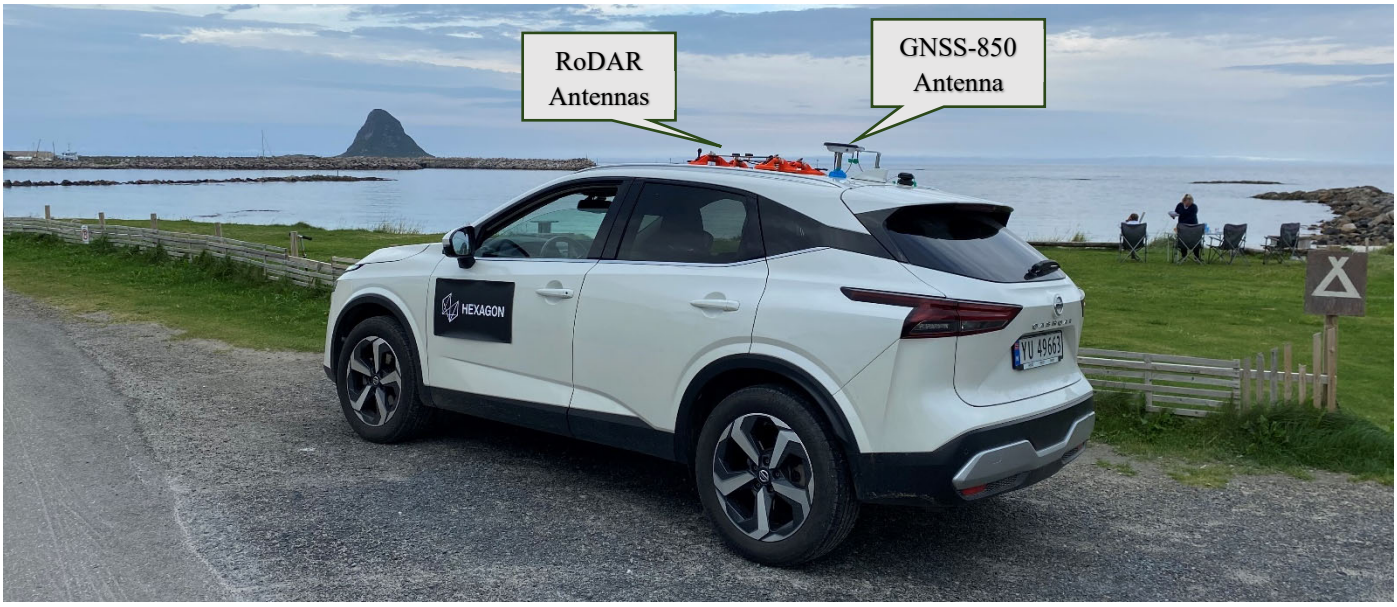

FIGURE 2 NovAtel test vehicle with single- and dual-antenna setup on the roof

Finally, the navigation message authenticity of Galileo E1 signals through the implementation of Open Service Navigation Message Authentication (OSNMA) was evaluated. This onboard feature validates the integrity of navigation messages, showcasing the receiver's capability to enhance trust in GNSS signals even under potentially compromised conditions. **FIGURE 2** shows the test vehicle with the antenna mounted on the roof. The receivers, including the NovAtel PwrPak7 and other test equipment, are arranged inside the vehicle to facilitate real-time monitoring, data logging, and analysis.

On Day 1 of Jammertest 2024, held on September 9, 2024, the focus was on high-power stationary jamming scenarios. The test sessions were conducted at the Bleik community centre. For this test, high-power stationary jamming scenarios were executed to evaluate GNSS receiver resilience under various interference conditions. The tests featured the "Porcus Major" jammer transmitting different signal types, including continuous wave (CW) signals, frequency sweeps, and pseudo-random noise (PRN) signals. These signals targeted multiple GNSS bands, such as L1, G1, L2, and L5, at a consistent power output of 50 W. Key scenarios included single-frequency and multi-frequency interference, as well as dynamic power ramping tests where signal strength increased incrementally from micro-watt levels to 50 W. A unique pyramid sequence test was also performed, covering a range of frequencies, to further stress test the systems. These scenarios were designed to measure GNSS receivers' ability to detect, mitigate, and maintain performance in the presence of various jamming techniques.

FIGURE 3 shows the GNSS signal upper and lower band spectrum during Day 1. As shown, a wide variety of jamming and attacks were generated, including single-band, dual-band, multi-band, high-power, chirp jammer and frequency sweep. The figure provides a visual representation of how these jamming techniques manifest within the spectrum, offering insights into their impact on GNSS signals and receiver behavior.

4.1 RoDAR performance on Day 1

This section presents selected test results from Day 1 of the Jammertest 2024. The focus is on evaluating the performance of GNSS receivers under high-power jamming scenarios. **FIGURE 4a** shows a detailed view of the signal spectrum centered on the GPS L1 C/A band as observed over time during the test. This visualization highlights the impact of a jamming signal specifically targeting this frequency band. The jammer employed in this scenario operates with a 5 MHz bandwidth, effectively spanning the key portion of the L1 C/A signal spectrum. **FIGURE 4b** shows the total in-band power across the L1, L2, and L5 frequency bands over time, as measured directly by the OEM7 receiver during a high-power ramping test. The results highlight the progressive rise and fall of jammer power throughout the test. In the absence of jamming, the baseline noise level at the L1 band is approximately -75 dBm, indicating a clear signal environment prior to interference.

FIGURE 4c shows the mean carrier-to-noise density ratio (C/N_0) values for GPS L1 C/A and Galileo E1 signals, measured by the RoDAR unit. For comparison, data from a competitor receiver was processed and overlaid on this figure. The comparison reveals differences in performance under jamming conditions. In the absence of jamming, the competitor receiver exhibits a higher average C/N_0 than the RoDAR unit. This is due to the GNSS-850 antenna used with the competitor receiver, which has a higher gain than the 1.2G antenna paired with the RoDAR unit. However, the performance gap changes significantly once the jammer is introduced. The competitor receiver experiences a substantial drop in C/N_0 values—by approximately 20 dB—due to the jamming signal. This decline eventually causes the competitor receiver to lose its ability to track signals entirely. In contrast, the RoDAR unit, benefiting from its null-steering technology to mitigate interference, maintains continuous tracking of GPS L1 signals throughout the test. These results demonstrate the resilience of the RoDAR system under high-power jamming conditions, highlighting its capability to sustain reliable navigation performance.

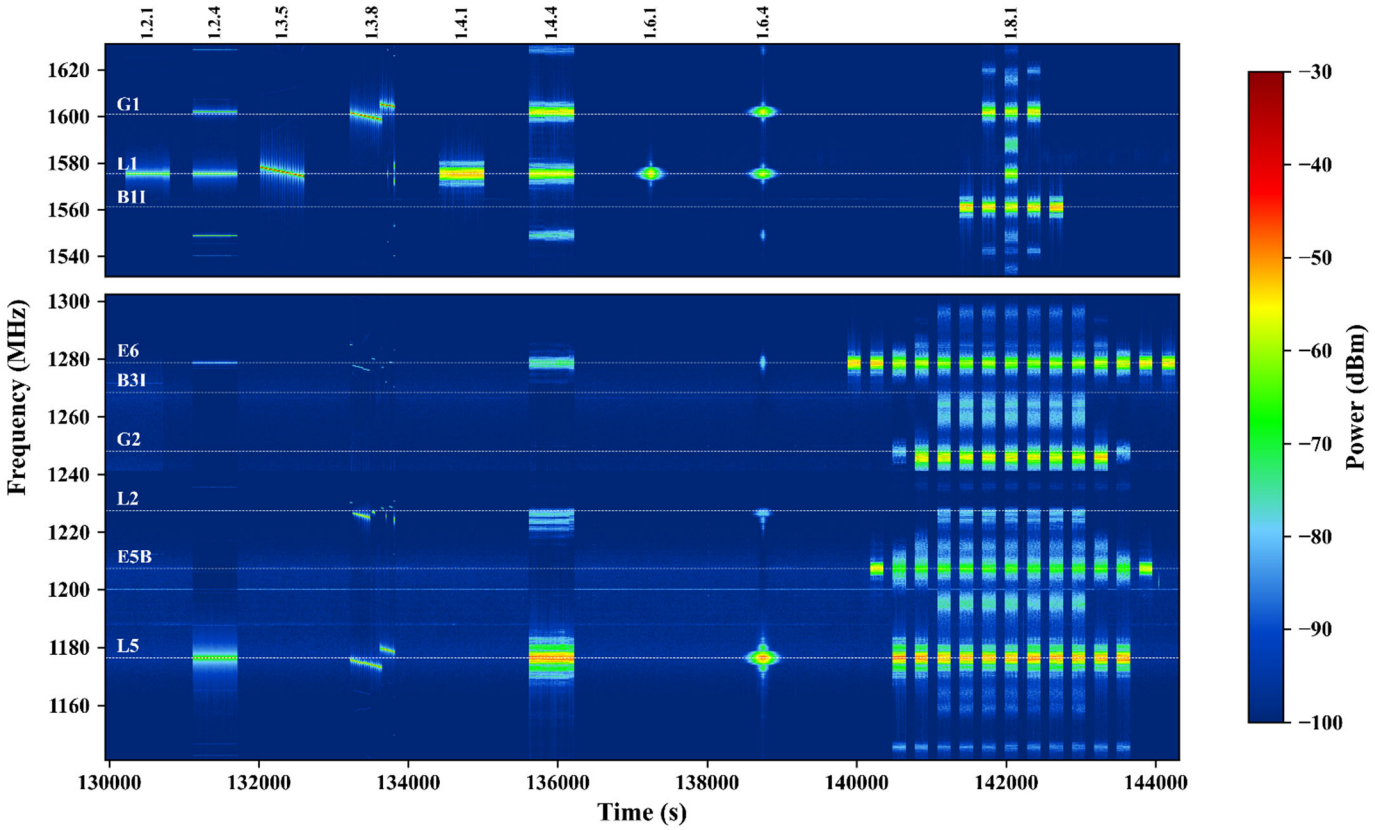

FIGURE 3 Signal spectrum at upper and lower GNSS bands during Day 1

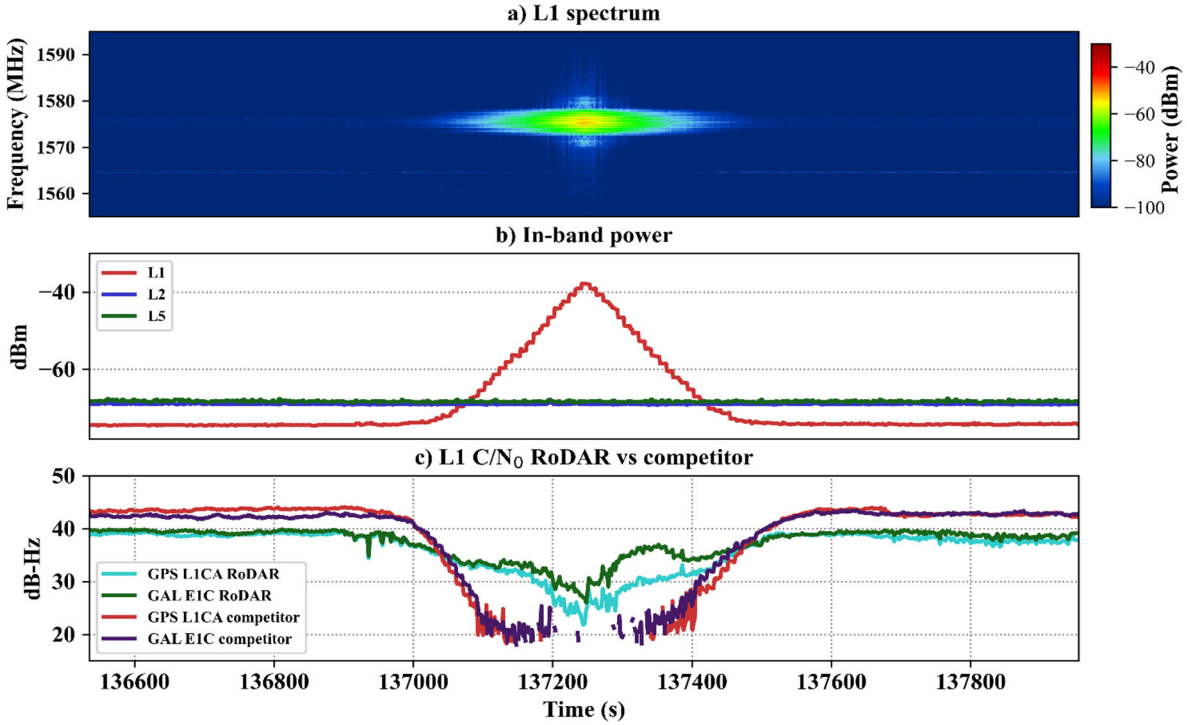

FIGURE 4 a) Signal spectrum centered on the GPS L1 C/A band b) Input power measured by ITK during the ramp power jammer at L1, L2, and L5 bands c) C/N₀ values of RoDAR and competitor receivers

Test 1.6.4 was designed similarly to the previously described test (1.6.1) with the primary difference being that the ramped power interference targeted all frequencies, rather than a single band. This variation allowed for a broader evaluation of GNSS receiver performance across multiple bands simultaneously under high-power jamming conditions.

FIGURE 5a illustrates the GNSS signal spectrum during the jamming event, clearly showing the broad-spectrum interference impacting the L1, L2, and L5 bands. The spectral plot highlights the presence and strength of jamming signals across these frequency ranges. **FIGURE 5b** provides a time-series representation of the total in-band power for the L1, L2, and L5 frequency bands. The graph demonstrates how jammer power increased gradually across all frequencies during the test and then decreased, following the ramp power profile. **FIGURE 5c** shows the mean C/N₀ values for GPS L5 and Galileo E5A signals, as measured by the RoDAR unit and a competitor receiver. The competitor receiver shows a significant drop in C/N₀ values—approximately 25 dB—caused by the strong jamming signals. This degradation in signal quality eventually results in the competitor receiver completely losing its ability to track both GPS L5 and Galileo E5A signals. In contrast, the RoDAR unit demonstrates superior resilience under these challenging conditions. The RoDAR unit effectively mitigates interference, maintaining stable C/N₀ values and continuous tracking of GPS L5 signals throughout the test. These results highlight the effectiveness of the RoDAR system in handling wideband jamming scenarios.

FIGURE 6 illustrates the outcomes of two scenarios that were part of Test 1.8.1, which assessed the performance of the system under conditions where the power levels at the L1, L2, and L5 frequency bands experienced a sudden surge. **FIGURE 6a** shows the input power levels for the L1, L2, and L5 bands. As shown in the figure, the power in all three bands increased significantly, by approximately 30 dB, simulating a challenging interference scenario. **FIGURE 6b** compares the average C/N₀ performance of the RoDAR receiver with that of a competitor receiver.

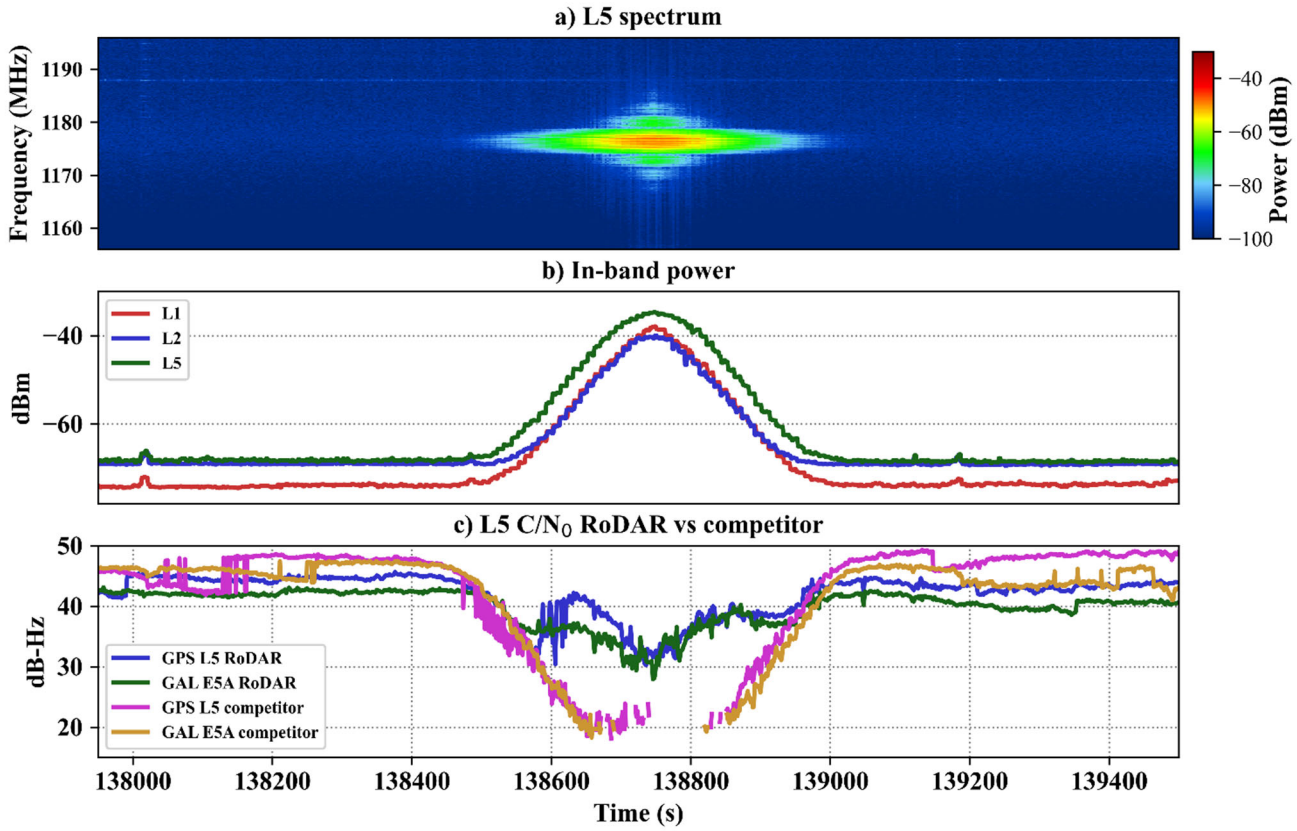

FIGURE 5 a) Signal spectrum centered on the GPS L5 band b) Input power measured by ITK during the ramp power jammer at L1, L2, and L5 bands c) C/N₀ values of RoDAR and competitor receivers

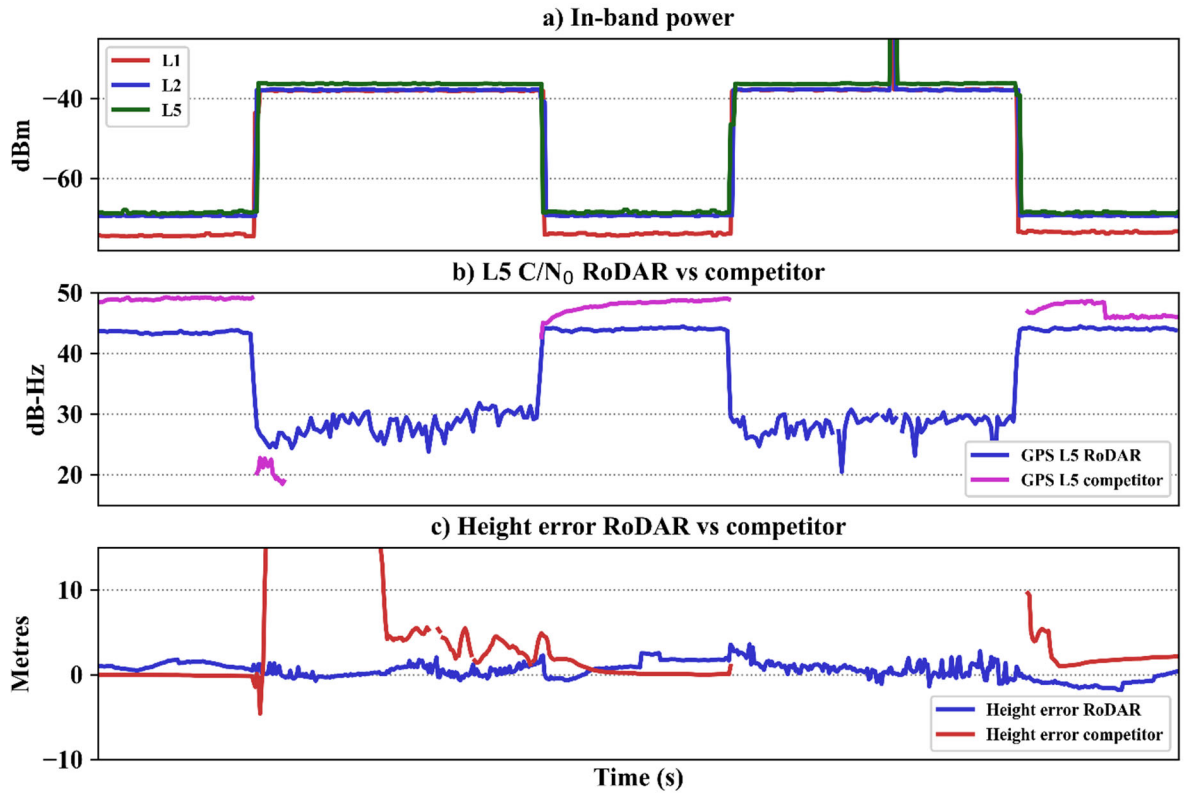

FIGURE 6 a) Input power at L1, L2 and L5 bands, b) Average C/N₀ RoDAR vs competitor at GPS L5, c) Height error of RoDAR vs competitor

The competitor receiver, which is capable of tracking all GNSS bands and is equivalent to the OEM7, exhibited a notable reduction in C/N₀ under these conditions. In contrast, the RoDAR receiver, which features null-steering capabilities at the GPS L5 band, effectively protected GPS L5, Galileo E5a, and BeiDou B2A signals. This enabled continuous tracking of these signals despite the interference.

FIGURE 6c provides a comparison of the position solution performance between the RoDAR receiver and the competitor receiver. The results highlight a clear distinction between the two systems. The competitor receiver struggled to manage the jammer's impact, resulting in the loss of position solutions. On the contrary, the RoDAR receiver maintained continuous position and navigation solutions throughout the test, demonstrating its robustness against jamming and interference.

4.2 Spoofing detection and mitigation results on Day 2

Day 2 of the testing involved assessing the system's resilience to jamming and meaconing attacks. This section focuses specifically on the results of the meaconing attack evaluations. The tests conducted during this phase included stationary meaconing scenarios with variations in both signal power and the duration of time the system was exposed to the meaconing signals. These scenarios were designed to simulate a GNSS signal retransmission environment, where authentic live-sky satellite signals were rebroadcasted. In such cases, the retransmitted GNSS signals represent a deceptive environment, appearing as real satellite data but with slight time delays. This creates a scenario where the system perceives an incorrect position, based on genuine but delayed satellite signals. The vehicle remained stationary throughout the duration of the experiment, providing a fixed reference point for comparison. Additionally, the meaconing position was positioned approximately 300 m above the height of the stationary vehicle. This elevation difference makes it straightforward to assess whether the position, as reported by the receiver, had been manipulated or not.

FIGURE 7 shows the signal spectrum logged during these tests, showing both the upper and lower GNSS frequency bands. These results are critical for evaluating the effectiveness of mitigation strategies against GNSS spoofing techniques like meaconing, where the authenticity of the signals makes detection and protection particularly challenging.

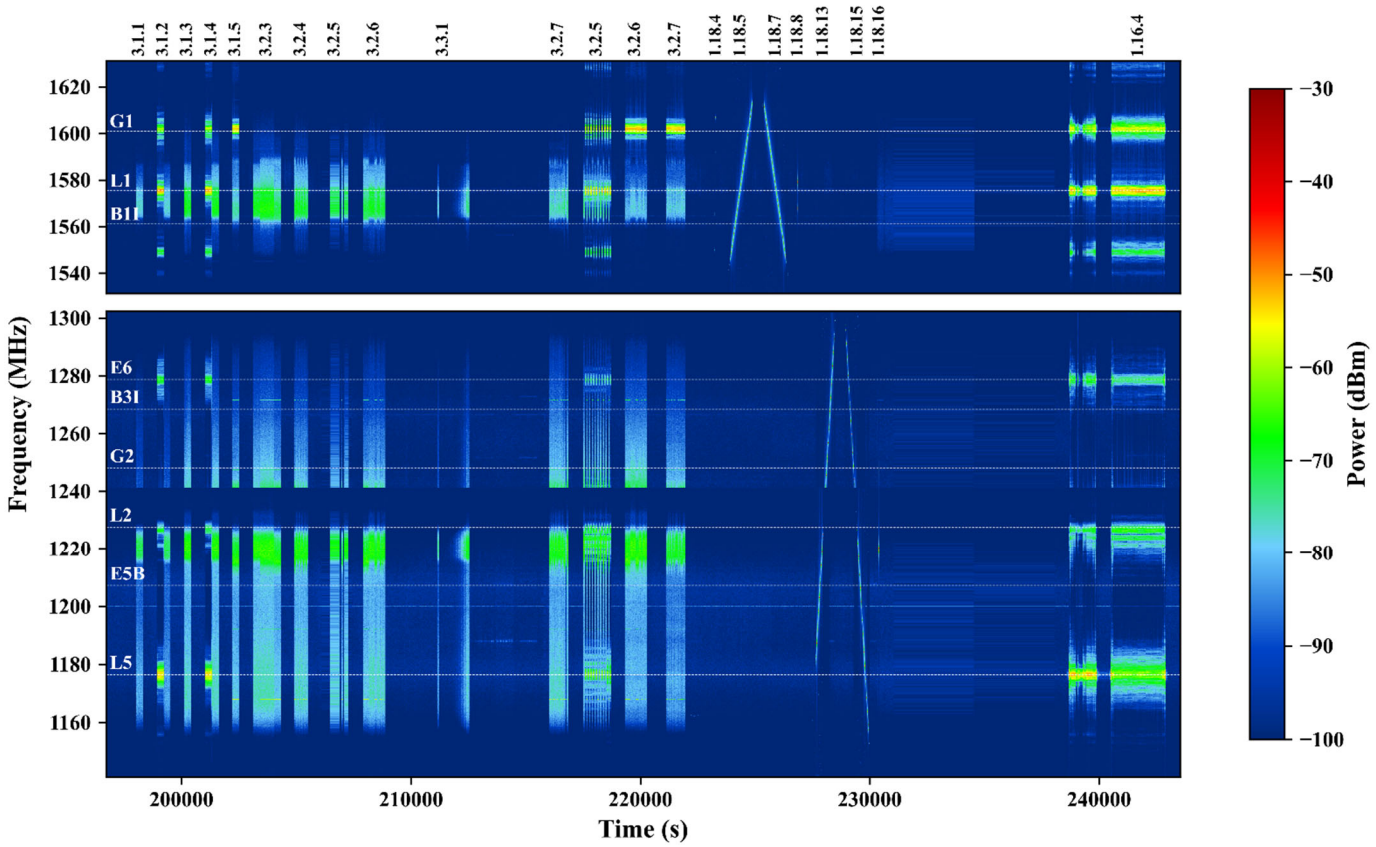

FIGURE 7 Signal spectrum at upper and lower GNSS bands during Day 2

FIGURE 8 shows a) the signal spectrum at the L1 band during the jamming and meaconing scenarios, b) in-band power measured by ITK at L1, L2 and L5 bands, c) average C/N$_0$ values (average of all tracked PRNs at a given epoch) of GPS L1 C/A, Galileo E1C and GPS L5. **FIGURE 9** shows the jamming, spoofing and OSNMA detection results along with the position error under the same jamming and meaconing results as in **FIGURE 8**. Four different scenarios, namely 3.1.4, 3.1.5, 3.2.3, and 3.2.4, are considered in these figures. **TABLE 1** provides more details of each scenario.

TABLE 1: Meaconing scenarios demonstrated in **FIGURE 8** and **FIGURE 9**

Scenario	Start time	Finish time	Description
3.1.4	201022	201622	Meacon F1.1: RX1 at 10 W with initial jamming.
3.1.5	202222	202522	Meacon F1.1: RX2 at 10 W
3.2.3	203122	204322	Meacon F1.1: RX1 and RX2 at 10 W turned on and off at different times
3.2.4	204922	205522	Meacon F1.1: RX1 and RX2 at 10 W alternating

The meaconing scenario shown **FIGURE 8** started with a high-power jammer at all three GNSS bands. **FIGURE 9** shows that the jamming flag is enabled. In this case, the single antenna receiver (PwrPak7) was overwhelmed and could not track any signals at the L1 and L5 bands. However, as shown in **FIGURE 8c**, the RoDAR receiver mitigated the jamming signal and tracked the authentic satellites. After the jamming event, the meaconing attack was initiated, and the single antenna receiver started tracking replayed GNSS signals. As shown in **FIGURE 8b**, the meaconing power decreased at the L1 and L5 bands. The SK spoofing detection module detected this attack as soon as there were enough tracking channels to provide position solutions (**FIGURE 9a**).

FIGURE 9b shows the OSNMA results for this scenario. The receiver tracked nine Galileo E1 signals where navigation messages were reported authentic, except for the epochs where jamming interference interrupted the reception of OSNMA-required data. The OSNMA results are color-coded. The blue dots refer to the epochs where authentication cannot be performed due to the lack of valid data required for OSNMA verification. This is usually the case in a cold start when the receiver is still waiting to receive data and set the crypto parameters.

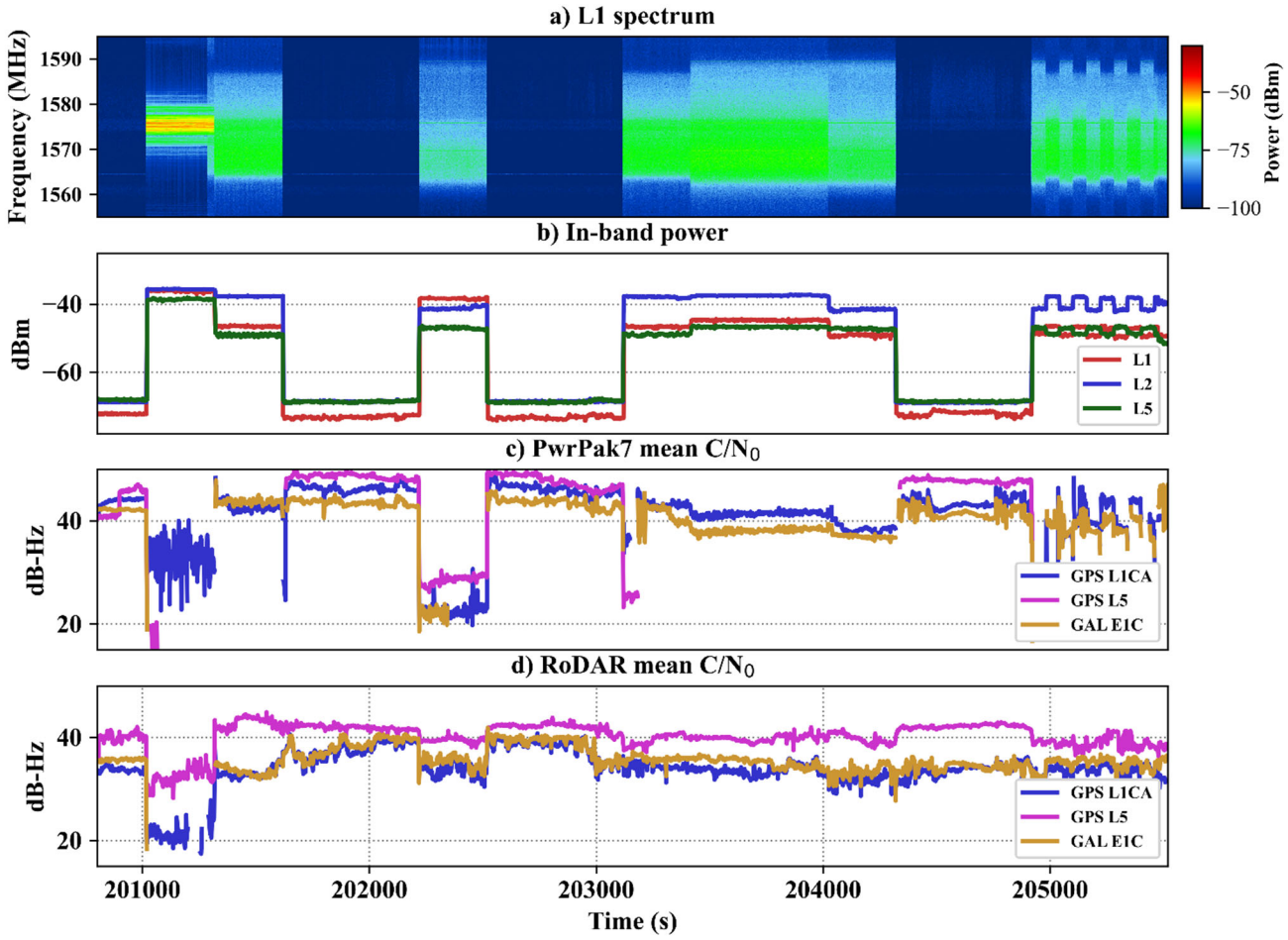

FIGURE 8 Monitoring results of the meaconing attack

This can also be the case when OSNMA data reception is interrupted and does not include all authentication-required information. The red dots indicate all data required for OSNMA (authenticating data and that to be authenticated) is available, but verification failed. This may happen when an unauthorized signal, with either an invalid navigation message or invalid OSNMA data or both, is being received by the receiver. The green dots refer to the situation when all data required for OSNMA is available and authentication is verified. Although not designed for mitigation of meaconing, this revealed the vulnerability of OSNMA service against meaconing attacks.

FIGURE 9c compares the position solutions of a receiver without considering the spoofing detection flag (spoofer not mitigated), a solution that considers the spoofing detection flag and removes the measurements getting into the position solutions, and RoDAR unit that mitigated the meaconing attack via null-steering. As shown, if a single antenna receiver ignores the spoofing detection flags, the position solution is spoofed. One possible remedy to the spoofing attack is to remove the detected measurements and prevent them from entering the position engine. As shown, the position solution is not spoofed; however, it suffered from the lack of enough satellites. In contrast, utilizing the antenna null-steering method RoDAR did not get spoofed and provided a reliable position solution.

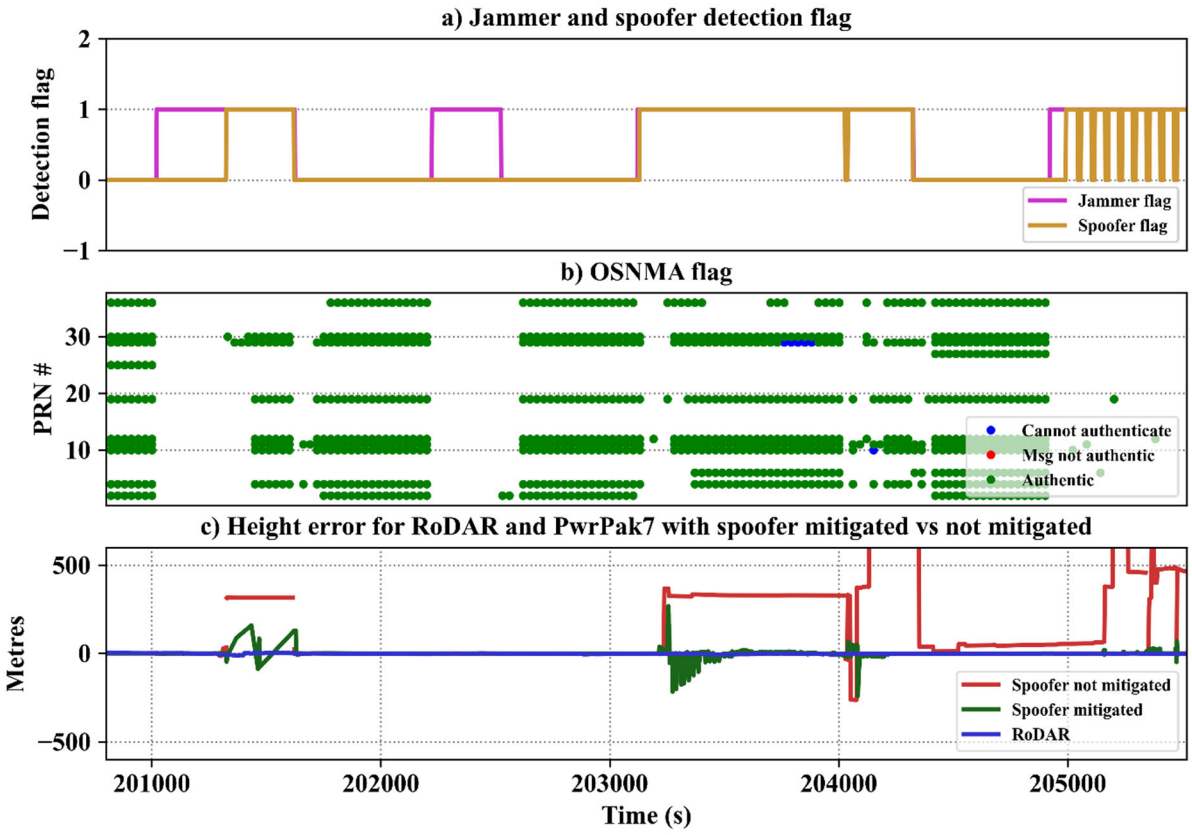

FIGURE 9 Detection and results of a meaconing attack

FIGURE 10 shows a) the signal spectrum at the L1 band during the jamming and meaconing scenarios, b) in-band power measured by ITK at L1, L2, and L5 bands, c) and d) average C/N_0 values (average of all tracked PRNs at a given epoch) of GPS L1 C/A, Galileo E1C, and GPS L5 for the competitor and RoDAR receivers, respectively. **FIGURE 11** shows a) jamming and spoofing and b) OSNMA detection results along with c) the position error under the same jamming and meaconing results as in

FIGURE 10. Three different scenarios, namely 3.2.7, 3.2.5 and 3.2.6, are considered in these figures. **TABLE 2** provides more details of each scenario.

TABLE 2: Meaconing scenarios demonstrated in **FIGURE 10** and **FIGURE 11**

Scenario	Start time	Finish time	Description
3.2.7	216019	216859	Meacon F1.1: RX1 and RX2 at 10 W alternating with different switching frequencies.
3.2.5	217519	218724	Meacon F1.1: RX1 and RX2 at 10 W alternating with breaks
3.2.6	219319	220279	Meacon F1.1: RX1 and RX2 at 10 W alternating with decreasing duration without breaks

As shown in

FIGURE 10d the RoDAR unit is capable of effectively mitigating spoofing attacks, ensuring the provision of continuous measurements and reliable position solutions. This capability is clearly reflected in the position solution results presented in **FIGURE 11c**, where the RoDAR unit maintains accuracy and stability under spoofing conditions. In contrast, the competitor receiver's performance is significantly impacted by the spoofing attack. Its measurements are compromised, leading to one of three outcomes: the position solution becomes unavailable, it is spoofed, or it suffers from noticeable degradation in accuracy and reliability. These results highlight the superior robustness of the RoDAR unit against spoofing attacks.

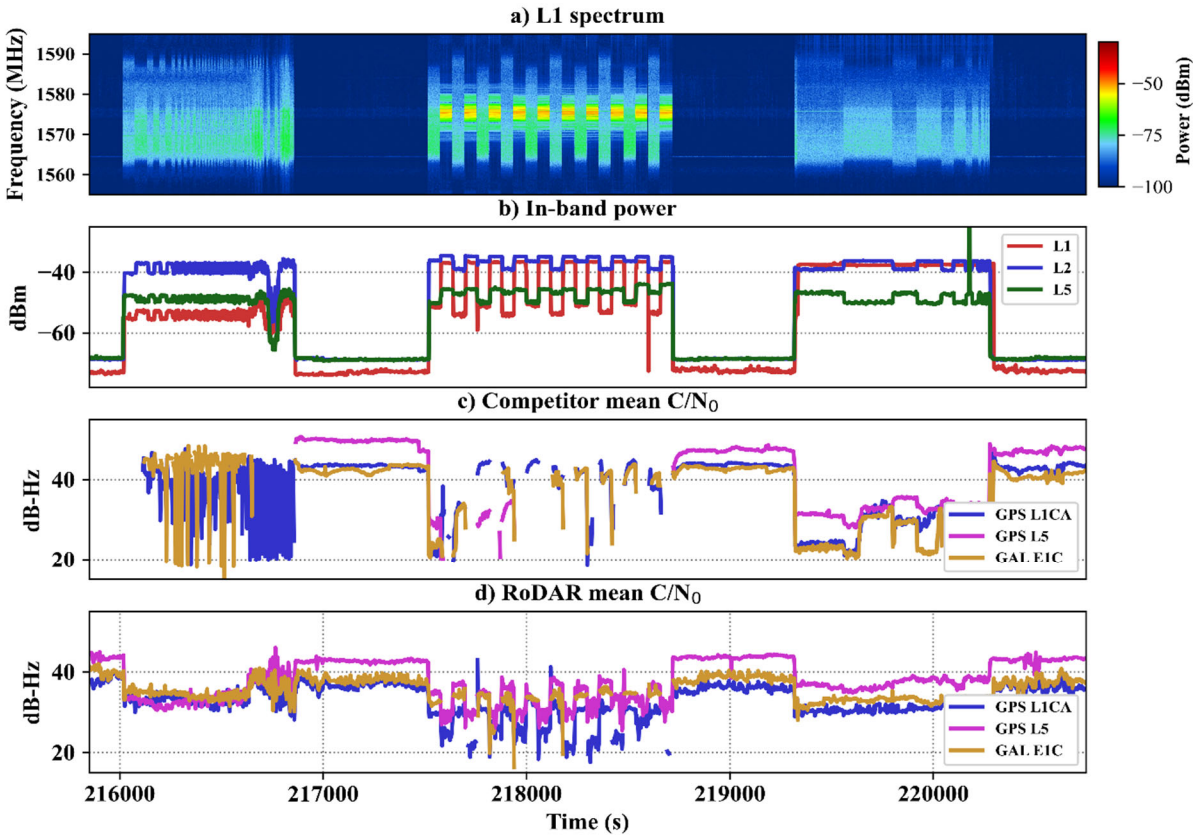

FIGURE 10 Monitoring of a meaconing attack

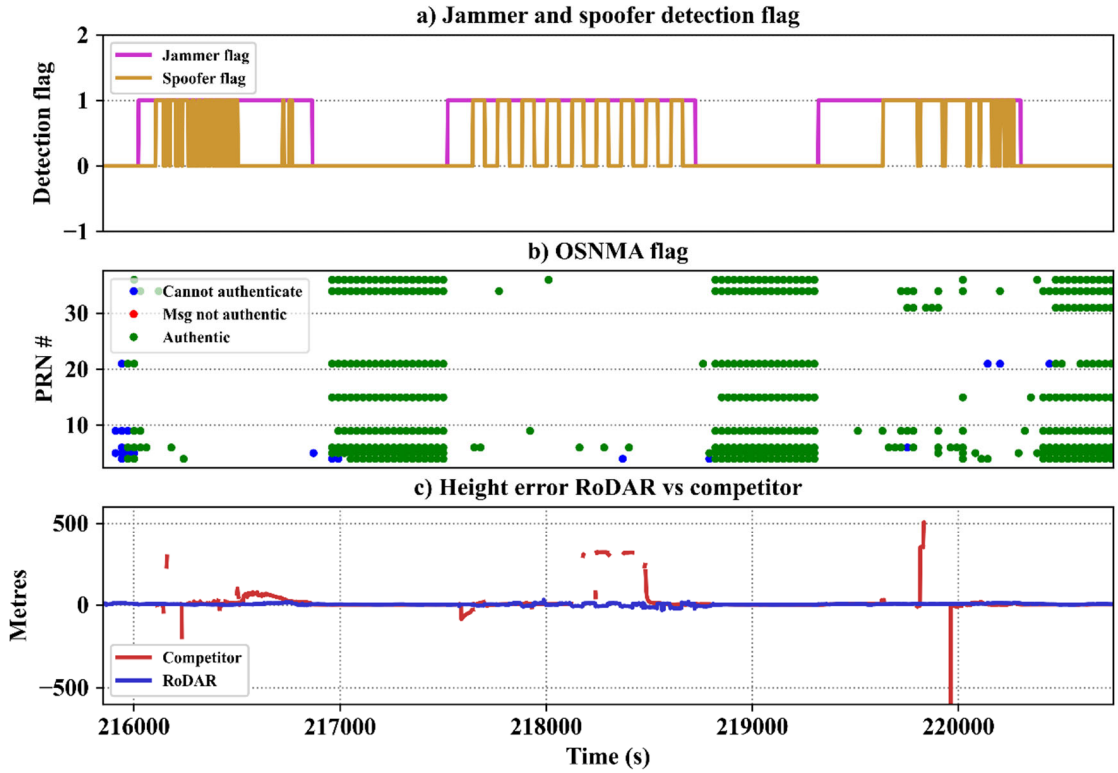

FIGURE 11 Detection and results of a meaconing attack

5 SUMMARY AND CONCLUSIONS

During the Norwegian Jammertest 2024, NovAtel's GRIT features were utilized to reliably detect and monitor interference and spoofing attacks. GRIT included modules for interference monitoring and characterization (ITK), receiver-based spoofing detection (SK), and the Robust Dual-Antenna Receiver (RoDAR). Additionally, Galileo Navigation Message Authentication using the OSNMA implementation was tested. The event spanned five days and featured live, over-the-air broadcast jamming and spoofing tests. An OEM7 receiver card housed in a PwrPak7 enclosure, paired with a GNSS-850 geodetic-grade antenna, was evaluated under a wide range of jamming and spoofing attack scenarios. These scenarios included single-band, dual-band, and multi-band interference, as well as high-power, directional, omni-directional, in-car, handheld, static, and kinematic configurations. Sophisticated spoofing attacks were also conducted, targeting both single and multiple frequency bands. During the tests, spoofing impacted the receiver's position and timing solutions. However, the onboard spoofing detection unit (SK) successfully identified all spoofing scenarios, including meaconing, in real-world, over-the-air conditions. The RoDAR system provided dual-band spatial null-steering protection along with support for multi-antenna and multi-constellation configurations. The experimental results highlighted RoDAR's superior interference mitigation capabilities compared to a competitor receiver under jamming and spoofing conditions. In jamming scenarios, RoDAR could withstand 15–25 dB more jamming power than the single-antenna receiver while maintaining position availability and accuracy. Against spoofing, RoDAR demonstrated strong resilience, using null steering to mitigate the effects of the spoofing source. The performance of position solutions incorporating feedback from the spoofing detection module was also validated, showcasing robust overall performance under attack.

REFERENCES

Bhatti, J., & Humphreys, T. E. (2017). Hostile control of ships via false GPS signals: Demonstration and detection. *Navigation*, *Journal of the Institute of Navigation*, vol. 64, no. 1.

Borio, D., & Gioia, C. (2015). A Dual-antenna spoofing detection system using GNSS commercial receivers. *ION GNSS+ 2015*, Tampa Florida

Broumandan,A., A. Pirsiavash, I. Trembley, S. Kennedy (2024) "Hexagon │ NovAtel's Jamming and Spoofing Detection and Classification Performance During the Norwegian JammerTest 2023," Proceedings of ION ITM conference 2024, Long Beach, California, January 22 - 25

Broumandan, A., & Curran, J. T. (2017). GNSS spoofing detection in covered spoofing attack using antenna array. *International Technical Symposium on Navigation and Timing (ITSNT) ,* 14-17 Nov, Toulouse, France.

Broumandan, A., Kennedy, S., & Schleppe, J. (2020). Demonstration of a multi-layer spoofing detection implemented in a high precision gnss receiver. *2020 IEEE/ION Position, Location and Navigation Symposium (PLANS)* DOI: 10.1109/PLANS46316.2020.9109842

Curran, J., Morrison, A., & O'Driscoll, C. (2018). Feasibility of Multi-Frequency Spoofing. *Inside GNSS*, https://insidegnss.com/infeasibility-of-multi-frequency-spoofing/

Galileo Open Service Navigation Message Authentication (OSNMA) Receiver Guidelines, (Jan. 2024). issue 1.3, European Union.

Galileo Open Service Navigation Message Authentication (OSNMA) Signal-In-Space Interface Control Document (SIS ICD). (Dec. 2022). issue 1.0, European Union.

Jafarnia-Jahromi, A., Broumandan, A., Nielsen, J., & Lachapelle, G. (2014). Pre-despreading authenticity verification for GPS L1 C/A signals. *Journal of the Institute of Navigation*, vol. 61, no. 1, 11 pages.

Jafarnia-Jahromi, A., Broumandan, A., Nielsen, J., & Lachapelle, G. (2012a, 29 May). GPS vulnerability to spoofing threats and a review of antispoofing techniques. *International Journal of Navigation and Observation,* vol. 2012, 16 pages.

Jafarnia-Jahromi, A., Broumandan, A., Nielsen, J, & Lachapelle G. (2012b, 1 May). GPS spoofer countermeasure effectiveness based on using signal strength, noise power and C/No observables. *International Journal of Satellite Communications and Networking*, 30:181–191, DOI: 10.1002/sat.1012.

Jafarnia-Jahromi, A., Daneshmand, S., Broumandan, A., Nielsen, J., & Lachapelle, G. (2013, April). PVT solution authentication based on monitoring the clock state for a moving GNSS receiver. *Proceedings of the European Navigation Conference*, 23-25 April 2013, Vienna, Austria, 11 pages.

Pirsiavash, A., Broumandan, A., & Kennedy, S. (2024). Galileo Open Service Navigation Message Authentication (OSNMA) Benefits, Challenges, and Limitations," *Proceedings of the 37th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2024)*, Baltimore, Maryland, September 2024, pp. 3440-3454. https://doi.org/10.33012/2024.19744

Pirsiavash, A. (2019). Receiver-level signal and measurement quality monitoring for reliable GNSS-based navigation. PhD Thesis, Department of Geomatics Engineering , University of Calgary, Calgary, AB, Canada.

Pirsiavash, A., Broumandan, A., Lachapelle, G., & O'Keefe, K. (2017). Detection and classification of GNSS structural interference based on monitoring the quality of signals at the tracking level. *6th ESA International colloquium of Scientific and Fundamental Aspects of Galileo*, 25-27 Oct 2017, Valencia, Spain.

Pirsiavash, A., Broumandan, A., & Lachapelle, G. (2016). Two-dimensional signal quality monitoring for spoofing detection. *In Proceedings of the ESA/ESTEC NAVITEC 2016 Conference*, Noordwijk, The Netherlands, 12 pages.

Psiaki, M. L., & Humphreys, T. E. (2016). GNSS spoofing and detection. *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1258–1270.

Vagle, N., Broumandan, A., & Lachapelle, G. (2018). Multiantenna GNSS and inertial sensors/odometer coupling for robust vehicular navigation. *IEEE Internet of Things Journal*, vol. 5, issue 6, pp 4816-4828.

Wesson, K. D., Gross, J. N., Humphreys, T. E., & Evans, B. L. (2017). GNSS signal authentication via power and distortion monitoring. *IEEE Transactions on Aerospace and Electronic Systems*, 54(2), 739-754.