Hexagon | NovAtel's Jamming and Spoofing Detection and Classification Performance During the Norwegian JammerTest 2023

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 receivers' 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 at the University of Calgary in geomatics engineering, in 2000 and 2002 respectively. She has spent a fascinating 19 years in R&D at NovAtel and A&P, developing leading-edge positioning technology and working with a diverse, global customer base.

Abstract — Global Navigation Satellite Systems (GNSS) are widely used in critical infrastructure and safety-of-life applications. With such widespread use, open signal descriptions, and a crowded RF spectrum, jamming and spoofing are well-known threats to GNSS. Various detection and mitigation methods have been developed to deal with these threats. GNSS Resilience and Integrity Technology (GRIT) is a firmware suite developed for NovAtel's OEM7 receivers to expand situational awareness and interference detection and mitigation tools across applications and environments to protect against GNSS threats including jamming and spoofing attacks. GRIT includes the Interference Toolkit (ITK) and Spoofing Detection Toolkit (SK) to identify when a GNSS signal is under threat. GRIT relies on different countermeasures ranging from jamming detection and characterization to spoofing detection and mitigation to provide solution integrity and reliability. The Galileo Open Service Navigation Message Authentication (OSNMA) provides message authentication as an additional layer of GNSS protection.

JammerTest 2023 was conducted September 18-22, 2023 in Bliek, Norway. Various attacks were generated to interfere with and manipulate over-the-air signals to mislead the participant's equipment. This paper shows the jamming and spoofing detection performance of NovAtel's OEM7 receivers with actual data collected during the JammerTest 2023. Spectrum monitoring and jamming characterization on all GNSS bands supports jamming detection. The effectiveness of GRIT anti-jam and anti-spoofing technology is demonstrated using representative complex spoofing and jamming test cases during this event. OSNMA results for various scenarios are provided and discussed to demonstrate it as a complementary layer of protection to be accompanied by other security features and monitoring techniques for full protection.

1 INTRODUCTION

Civilian applications including vehicular navigation, electrical power grids and digital communication networks rely on GNSS-based position and timing services, and the consequences of disruption of these systems endanger safety-of-life and critical applications. GNSS signals are susceptible to jamming and spoofing attacks due to being weak near the Earth's surface. Since the civilian GNSS signal structure is known, the implementation of spoofing attacks is not complicated. In recent years, the implementation of software receiver-based spoofers has become feasible and affordable (Curran et al., 2018). Recent spoofing

activities reported in China and the Middle East provide actual evidence of position and time distortion in civilian applications (Divis, 2019; Sinister Spoofing in Shanghai, 2019).

Different types of spoofing attacks have been described in the literature. A repeater or meaconing attack is simple and effective. A repeater consists of a GNSS antenna to capture actual GNSS signals, an amplifier to boost the signal power and a transmitting antenna to propagate high-power signals to overpower the reception of authentic GNSS signals at the target receiver. The encrypted ranging code and navigation messages are not immune to this type of attack. In a signal simulator case, simulated signals are paired with an RF transmitter. The generated spoofing signals are not necessarily synchronized to the real GNSS signals. A more complicated type of spoofing attack consists of a GNSS receiver coupled with a spoofing transmitter. The receiver-based spoofer synchronizes itself with the current GNSS signals and extracts the time and navigation message, and then generates spoofing signals knowing the approximate position of its target receiver. This type of spoofer is relatively hard to detect since the spoofing signals are synchronized with the real GNSS satellites. A typical example of this attack is spoofing signals generated by software-defined radios such as HackRF (Curran et al., 2018). Several spoofing detection techniques have been proposed in the literature which use specific features of the counterfeit signals to distinguish them from authentic ones using a single antenna receiver (Bhatti & Humphreys, 2017; Pirsiavash et al., 2016; Psiaki & Humphreys, 2016). Multi-antenna spoofing detection has also been extensively investigated (Borio & Gioia, 2015; Vagle et al., 2018). The single antenna-based spoofing detection metrics are implemented in the pre-despreading or post-despreading layers of a GNSS receiver and are most effective when both spoofing and authentic signals are present. Pre-despreading signal monitoring metrics have been used to detect the presence of excessive amounts of power in GNSS bands (Jafarnia-Jahromi et al., 2014, 2012a, 2012b). These metrics rely on the assumption that spoofing signals are more powerful than the authentic ones. Post-despreading methods are used to detect abnormal behavior of GNSS signals, after removing the spreading code, caused by the presence of both spoofing and authentic signals (Broumandan & Curran 2017; Jafarnia-Jahromi et al., 2013; Nielsen et al., 2012; Pirsiavash 2019; Pirsiavash et al., 2017; Wesson et al., 2017).

In Broumandan et al., (2020) a wide range of spoofing attack scenarios and their features are described. Then various detectors addressing different spoofing scenarios are defined using metrics at different layers of a GNSS receiver with a single antenna input. The implemented detection unit was tested in different spoofing and non-spoofing scenarios to analyze the detection and false alarm probabilities. This paper extends the receiver based spoofing detection capability of Broumandan et al., (2020) to multi-frequency, multi-constellation. Cryptologic protection and GNSS security enhancement of the GNSS receivers is also discussed by presenting the research-version implementation of the newly developed Galileo E1B Open Service Navigation Message Authentication (OSNMA). The process is based on the Timed Efficient Stream Loss-tolerant Authentication (TESLA) protocol and an authentication key. The key is broadcast with delays as a part of a one-way chain whose root is public and renewed by a Merkle tree. The root key is authenticated by a symmetric private/public-key tactic named Elliptic Curve Digital Signature Algorithm (ECDSA), optimized by using the same key chain for all satellites, and auto and cross-authentication of data from different ones (Galileo OSNMA Receiver Guideline, 2022; Galileo OSNMA SIS ICD, 2022).

2 SPOOFING ATTACK TYPES

Figure 1 illustrates possible spoofing scenarios (Broumandan et al., 2020). Green and red triangles represent authentic and spoofing correlation peaks with relative power level. Figure 1a shows a jamming/spoofing attack. In this case, the spoofer tries to first jam and then spoof the target receiver, hence the spoofing power is much higher than the authentic one. This can be done by masking the authentic signals by increasing the input power and introducing the spoofing signals with reasonable C/N_0. This is a common and an effective spoofing attack and most of the spoofing events during JammerTest 2023 were high power spoofing attacks. However, due to high spoofing power, the detection of this type of attack is relatively easy. Monitoring the antenna input power can be used to detect this type of attack.

Figure 1b shows a matched power attack where the spoofing power is within a few dB of the authentic ones. This type of attack is usually used in synchronized spoofing cases where the spoofer has knowledge of the receiver position and actual GNSS signals. This attack does not significantly increase the noise level and as such power monitoring metrics cannot be used to detect the attack. During the JammerTest 2023 a few scenarios with matched power attack were introduced. Figure 1c shows a synchronized attack where the correlation function of authentic and spoofing signals overlaps. The spoofing power is within the authentic signals power range and hence the attack does not significantly increase the total input power. This type of attack causes distortion of the correlation peak and can be detected by monitoring the correlation function distortion. A meaconing attack can cause an overlapped spoofing scenario. Depending on the spoofing power, the correlation peaks may or may not be distorted. Meaconing attacks were introduced during the JammerTest 2023. Figure 1d shows a covered attack. In this case, the spoofer masks the reception of the authentic signals by covering the target receiver antenna and injecting the spoofing signals. Detection of this type of attack is very difficult for a single antenna receiver. This type of attack requires access to the target antenna. Regardless of the type of spoofing scenario described above, the spoofer can impact the position, navigation or timing (PNT) solutions of a receiver.

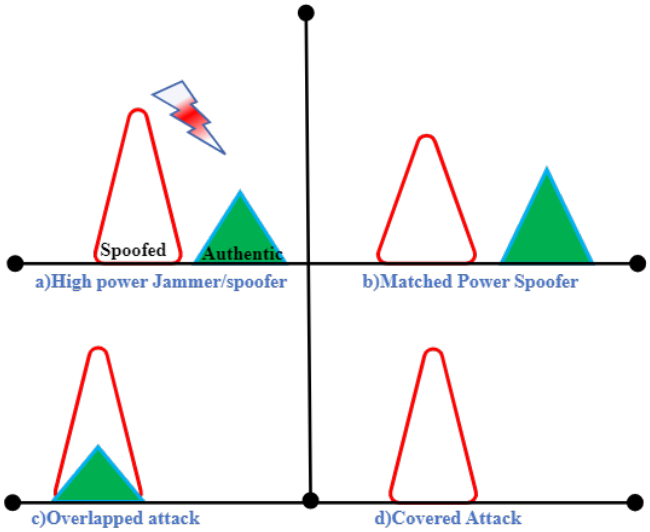

Figure 1 Different spoofing attack scenarios considering authentic-spoofing relative power and delay.

3 SPOOFING DETECTION

A real-time Spoofing Detection Toolkit (SK), employing a selection of the most effective detection metrics, was implemented onboard NovAtel's OEM7 generation of receivers. In the testing, the detection unit monitors GPS L1/L5, Galileo E1/E5a/E5b and BDS B1C/B2a observations. The detection rate used is 0.5 Hz. The detection metric outputs are fed to an onboard central spoofing detection unit, which provides a decision as to whether the receiver is under spoofing attack every 2 seconds. The main feature of the spoofing detection unit is to reduce the probability of false detection due to the presence of jamming and multipath signals while also detecting the spoofing attack with high confidence. The implemented spoofing detection should detect almost all spoofing scenarios in JammerTest 2023. More information regarding the performance of SK can be found in Broumandan et al., (2020).

4 OSNMA

OSNMA provides 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. Enabling OSNMA on the receiver necessitates the essential cryptographic functions to validate the received secret keys, retrieve the authentication codes, and verify the authenticity of the navigation data. The process is based on the 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, consisting of an 8-bit Header and Root Key (KROOT) or HKROOT, and a 32-bit Message Authentication Code (MAC) and Key or 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 Key Renewal (PKR) and Root Key (KROOT) information. MACK includes the TESLA chain key and the authentication tags used to verify the authenticity of the navigation data (Galileo OSNMA SIS ICD, 2022). **Figure 2** provides a high-level illustration of the general OSNMA operation, which can be considered as a state machine with three consecutive states (Galileo OSNMA Receiver Guideline, 2022).

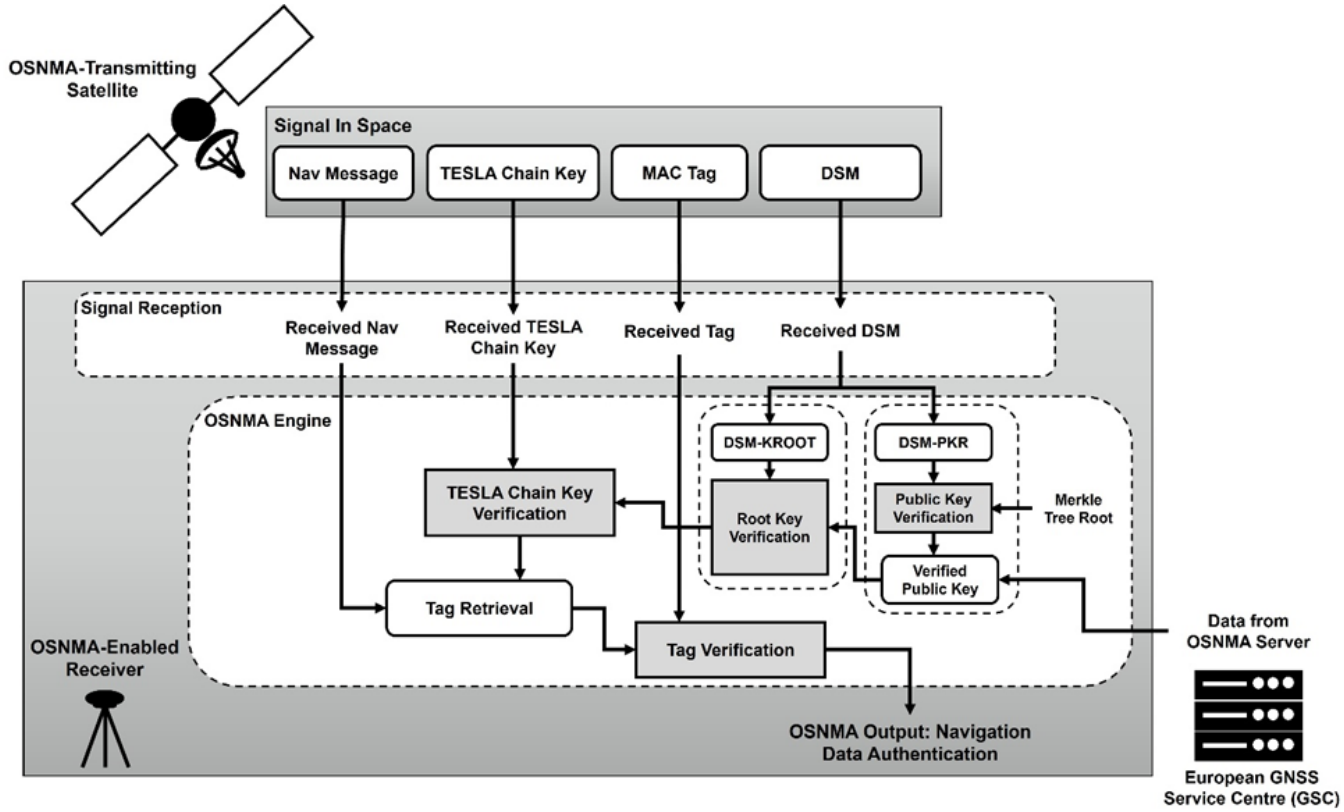

Figure 2 OSNMA process

The first state is initialization where the receiver is retrieving and verifying the public key 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, 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.

OSNMA protects navigation messages by making them unpredictable. It exploits a form of asymmetric cryptography based on the delayed sequence of lightweight symmetric keys; thus, it introduces a higher level of security, outperforming most of the solely symmetric solutions, and has a lower complexity than that of the purely asymmetric encryption systems. OSNMA is tenable for civil applications as it monitors the validity of the received chain keys using a publicly known key verification technique. It does not require costly hack-resistant hardware and infrastructure for secure allocation of the secret keys in the user terminal, making it affordable for public commercial and civil usage.

However, some consideration is required when using OSNMA for authenticity verification. The navigation message is a critical part of the PNT solution and once it is decoded and authenticated, it can be used for some hours. The verification of the navigation message, however, does not assure the authenticity of range or position, velocity and time (PVT) solutions. This may cause some confusion for a receiver that tries to identify if the signal under the test is reliable or not. For instance, consider a Galileo receiver operating in a dense urban canyon where the navigation data is corrupted by multipath fading. The OSNMA may not verify the authenticity of this signal, however, the receiver may be able to operate and provide a valid range in some intervals. If the receiver decides to not include this signal since the authenticity of it is not verified, it may suffer from signal availability and geometry impact on the navigation solution. Another example is meaconing and low latency spoofing attacks where authentic signals are re-broadcasted to create an intended position/time offset. In such a case, a stand-alone OSNMA module would validate the navigation data while the PVT solution is spoofed. OSNMA can only validate the authenticity of the navigation message with latency. Also, for receivers connected to a network and operating in challenging GNSS environments, decoding navigation data from live data may not be plausible due to a high bit error rate and longer time to fix. For such applications, an assisted GNSS approach by accessing navigation data via other sources may be more sensible.

5 JAMMERTEST 2023

In September 2023, the Norwegian Public Roads Administration in conjunction with the Norwegian Communications Authority, Norwegian Metrology Service and the Norwegian Space Agency hosted JammerTest 2023 located at Bleik in Andøya. Live over-the-air broadcast jamming and spoofing tests were conducted over five days. During JammerTest, OEM7 receiver cards inside PwrPak7 enclosures and a GNSS-850 geodetic grade antenna were evaluated. A wide variety of jamming and spoofing attacks were generated, including single-band, dual-band, multi-band, high power, directional, omni-directional, in-car, handheld, static and kinematic tests. Figure 3 shows NovAtel's test vehicle with the GNSS-850 antenna. The PwrPak7 receiver with GNSS-850 antenna was used for spectrum monitoring and situational awareness including jamming and spoofing detection. NovAtel's Interference Toolkit (ITK) and Spoofing Detection Toolkit (SK) logs were collected to analyze data sets in real-time and in post-processing. ITK logs were used to detect jamming signals and characterize their parameters including power, bandwidth, and their temporal and spectral behaviors. SK logs were used to detect spoofing attacks and to distinguish spoofing events from jamming attacks.

The PwrPak7 was configured for multi-frequency and multi-constellation operation. During the test the receiver tracked GPS L1/L2/L5, Galileo E1/E5/E5a/E5b/E6, BeiDou B1/B1C/B2/B2a/B2b/B3 and GLONASS L1/L2/L3 signals. The position estimation results are based on all available measurements. In the following sections, the test outcomes and receiver behavior are presented under jamming and spoofing events. Results are reported for days 2-5 as there was no spoofing test during the first day. Average C/N_0 values as a signal quality monitoring metric are demonstrated. The receiver position and timing errors under spoofing attack are shown. The receiver input power monitoring reported by ITK logs and real-time spoofing detection results using SK logs will be demonstrated. Finally, navigation message authenticity for Galileo E1 signals is evaluated using onboard OSNMA implementation. Please note that the results provided in this paper are based on the observation capabilities of the OEM7 receiver under the jamming/spoofing attacks. There may be details of the attack scenarios that were not observable by the OEM7 receiver.

Figure 3 NovAtel's test vehicle with GNSS-850 antenna on the roof

5.1 Day 2 (Tuesday, September 19):

On day 2 the transmission plan included a high-power ramp jamming test in the morning and meaconing in the afternoon. Here, the results of the meaconing attack in the afternoon are provided. These tests include stationary meaconing with varying power and time exposure. The scenarios are described as GNSS retransmission of real live sky signals, where the GNSS environment will have the wrong position with real satellite data, only slightly time delayed. The spoofed position is located at 69.2803484 N, 16.0074695 E.

Figure 4 shows a) average C/N_0 values (average of all tracked PRNs at a given epoch) of GPS L1CA and Galileo E1, b) position error, c) in-band power measured by ITK, d) spoofing detection bit measured by SK and e) Galileo E1 OSNMA detection results per pseudo-random noise (PRN). The yellow and red shaded areas in the plots refer to the jamming and spoofing scenarios 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. 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 the navigation message is corrupted and cannot be corrected due to propagation environment or interference, or an unauthorized signal, with either 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. Three different meaconing scenarios were identified during day 2 and are labeled by (1), (2), and (3) in Figure 4..

Scenario 1 started with a high-power jammer at all three GNSS bands. This is shown with the yellow area in Figure 4 when the receiver was overwhelmed and could not track any signals at the L1 band. This is observable by comparing the results of Figure 4a and Figure 4c under the jamming event.

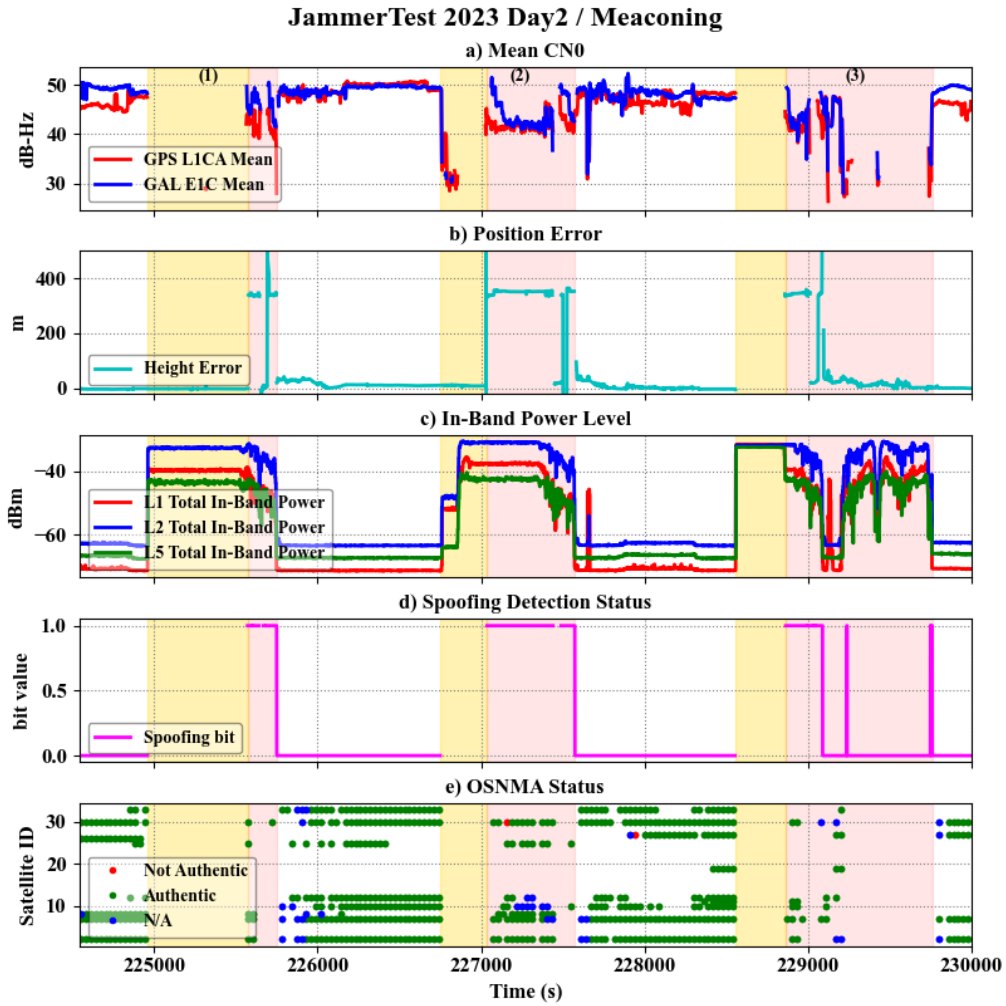

Figure 4 Monitoring, detection, and positioning results – day 2

After the jamming event, the meaconing attack was initiated, and the receiver started tracking replayed GNSS signals. As shown in Figure 4c the meaconing power gradually decreased at all bands. The receiver height jumped by about 350 m. The SK spoofing detection module detected this attack as soon as there were enough tracking channels to provide position solutions (Figure 4d). As shown in Figure 4e, for a few epochs, the receiver could track four Galileo E1 signals. Since in a meaconing attack the navigation data is entirely replicated from an authentic source, the navigation message was reported authentic by the OSNMA module.

Scenario 2 initiated with different jamming power characteristics as shown in Figure 4c on L1, L2 and L5 bands. As soon as the receiver started tracking spoofed signals, the reported position jumped, and the spoofing attack was immediately detected by SK. Figure 4e shows the OSNMA results for this scenario. The receiver tracked seven Galileo E1 signals where navigation messages were reported authentic, except for the epochs where spoofing interference interrupted the reception of OSNMA-required data (blue) or caused bit errors in the navigation data and thus raised the red flag.

Scenario 3 started with high-power jamming at all three GNSS bands that lasted about 5 minutes followed by a spoofing attack. As shown in Figure 4c, the spoofing power was changed during this scenario. During this test, the receiver position initially was spoofed and the jump in the position solution correlates with the spoofing detection results. However, after about 5 min from the start of the spoofing scenario, the spoofing power decreased and the receiver started tracking authentic signals. After about 10 min, the spoofing power increased, however, the receiver held on to the authentic signals at the L5 band. As such, it did not track any spoofing signals at L1 and L2 bands. Hence, during this period the receiver did not track spoofing signals and the spoofing detection correctly did not detect any attack. The receiver did not track any Galileo E1 signals and hence there are no OSNMA results for this test.

5.2 Day 3 (Wednesday, September 20):

On day 3 a stationary spoofing attack generated a static false position or false route. The spoofed route followed a path around Bleik. Simulated signals were transmitted from the Bleik community house. This spoofing scenario included incoherent spoofing from stationary spoofer using synthetic ephemerides. Incoherent spoofing is defined as reception of transmitted simulated GNSS signals that are not code-phase aligned with live sky signals. Simulated signals were transmitted from a stationary antenna near the Bleik community house. Generated spoofing scenarios used satellite ephemerides different from live sky satellites. Simulated signals used one or more constellations and one or more signal bands. Figure 5 shows different metrics and detection results from day 3. Five different scenarios (4-8) are identified.

Scenario 4 started with a high-power spoofing attack. The high-power spoofer increased the input power by about 30 dB at all GNSS bands. The average C/N_0 as shown in Figure 5a was increased by about 8 dB. In this scenario, there was no spoofing attack on the L5 band. The SK spoofing detection module immediately detected this attack as soon as the receiver tracked GNSS signals. The receiver position was also distorted but not spoofed (Figure 5b). In this scenario, the OSNMA data field was filled by an artificial pattern of repeated "0" and "1" bits, therefore the TESLA chain keys were not verified and consequently, the OSNMA classified this attack as not authentic (Figure 5e). As expected, under the nominal operation of OSNMA, there is a lag of two subframes (or 60 s) in navigation message authentication as the receiver needs to wait for the authentication key embedded in the upcoming subframe to authenticate navigation data from the preceding epoch (Galileo OSNMA SIS ICD, 2022), which should be fine in most positioning applications given the validity of navigation messages over time. At the end of Scenario 4, OSNMA restarted authenticating the navigation message (as shown by blue dots) and the SK-based spoofing detection flag was set to 0 indicating the spoofing was not present anymore.

Scenarios 5 and 6 were very similar and all GNSS bands were spoofed. Both SK and OSNMA detected these events as shown in Figure d) and e). The receiver PVT solutions were spoofed in these scenarios.

Scenario 7 initiated with a high-power jamming attack that lasted for about 5 min. The spoofing attack on all bands then started. The SK and OSNMA results are shown in Figure 5d and Figure 5e. The user position was spoofed in this scenario.

Scenario 8 initiated with a moderate-power spoofing attack as shown in Figure 5c. The spoofer could successfully spoof GPS L1 and Galileo E1 signals as indicated by the average C/N_0 results since it increased by about 8 dB. However, some of the signals, such as BDS B2A, were not spoofed. Hence, the receiver integrity monitoring did not report any position solution for the most part in this scenario.

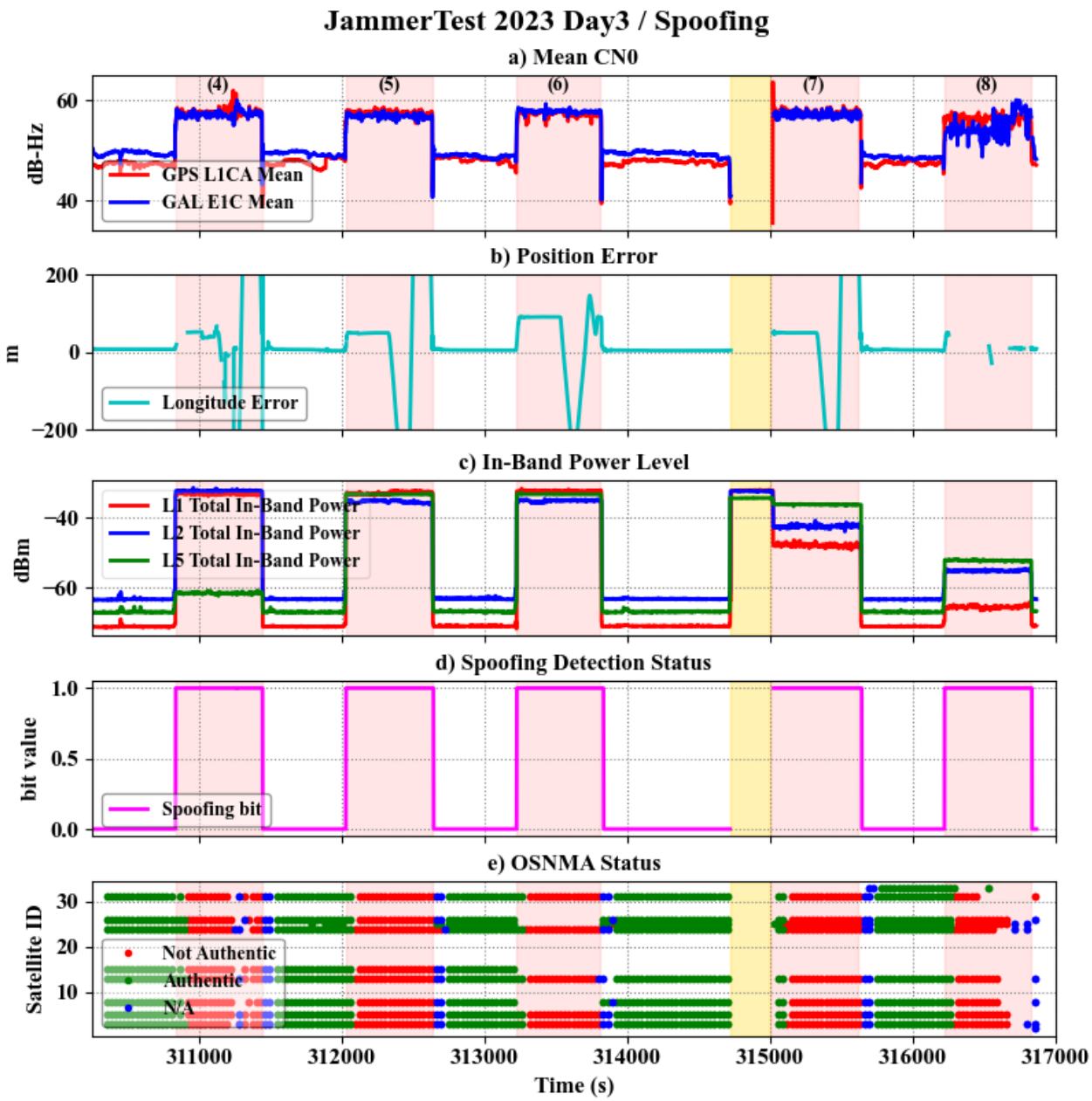

Figure 5 Monitoring, detection and positioning results – day 3

5.3 Day 4 (Thursday, September 21):

In the morning of day 4, tests consisted of two different types of time spoofing scenarios. Simulated signals were transmitted from a stationary antenna near the Bleik community house. The first scenario consisted of incoherent time spoofing from a stationary spoofer using synthetic ephemerides. Generated spoofing scenarios used satellite ephemerides different from live sky satellites. The second one consisted of coherent time spoofing from a stationary spoofer using broadcast (true) ephemerides. For all tests, simulated signals used one or more constellations and one or more signal bands. Scenarios 9-13 shown in Figure 6 provide results in the morning and Scenarios 14-17 shown in Figure 7 presents results of the spoofing scenario during the afternoon.

Scenario 9 demonstrated a non-coherent spoofing attack. The spoofing power gradually increased in 5 dB steps. Initially, the lower power spoofer acts as a jammer and consequently reduces the average C/N_0 to the point that the receiver was forced to re-acquire the signals and at that point, the receiver started tracking the spoofed signals. The receiver position solution in this case is not affected by the spoofer (Figure 6b). The SK spoofing detection module detected the presence of spoofing for various spoofing

powers as long as there were enough tracked signals. For the majority of this scenario, the receiver did not track any Galileo E1 signals resulting in no OSNMA outputs.

Scenario 10 started with a matched-power spoofing attack (about 2 dB increased input power). This scenario did not impact the tracking signals and hence position and timing solutions. The SK spoofing detection module detected the low-power spoofing attack in this phase of the test as shown in Figure 6d. In the second phase of Scenario 10, the spoofer power was increased as shown in the C/N_0 and input power results, and the time solution was impacted. The SK spoofing detection module detected this high-power spoofing attack. During this phase, the receiver lost track of Galileo signals except for PRN 24 where the OSNMA identified the synthetic ephemerides by reporting the inauthenticity of the navigation message.

Scenario 11 started with a high-power jammer followed by high-power spoofing. Only GPS L1CA was spoofed and hence the receiver could not track any Galileo signals for OSNMA validation, except for PRN 33 where synthetic ephemerides were detected. The spoofing attack was detected by the receiver.

Scenario 12 demonstrated a matched-power spoofing attack. As shown in Figure 6c, the input power was changed and hence the methods based on monitoring the input power could not be used to detect this type of attack. As shown, the spoofing attack was detected by the receiver-based SK spoofing detection module. This scenario was a coherent time spoofing where the spoofer used broadcast (true) ephemerides, so as expected, the OSNMA unit confirmed the authenticity of the navigation message and could not detect the attack.

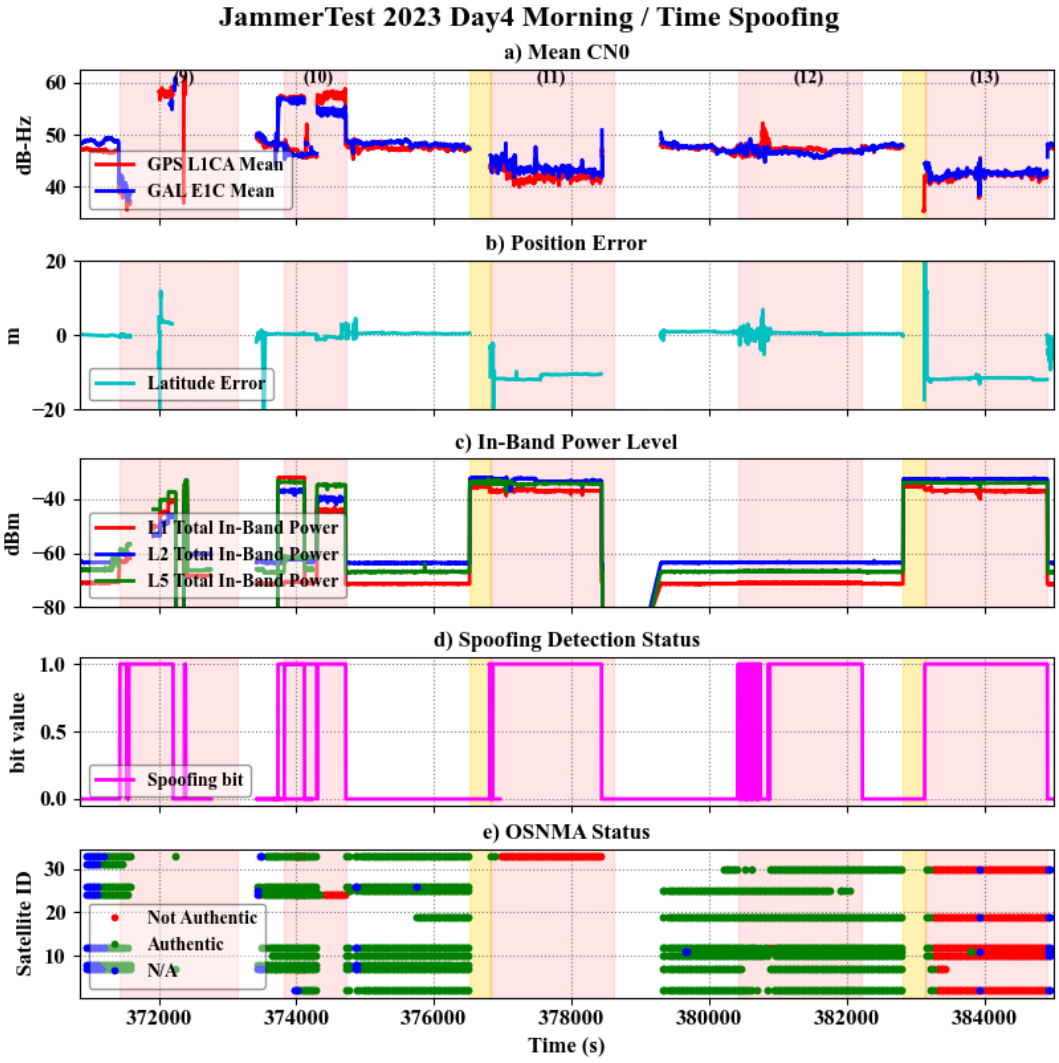

Figure 6 Monitoring, detection and positioning results – day 4 morning

Scenario 13 started with a high-power jammer followed by a high-power spoofing attack. The SK spoofing detection module detected the attack and the OSNMA module flagged not-authentic since the OSNMA data bits were filled by the artificial pattern of repeated "01"s and thus the TESLA keys were not verified.
On the afternoon of day 4, the motorcade spoofing activity occurred. These tests consisted of small jammers and simple low-power spoofers onboard a moving vehicle that the user vehicle followed. The results for this test are shown in Figure 7. Four spoofing scenarios were identified in this test.
Scenario 14 started with an L1band spoofing attack as shown in Figure 7. Initially, the receiver tracked the spoofing signal, but the receiver integrity monitoring rejected these measurements. After several minutes the receiver started tracking the spoofed signals at GPS L1 and Galileo E1 as shown in Figure 7a. SK detected the attack as soon as the receiver started tracking the spoofed signals. OSNMA did not report any case of navigation message inauthenticity since the scenario consisted of broadcast (true) ephemerides. During this test, the receiver position was not spoofed since spoofer was only applied on the L1 band.

Scenario 15 was similar to that of **Scenario 14** and the receiver briefly tracked the spoofing signals at the L1 band. The spoofing attack was detected as soon as these signals were tracked.

Scenario 16 initiated with a spoofing attack and the receiver tracked signals at the L1 band as shown in Figure 7. The SK spoofing detection module detected this attack. As expected, the OSNMA unit authenticated the broadcast (true) ephemerides used in this scenario, except for the blue-colored epochs where the reception of OSNMA-required data was interrupted by the spoofer.

Scenario 17 initiated with high-power jammer at the L1 signal only where the receiver did not track any spoofed signal hence there was no spoofing observed from the onboard SK spoofing detection module or OSNMA.

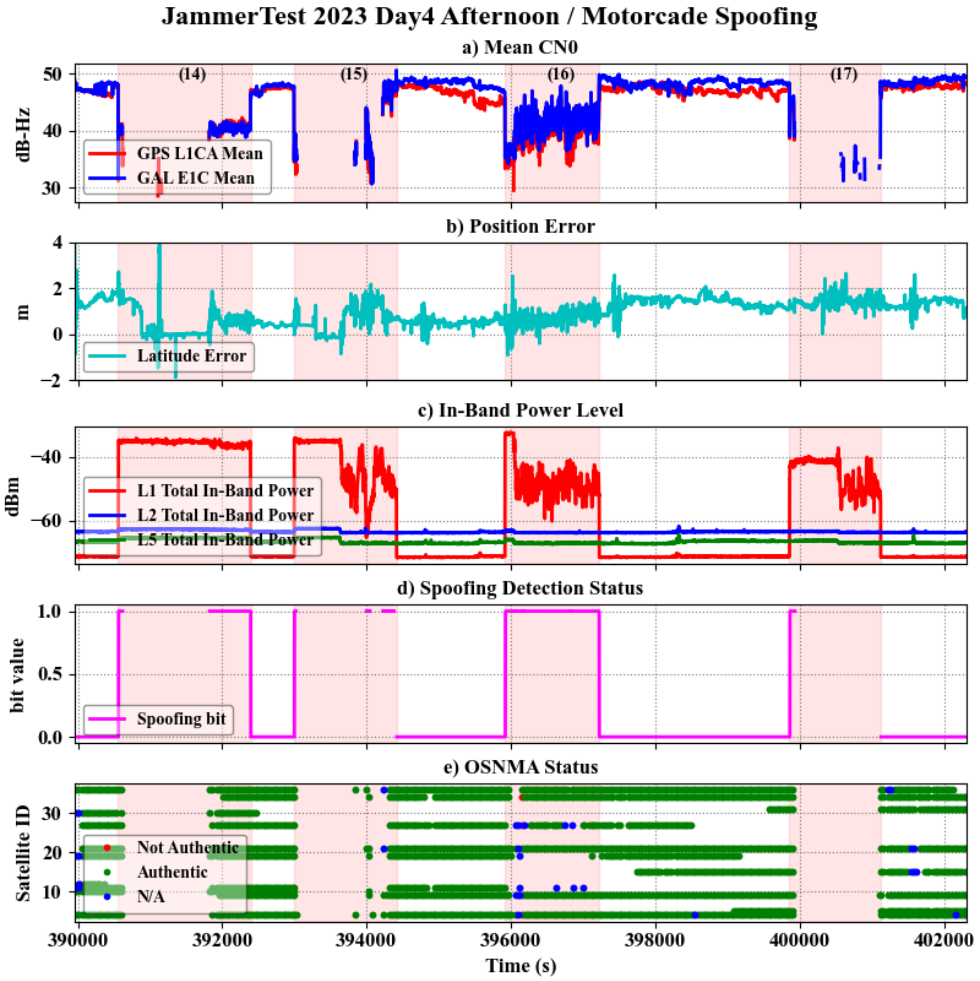

Figure 7 Monitoring, detection and positioning results – day 4 afternoon

5.4 Day 5 (Friday, September 22):

This session included a series of diverse tests: high-power jamming, stationary meaconing, spoofing and some low-power commercially available jammers such as handheld, USB and cigarette lighter jammers. Both coherent and incoherent spoofing scenarios using broadcast (true) ephemeris were included as well as some scenarios with incoherent time spoofing from a stationary spoofer using synthetic ephemerides.

Scenario 18 started with a high-power jammer followed by a meaconing attack. The receiver tracked spoofed GPS and Galileo signals at the L1 band, impacting the position estimate of the receiver, but the attack was detected successfully by the onboard SK unit. The OSNMA unit verified the authenticity of the navigation data during the meaconing attack as expected. This excludes the epochs where spoofing interference interrupted the reception of OSNMA-required data or caused bit errors in the navigation data.

Scenario 19 started with a high-power spoofer. OSNMA and the receiver-based SK spoofing detection module both detected this attack. The receiver position was affected as shown in **Figure 7**b. The OSNMA module reported not-authentic as the OSNMA data was filled by the repeated pattern of "01"s for all Galileo PRNs.

Scenario 20 started with a spoofer at the L1 band and hence the receiver did not track any signal at L1. Since there was not any tracked signal at L1 and were authentic signals at other bands, SK detected this scenario as authentic. OSNMA was not available during this test since the receiver did not track any Galileo E1 signals.

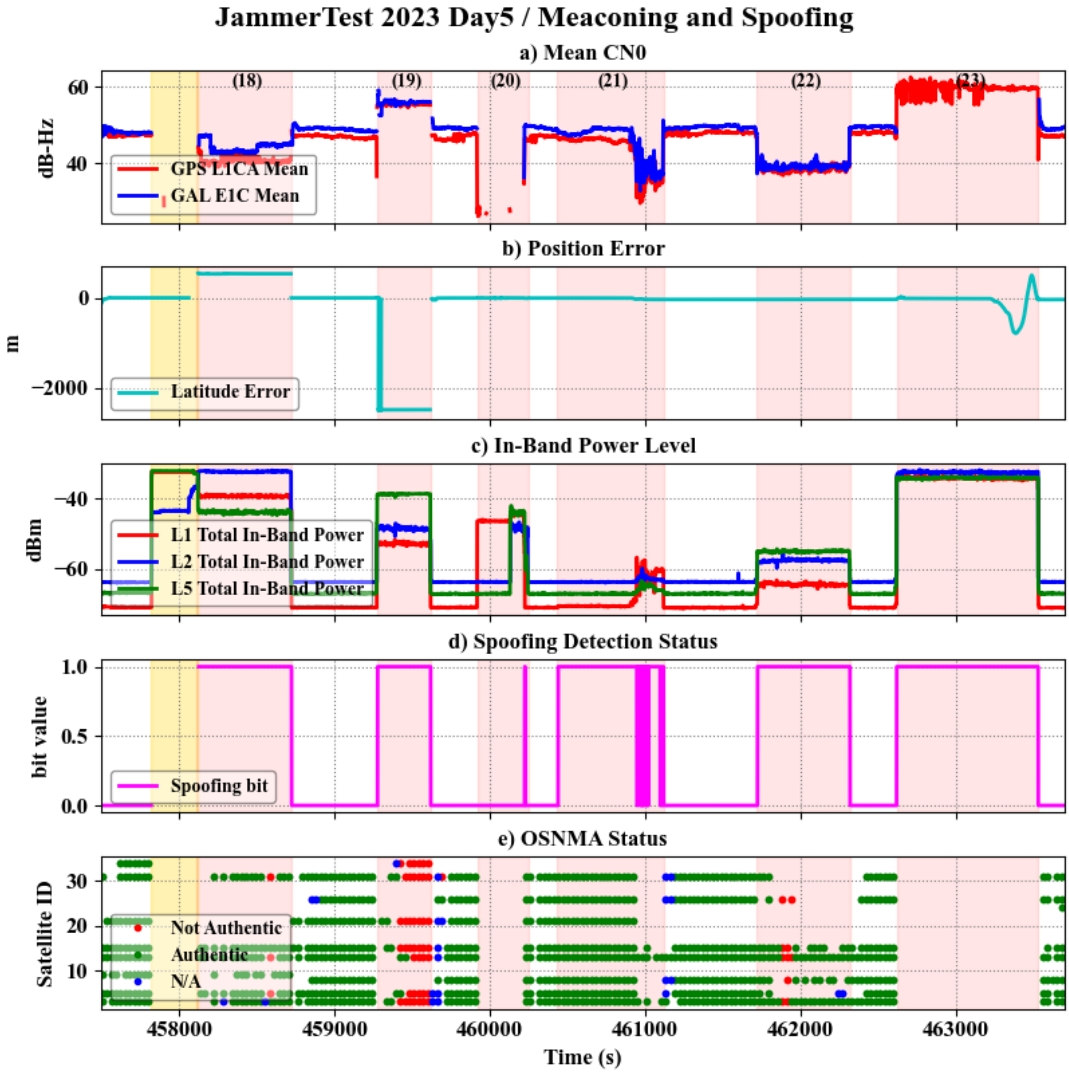

Figure 8 Monitoring, detection, and positioning results – day 5

Scenario 21 started with a matched-power spoofing attack as the input power at L1 slightly increased. The spoofing was detected by the receiver-based SK spoofing detection module.

Scenario 22 started with spoofing signals at all bands. This included incoherent time spoofing from a stationary spoofer using synthetic ephemerides which was detected by the onboard SK spoofing detection module. This was a time spoofing and hence no impact on the position solution weas observed. In both spoofing Scenarios 21 and 22, authentic Galileo signals were tracked by the receiver where the authenticity of Galileo E1 navigation messages were verified by the OSNMA unit.

Scenario 23 initiated with a high-power jammer and spoofer at all three bands as shown in Figure 8. The receiver position was impacted as shown in Figure 8b. The receiver only tracks GPS L1 signals in this case, hence there were no outcomes from OSNMA unit. The spoofing attack was successfully detected by SK.

Table 1 summarizes the spoofing detection and OSNMA verification results. In all the detection scenarios, SK detected the attack immediately (within 2 s) whereas it took about 60 s for OSNMA to report a decision.

Table 1 Different attack and test scenarios

Scenario	Spoofing Scenario	PNT Spoofed	OEM7 Spoofing Detection	OSNMA[1]
1	10 W Meaconing	Yes	Detected	Authenticated
2		Yes	Detected	Authenticated[2]
3		Yes	Detected	Authenticated[2]
4	Coherent stationary spoofer using broadcast (true) ephemerides, with artificial OSNMA data field[3]	Yes	Detected	Not Authenticated
5		Yes	Detected	Not Authenticated
6		Yes	Detected	Not Authenticated
7		Yes	Detected	Not Authenticated
8		Yes	Detected	Not Authenticated
9	Incoherent time stationary spoofer using synthetic ephemerides	Yes	Detected	N/A
10		Yes	Detected	Not Authenticated
11		Yes	Detected	Not Authenticated
12	Coherent time spoofing from stationary spoofer using broadcast (true) ephemerides	Yes	Detected	Authenticated
13	Coherent time spoofing from stationary spoofer using broadcast (true) ephemerides, with artificial OSNMA data field[3]	Yes	Detected	Not Authenticated
14	Motorcade coherent spoofing from stationary spoofer using broadcast (true) ephemerides	No	Detected	Authenticated
15		No	Detected	Authenticated
16		No	Detected	Authenticated[2]
17		No	N/A	N/A
18	Meaconing	Yes	Detected	Authenticated[2]
19	Incoherent spoofing from stationary spoofer using broadcast (true) ephemerides, with artificial OSNMA data field[3]	Yes	Detected	Not Authenticated
20	Incoherent time spoofing from stationary spoofer using synthetic ephemerides	No	N/A	N/A
21	Similar to 20, low power	No	Detected	Authenticated
22	Similar to 20	No	Detected	Authenticated
23	Similar to 4-7	Yes	Detected	N/A

Comments:

1. Wherever the receiver could track Galileo E1 signals
2. Except for the epochs where spoofing interference interrupts the reception of OSNMA-required data or caused bit errors in the navigation data
3. Filled by a pattern of repeated “0” and “1”s for OSNMA data-bits

6 SUMMARY AND CONCLUSIONS

During the Norwegian JammerTest 2023, NovAtel's GRIT features were used to reliably detect and monitor interference and spoofing attacks. GRIT included interference monitoring and characterization (i.e., ITK), and receiver-based spoofing detection (i.e., SK) modules. Galileo navigation message authentication using OSNMA implementation was also tested. Live over-the-air broadcast jamming and spoofing tests were conducted over five days. During JammerTest, an OEM7 receiver card inside a PwrPak7 enclosure paired with a GNSS-850 geodetic grade antenna was evaluated. A wide variety of jammer and spoofing attacks were tested, including single-band, dual-band, multi-band, high-power, directional, omni-directional, in-car, handheld, static and kinematic tests. Comprehensive spoofing attacks at single and multiple bands were generated. The spoofing attacks included meaconing, matched-power and high-power scenarios. Actual and synthesized navigation messages were generated which enabled verification of the OSNMA. During these tests, spoofing affected the position and timing solutions of the receiver.

These tests revealed very accurate spoofing detection results using SK in real-world, over-the-air conditions that compared well with previous testing performed in controlled laboratory conditions. The onboard spoofing detection unit (SK) detected all the spoofing scenarios including meaconing, matched-power and high-power spoofing attacks at single and multiple bands. The OSNMA module successfully detected scenarios where the OSNMA data field was manipulated, or the navigation message was synthesized. As expected, OSNMA authenticated the navigation message of meaconing attacks. SK detected all the spoofing attacks almost immediately, whereas in the nominal operation of OSNMA, the receiver needed to wait for a cryptographic key embedded in the upcoming subframe(s) which takes about 60 s in its nominal OSNMA operation. It was observed that intermittent jamming events disrupted the navigation message decoding process and hence impacted the OSNMA process in not authenticating the non-spoofed Galileo signals. The implemented receiver-based spoofing detection is a multi-constellation and multi-frequency detector that checks the authenticity of each signal at each band. OSNMA authenticates the navigation message on Galileo E1 and if this signal is not available, the authenticity of the rest of Galileo signals cannot be verified. For receivers that were designed without security in mind, the OSNMA scheme provides a means of authentication and spoofing awareness with increased signal complexity on E1B. For NovAtel's OEM7, a multi-layered spoofing detection approach has been implemented, which is specifically supported by receiver design choices. OSNMA can become another layer in that multi-layered approach; however, as shown in the JammerTest 2023 results, the OEM7 specific methods offer faster detection of spoofing under more types of attacks.

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., & 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/

Divis, D. A. (2019). New report details GNSS spoofing including denial-of-service attacks. *Inside GNSS,* https://insidegnss.com/new-report-details-gnss-spoofing-including-denial-of-service-attacks/

Galileo Open Service Navigation Message Authentication (OSNMA) Receiver Guideline. (Dec. 2022). issue 1.0, 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.

Nielsen, J., Dehghanian, V., & Lachapelle, G. (2012). Effectiveness of GNSS spoofing countermeasure based on receiver CNR measurements. *International Journal of Navigation and Observations*, vol. 2012, Article ID 501679, 9 pages, 2012. doi:10.1155/2012/501679.

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.

Sinister Spoofing in Shanghai. (Dec. 2019). *Inside GNSS*, https://insidegnss.com/sinister-spoofing-in-shanghai/

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.