engineering proceedings

MDPI

Proceeding Paper

Performance Characterization of Hexagon | NovAtel's Robust Dual-Antenna Receiver (RoDAR) during the Norwegian Jamming Trial 2022 †

Ali Broumandan * and Sandy Kennedy

Hexagon | NovAtel, Calgary, AB T3K 2L5, Canada; sandy.kennedy@hexagon.com
* Correspondence: ali.broumandan@hexagon.com
† Presented at the European Navigation Conference 2023, Noordwijk, The Netherlands, 31 May–2 June 2023.

Abstract: NovAtel has recently leveraged its expertise in both receiver design and anti-jam technology to develop solutions for space- and weight-constrained applications in challenged GNSS environments. Robust Dual-Antenna Receiver (RoDAR), is based on a commercial dual-antenna receiver, originally designed for attitude determination, and employs special firmware to mitigate jammers and spoofers without an increase in size or power consumption. With RoDAR, the multi-frequency, multi-constellation dual-antenna receiver is capable of null-steering at two different frequency bands (e.g., L1 and L5). In September 2022, the Norwegian Public Roads Administration hosted JammerTest, a live, over-the-air broadcast jamming and spoofing test. This paper presents the jamming and spoofing detection and mitigation performance of RoDAR during this live broadcast test. The interference detection provides spectrum monitoring and jamming characterization on all GNSS bands. The mitigation is carried out by steering a null formed on-board the receiver towards a jamming/spoofing source at GPS L1 and L5 bands. The null steering performance is characterized as a function of signal and position availability compared to a non-protected NovAtel receiver. The effectiveness of the anti-jam and anti-spoofing technology is demonstrated using representative complex spoofing and jamming test cases during this event.

Keywords: detection; GNSS; high precision; jamming; null steering; mitigation; spoofing

Citation: Broumandan, A.; Kennedy, S. Performance Characterization of Hexagon | NovAtel's Robust Dual-Antenna Receiver (RoDAR) during the Norwegian Jamming Trial 2022. *Eng. Proc.* **2023**, *54*, 28. https://doi.org/10.3390/ENC2023-15470

Academic Editors: Tom Willems and Okko Bleeker

Published: 29 October 2023

1. Introduction

Global Navigation Satellite Systems 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. The most common type of intentional interference is jamming, which aims to prevent GNSS receivers from providing position and timing solutions. Interference can be suppressed in the time, frequency and/or spatial domains. Although methods for suppressing narrowband interference in the time/frequency domain have been widely studied [1,2], their performance degrades when presented with wideband interference. Spatial processing techniques can effectively mitigate both narrowband and wideband interference [3], for example, antenna array processing [4–10].

Spoofing is another form of intentional interference. Several spoofing detection methods have been proposed in the literature to distinguish counterfeit signals from authentic ones using both single-antenna and multi-antenna receivers [11]. In a single-antenna GNSS receiver, spoofing detection metrics are implemented in pre-despreading or post-despreading layers and are most effective when both spoofing and authentic signals are present. Pre-despreading and intermediate frequency signal monitoring metrics have been used to detect the presence of excessive amounts of power in GNSS bands [12]. Multi-antenna receivers can employ spatial processing techniques to defeat interfering signals regardless of their temporal or spectral characteristics, and are equally effective on narrow

and wideband interferers including spoofed signals. Spatial processing is one of the most powerful countermeasures against various types of jamming and spoofing signals, but it typically comes with the burden of additional cost and power consumption.

NovAtel's GNSS Resilience and Integrity Technology (GRIT) is within the firmware of all OEM7 receivers for situational awareness and interference detection and mitigation tools. GRIT includes NovAtel's Interference Toolkit (ITK) and spoofing detection toolkit (SK) [12] to identify when a GNSS signal is under threat. For the dual-antenna variants of the OEM7 family, NovAtel's Robust Dual-Antenna Receiver (RoDAR) firmware option mitigates jammers and spoofers without an increase in size or power consumption. With RoDAR, the multi-frequency, multi-constellation dual-antenna receiver is capable of null-steering at two different frequency bands (e.g., L1 and L5). When not actively null-steering, RoDAR firmware also supports high-precision modes such as RTK, PPP and dual-antenna heading estimation.

2. GRIT

NovAtel's GRIT includes the toolkits discussed below.

Interference Toolkit (ITK): identifies when interference is present and characterizes the detected jammer in time and frequency domains. Mitigation options include implementing notch filters at detected frequencies, and High Dynamic Range (HDR) mode for wideband interference effect [13].

Spoofing Detection: further evaluates the incoming signals at different layers of GNSS receiver including IF sample, tracking and position level to characterize the radio frequency (RF) environment to identify when positioning, navigation and timing (PNT) is at risk from counterfeit signals [12].

RoDAR: offers an active anti-jamming tool that uses spatial processing to protect against all interference types, including the mitigation of wideband interference and spoofing signals. The operation of RoDAR is shown in Figure 1. The RF signals from two antennas are passed to the null-steering weight calculation unit after down conversion and digitization. Then, the second antenna signal undergoes phase rotation and gains compensation based on the calculated array weights and is removed from the first antenna signal. The resultant samples are jammer and spoofer free. The cleaned signals are then passed on to the tracking and position, velocity and time (PVT) solution module. RoDAR offers up to 30 dB of nominal protection compared to a non-protected receiver, and is classified as a commercial good for export control purposes.

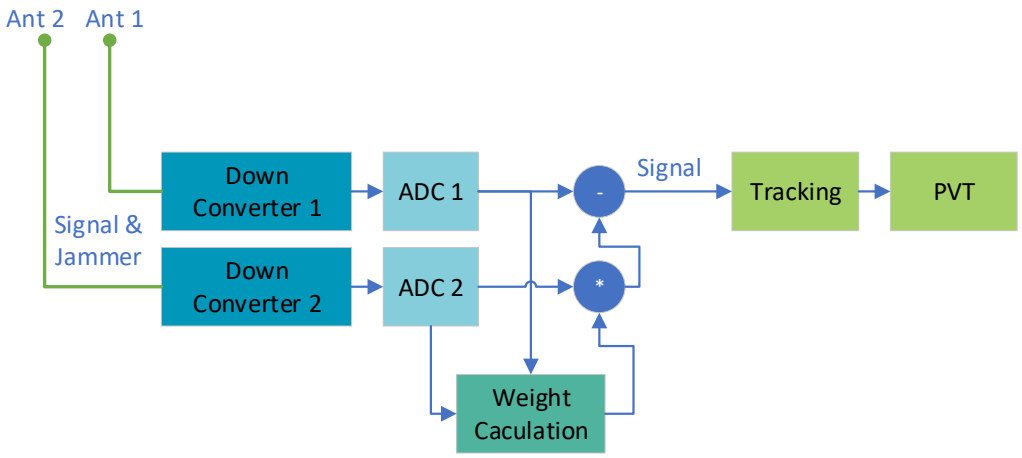

Figure 1. RoDAR operation.

OEM7′s multi-constellation and multi-frequency support protects with diversity, and then if the situation turns very hostile, RoDAR provides active anti-jamming on two GNSS bands.

3. GRIT at Work: Norwegian Jamming and Spoofing Trial 2022

In September 2022, the Norwegian Public Roads Administration in conjunction with the Norwegian Communications Authority, Norwegian Metrology Service and the Norwegian Space Agency hosted JammerTest 2022, located at Bleik in Andøya. Live over-the-air broadcast jamming and spoofing tests were conducted over five days. This event provided a unique opportunity for international companies from varying sectors to step away from the safety of their simulators and controlled environments and test their ware's resiliency in real-world, hostile GNSS scenarios.

During JammerTest, dual-antenna and single-antenna OEM7 cards were evaluated, with different antennas representing different design priorities. A wide variety of jammers were tested, including single-band, dual-band, multi-band, high-power, directional, omni-directional, in-car, handheld, Norwegian Defense-owned, static and kinematic tests. RoDAR on OEM718D receiver cards, coupled to antennas from Hexagon | Antcom, were mounted to a test vehicle for the stationary jammer test series, along with PwrPak7 enclosed receiver and GNSS-850 geodetic grade antenna for reference [14].

Figure 2 shows NovAtel's test vehicle with the 1.2 G antennas from Antcom used as RoDAR arrays and the GNSS-850 antenna. The 1.2 G is a triple frequency GNSS antenna covering upper and lower bands including BDS B1, GPS L1 and GLO L1, and GPS L2, GPS L5/GalE5a and GalE5b bands. RoDAR on 718D protects the GPS L1CA and GPS L5 encoders and all other signals sharing those encoders. For instance, null steering at GPS L1CA band protects GalE1 and BDS B1C.

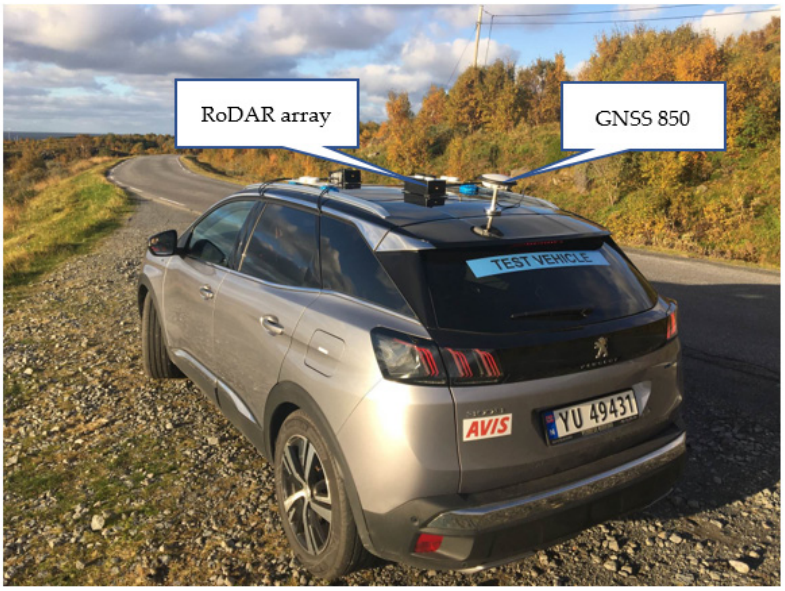

Figure 2. NovAtel's test vehicle with 4 RoDAR array and one GNSS-850 antenna on the roof.

The PwrPak7 receiver with GNSS-850 antenna was used for spectrum monitoring and situational awareness, while the RoDAR receivers were used for jamming and spoofing detection and mitigation. NovAtel's ITK (Interference Toolkit) and spoofing detection 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. Spoofing detection logs were used to detect spoofing attacks and to distinguish spoofing events from jamming attacks.

The first three days of testing featured jamming attacks. Spoofing and jamming scenarios were propagated during the fourth day.

3.1. Jamming Test and Results

Different jamming types including single- and multi-band jamming scenarios were generated during this event. The single-band or multiple-band attacks with a mid-power jammer did not affect the position solution of the non-protected PwrPak7 or RoDAR. This is because OEM7 cards tracks all observable GNSS signals, providing resiliency against jamming and spoofing attacks via frequency diversity. Single-point positioning at the meter level of accuracy was of interest in these tests, rather than high-precision positioning at the centimeter level.

Next, the multi-frequency, high-power jamming attack is examined. Figure 3 shows the total in-band power as a function of time at L1, L2 and L5 during this jamming event, as measured by the OEM7 receiver itself [15]. The jammer power was gradually increased and then decreased in a ramping power test on all GNSS bands. As shown, in case of L1, the noise level is at −70 dBm when no jamming is present.

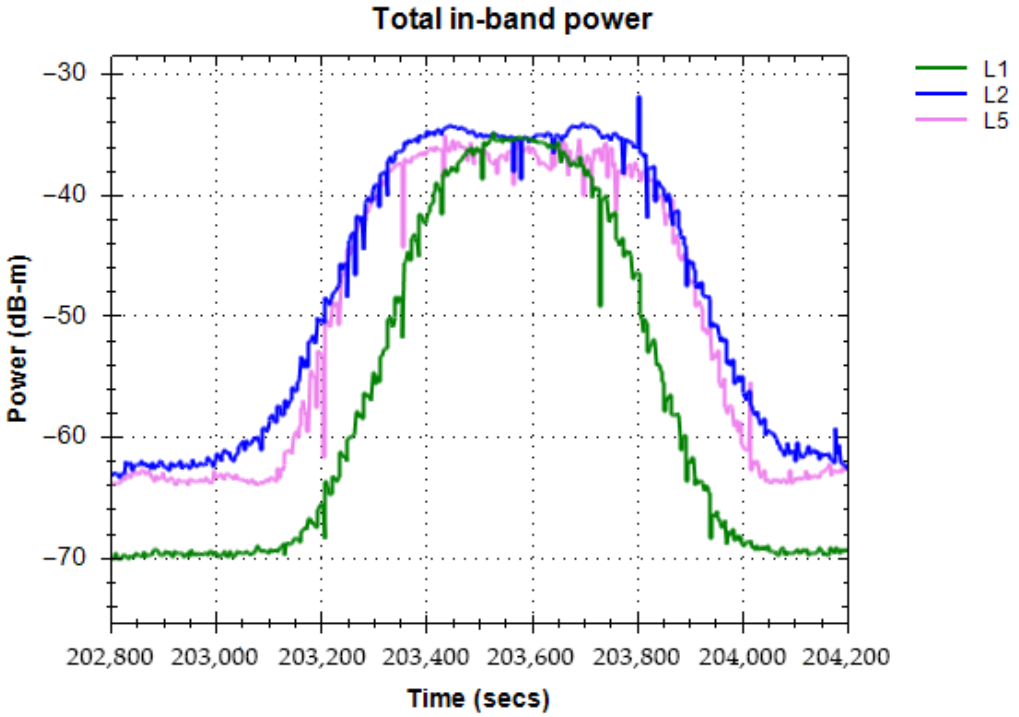

Figure 3. Input power measured by ITK during the ramp power jammer at L1, L2 and L5 bands.

Figure 4 shows mean CN0 values of GPS L1CA and L5 for the PwrPak7 and RoDAR units. GPS L1CA and L5 are protected by RoDAR with active null forming. The initial average CN0 of PwrPak7 is higher than RoDAR, because the GNSS-850 antenna paired with the PwrPak7 has a higher gain than the 1.2 G antenna used with the RoDAR unit. By introducing the jammer, the PwrPak7 CN0 values fell about 20 dB, and eventually, the receiver dropped the signals, while RoDAR maintained continuous tracking.

Figure 5 shows the reported position accuracy of RoDAR compared to the unprotected PwrPak7 under the high-power jammer. The single-point position standard deviation demonstrates the receiver's confidence in the solution. As shown, the PwrPak7 position solution degraded badly when the extra in-band power exceeded 15 dB. The RoDAR unit continued to provide a reliable position solution.

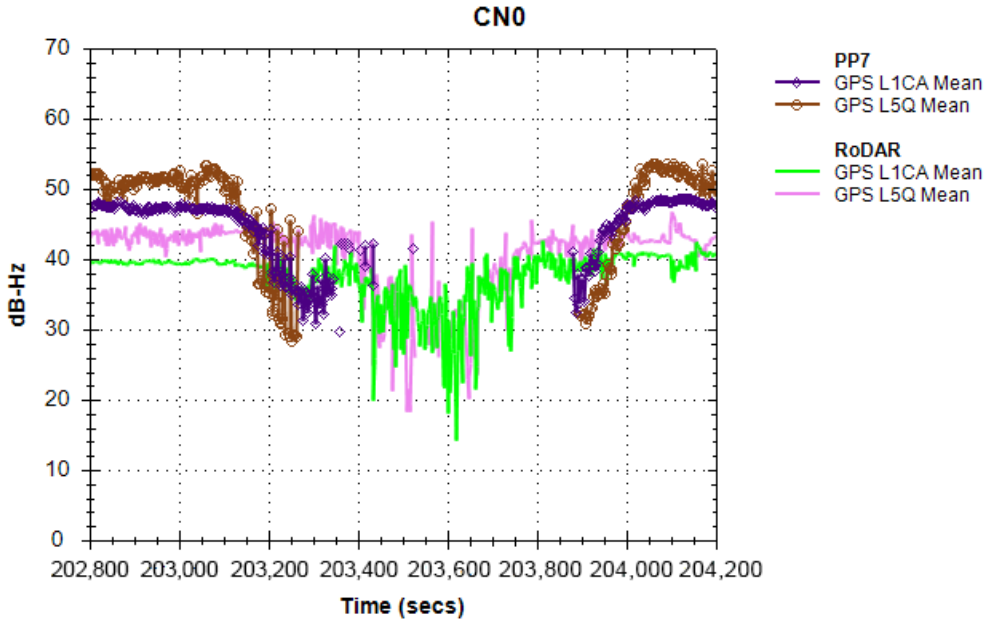

Figure 4. Average CN0 variation during the ramp power jamming for GPS L1 and L5.

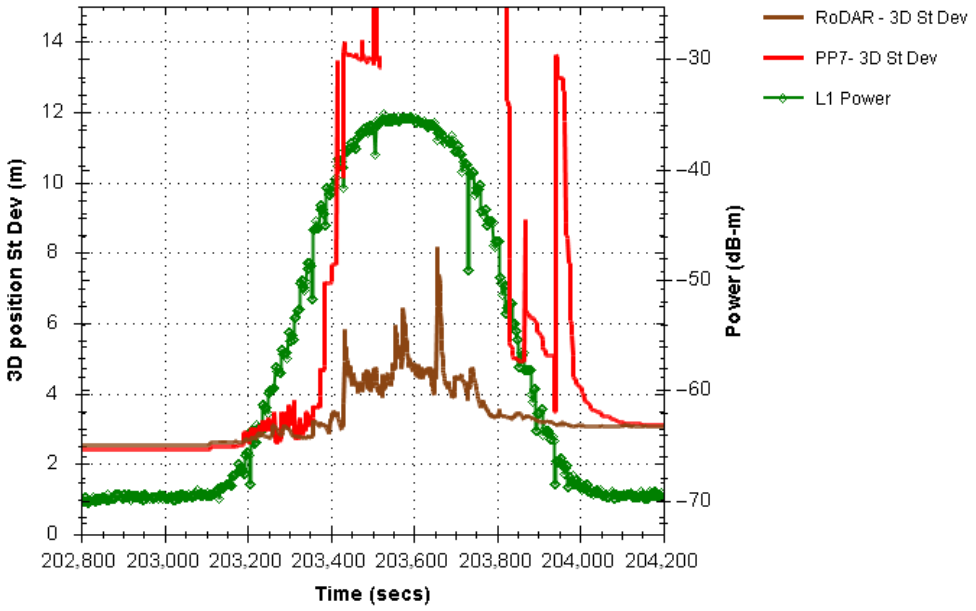

Figure 5. L1 Total in-band power, 3D position standard deviation for RoDAR and PwrPak7.

3.2. Spoofing Attack

The spoofing mitigation performance of RoDAR is evaluated and compared to the unprotected PwrPak7 receiver in this section. Each spoofing attack began with a period of high-power jamming at all GNSS bands followed by a spoofing transmission on GPS L1CA while jamming continued all other bands.

ITK logs enable visualization of jamming and spoofing attacks in the frequency and time domains. Figure 6 shows the Power Spectral Density (PSD) of all GNSS bands in clean, no-jamming conditions. This can be used to compare the jamming and spoofing power level and shape of the spectrum during the attacks.

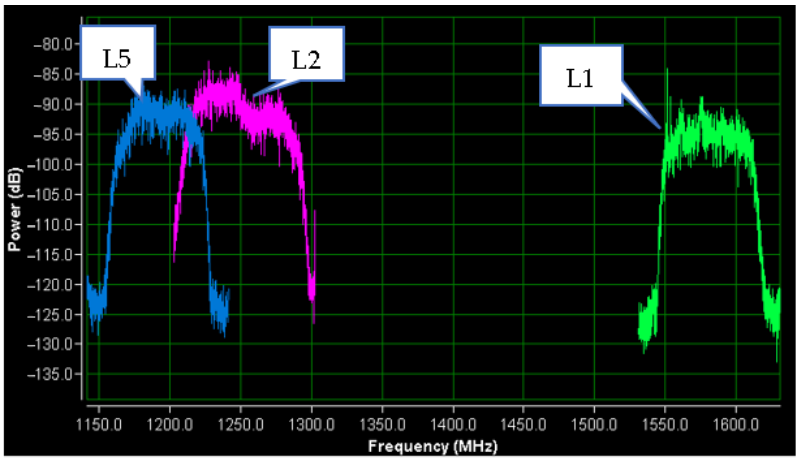

Figure 6. Spectrum of GNSS bands (L1, L2, L5) under clean, open-sky condition.

Figure 7 shows the PSD of L1 band (GPS L1, BDS B1, GLO L1) during the high-power jamming that began the attack. As shown, the input power is significantly increased compared to the plots in Figure 6 due to the jamming effect. A 20 MHz wideband jammer at the centre of GPS L1 (1575 MHz) is observable. BeiDou B1I at 1561 MHz and GLONASS L1 located at 1602–1615 MHz were also jammed.

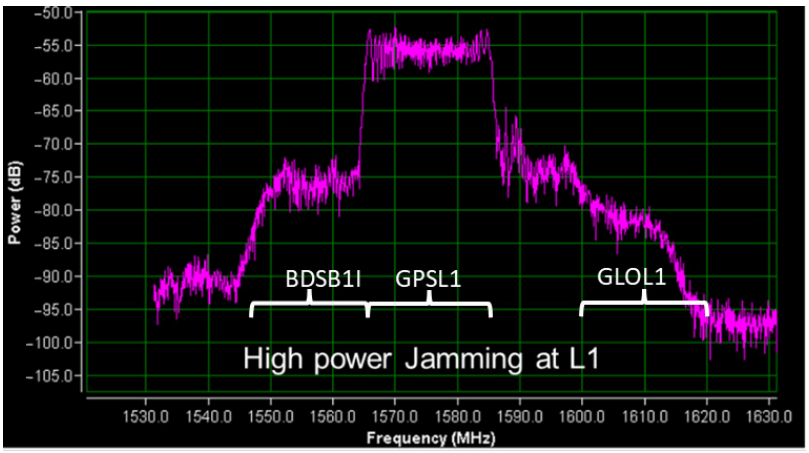

Figure 7. Spectrum of GNSS L1 band under high power jamming attack.

Figure 8 shows the PSD as the attack transitioned to spoofing. Comparing the PSD plots of Figures 7 and 8 reveals useful information. After the initial jamming period, the 20 MHz wideband jammer was moved to the GLO L1 band. The power of this jammer was also reduced. BDS B1I had a similar input power level compared to the benign condition (comparing Figures 6 and 8). This indicates this signal was not spoofed. GPS L1 input power was slightly increased. The spoofing detection toolkit detected a matched-power spoofing attack (where the spoofing power is marginally higher than the authentic signals) in this case.

Figure 9 shows the GPS L1 input power (blue) during the spoofing episodes. The scenario started with a clean, benign environment followed by knockout jamming (PSD was shown in Figure 7) at all GNSS bands and then a spoofing scenario (PSD was shown in Figure 8). The average CN0 values for GPS L1CA for RoDAR and PwrPak7 are also shown in Figure 9. The mean CN0 values in the benign stage were 43 and 48 dB-Hz for RoDAR and PwrPak7, respectively. The difference in CN0 values is due to higher grade antenna used for PwrPak7. During the jamming event, both receivers were overwhelmed and could not track anything.

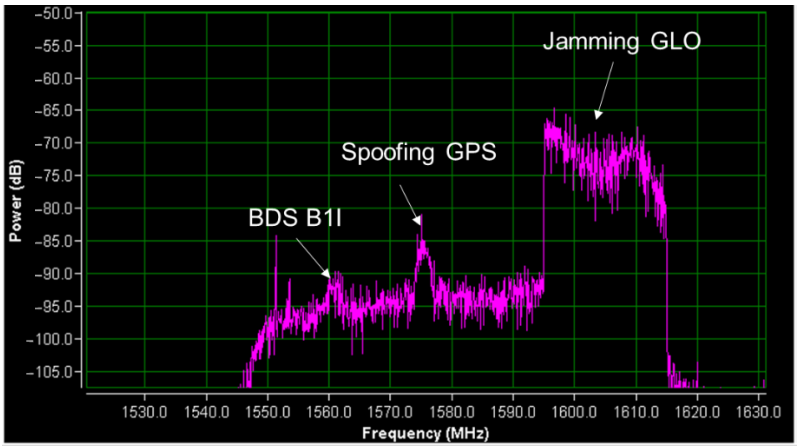

Figure 8. Spectrum of GNSS L1 band under jamming attack and spoofing attack.

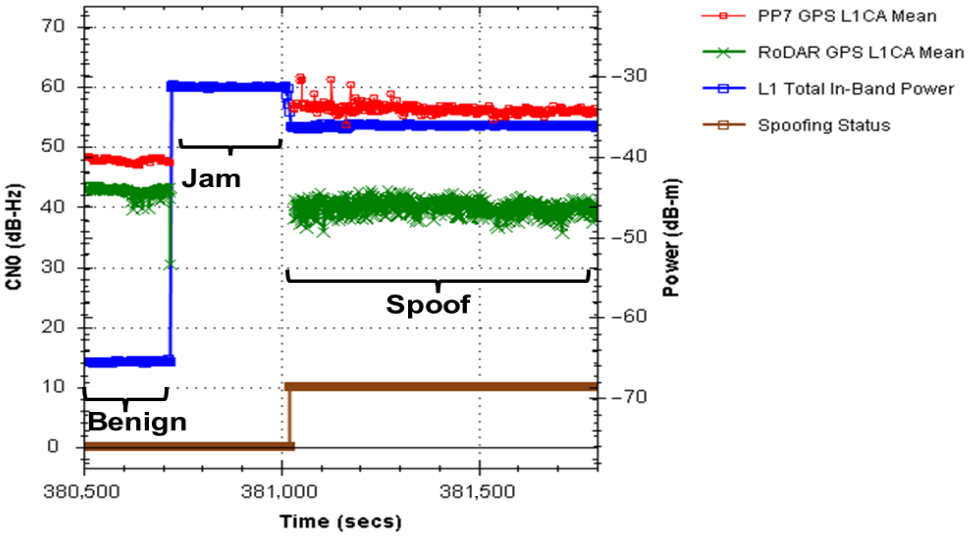

Figure 9. GPS L1 input power, mean CN0 for GPS L1CA for RoDAR and PwrPak7 units.

During the spoofing attack, the PwrPak7 mean CN0 jumped from 48 to 56 dB-Hz (red curve) due to tracking the strong spoofed signals, while RoDAR tracked authentic signals, which its lower CN0 reflects. The on-board spoofing detection status from the PwrPak7 is also shown in this figure.

Figure 10 shows all L1 band signals tracked by PwrPak7 during the spoofing attack. During the spoofing stage, PwrPak7 could only track GPS L1CA and BDS B1I. GLO L1 was jammed, GPS L1 was spoofed, and authentic BDS B1I slipped through because it was not jammed nor spoofed. The CN0 values of GPS L1CA were increased (spoofed), whereas the CN0 values of BDS B1I were reduced (no spoofed signal, higher noise floor from in-band jammer).

Figure 11 shows CN0 of L1 signals tracked during the spoofing stage by the RoDAR unit. RoDAR tracked authentic GPS L1CA, GalE1 and BDS B1I.

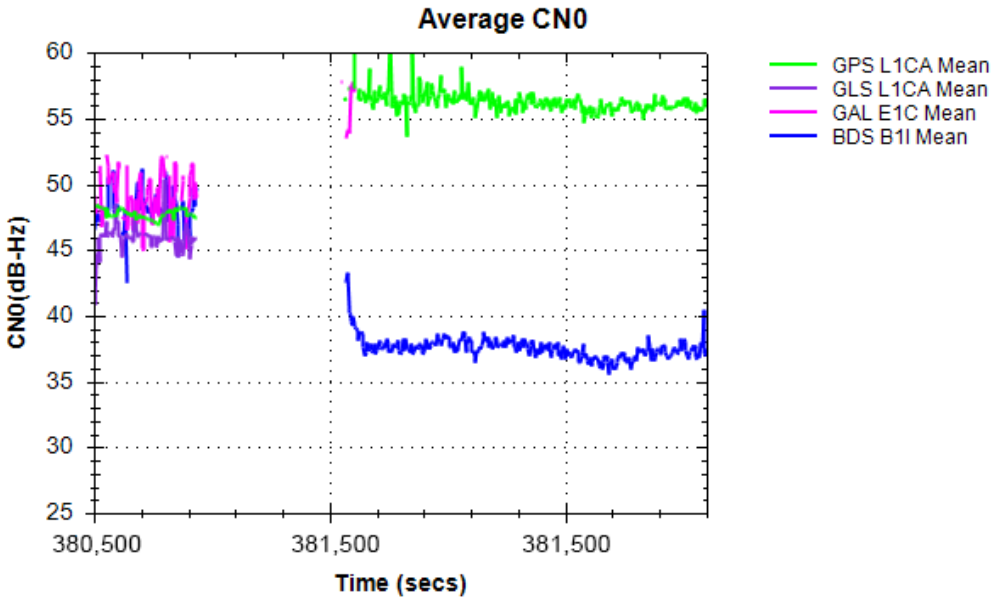

Figure 10. Average CN0 of signals at L1 band tracked by PwrPak7.

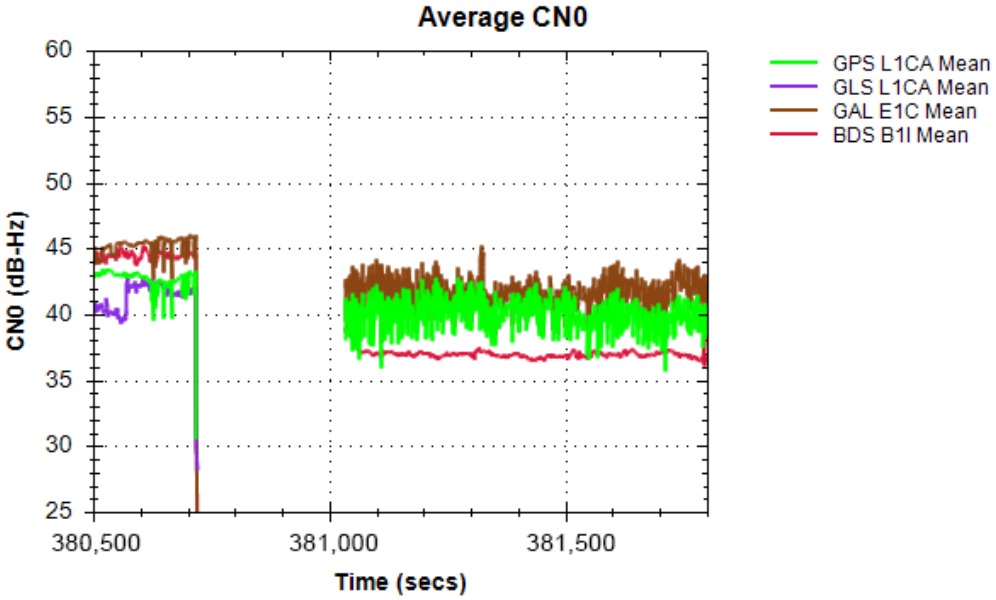

Figure 11. Average CN0 of signals at L1 band tracked by RoDAR.

4. Summary and Conclusions

During the Norwegian jamming and spoofing trials, NovAtel's GRIT features were used to reliably detect, monitor and mitigate interference and spoofing signals. These tests revealed very accurate spoofing detection results in real-world, over-the-air conditions that compared well with previous testing performed in controlled laboratory conditions. RoDAR provides dual-band spatial null-steering protection and multi-antenna, multi-constellation support. The experimental results in this trial demonstrated RoDAR's interference mitigation capabilities compared to the single-antenna PwrPak7 receiver under jamming and spoofing attacks. In the case of jamming, RoDAR was able to withstand 15–25 dB more jamming power than the single-antenna receiver in terms of position availability and accuracy. During the spoofing attack, the RoDAR unit successfully mitigated the spoofing signals, whereas the non-protected receiver tracked the spoofing signals. However, the non-protected receiver did correctly detect and report the spoofing. Neither RoDAR nor the PwrPak7 receivers provided a spoofed position during the spoofing trial.

For RoDAR, this resiliency was due to using null steering to suppress the spoofing attack. The PwrPak7's resiliency was due to signal diversity (multi-constellation support) and internal integrity checks.

Author Contributions: A.B. processed the data sets; A.B. and S.K. both contributed to the writing of the manuscript. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: Authors Ali Broumandan and Sandy Kennedy were employed by Hexagon | NovAtel.

References

1. Pickholtz, R.L.; Schilling, D.L.; Milstein, L.B. Theory of spread-spectrum communications-a tutorial. *IEEE Trans. Commun.* **1982**, *30*, 855–884. [CrossRef]
2. Chang, C.L.; Juang, J.C. Performance analysis of narrowband interference mitigation and near-far resistance scheme for GNSS receivers. *Signal Process. Elseveir* **2010**, *90*, 2676–2685. [CrossRef]
3. Van Trees, H.L. *Optimum Array Processing, Detection, Estimation, and Modulation Theory, Part IV*; Wiley-Interscience: New York, NY, USA, 2002.
4. Fante, R.L.; Vaccaro, J.J. Cancellation of jammers and jammer multipath in a GPS receiver. *IEEE Aerosp. Electron. Syst. Mag.* **1998**, *13*, 25–28. [CrossRef]
5. Fante, R.L.; Vaccaro, J.J. Wideband cancellation of interference in a GPS receive array. *IEEE Trans. Aerosp. Electron. Syst.* **2000**, *36*, 549–564. [CrossRef]
6. Amin, M.G.; Sun, W. A novel interference suppression scheme for global navigation satellite systems using antenna array. *IEEE J. Sel. Areas Commun.* **2005**, *23*, 999–1012. [CrossRef]
7. Sun, W.; Amin, M.G. A self-coherence anti-jamming GPS receiver. *IEEE Trans. Signal Process.* **2005**, *53*, 3910–3915. [CrossRef]
8. Zoltowski, M.D.; Gecan, A.S. Advanced adaptive null steering concepts for GPS. In Proceedings of the Military Communications Conference, MILCOM 95, IEEE, San Diego, CA, USA, 5–8 November 1995; pp. 1214–1218.
9. Brown, A.; Gerein, N. Test results of a digital beamforming GPS receiver in a jamming environment. In Proceedings of the ION GPS 2001, Salt Lake City, UT, USA, 11–14 September 2001; pp. 894–903.
10. Seco-Granados, G.; Fernández-Rubio, J.A.; Fernández-Prades, C. ML estimator and hybrid beamformer for multipath and interference mitigation in GNSS receivers. *IEEE Trans. Signal Process.* **2005**, *53*, 1194–1208. [CrossRef]
11. Borio, D.; Gioia, C. A Dual-antenna Spoofing Detection System Using GNSS Commercial Receivers. In Proceedings of the 28th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2015), Tampa, FL, USA, 14–18 September 2015.
12. Broumandan, A.; Kennedy, S.; Schleppe, J. Demonstration of a Multi-Layer Spoofing Detection Implemented in a High Precision GNSS Receiver. In Proceedings of the 2020 IEEE/ION Position, Location and Navigation Symposium (PLANS), Portland, OR, USA, 20–23 April 2020. [CrossRef]
13. Gao, F.; Kennedy, S. Demonstrated Interference Detection and Mitigation with a Multi-frequency High Precision Receiver. In Proceedings of the 29th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2016), Portland, OR, USA, 12–16 September 2016; pp. 159–170.
14. Available online: https://novatel.com/products/receivers/enclosures (accessed on 27 November 2023).
15. Alves, P.; Himmelfarb, M. Interference Mapping Using Receiver Power. In Proceedings of the 31st International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2018), Miami, FL, USA, 24–28 September 2018.