engineering proceedings

MDPI

Proceeding Paper

Jammertest 2022: Jamming and Spoofing Lessons Learned †

Aiden Morrison [1,*], Nadezda Sokolova [1], Anders Solberg [2], Nicolai Gerrard [3], Anders Rødningsby [4], Harald Hauglin [5], Thomas Rødningen [5] and Tor Dahlø [2]

[1] SINTEF, 7034 Trondheim, Norway; nadia.sokolova@sintef.no
[2] The Norwegian Mapping Authority, 3511 Hønefoss, Norway; anders.martin.solberg@kartverket.no (A.S.); tor-ole.dahlo@kartverket.no (T.D.)
[3] Norwegian Communications Authority, 4790 Lillesand, Norway; nicolai.gerrard@nkom.no
[4] Norwegian Defense Research Establishment, 2007 Kjeller, Norway; anders.rodningsby@ffi.no
[5] Norwegian Metrology Service, 7075 Tiller, Norway; hha@justervesenet.no (H.H.); thr@justervesenet.no (T.R.)
* Correspondence: aiden.morrison@sintef.no
† Presented at the European Navigation Conference 2023, Noordwijk, The Netherlands, 31 May–2 June 2023.

Abstract: Jammertest 2022 was a week-long series of satellite navigation and timing signal jamming and spoofing exercises carried out on the Norwegian island of Andøya in September of 2022. Organized via a collaboration between the Norwegian spectrum management authority, defense research establishment, public roads administration, metrology service, and others, the result was the largest known GNSS jamming and spoofing event open to international collaboration and provided an open-access data and publication policy for participants. This paper reviews the event's organization, scheduled tests, noteworthy jamming observations, noteworthy spoofing observations, and the unexpected observations found during the event and also presents information on what data are publicly available to interested parties, along with the contact information needed to obtain these data.

Keywords: GNSS; jamming; spoofing; RFI; PPD

Citation: Morrison, A.; Sokolova, N.; Solberg, A.; Gerrard, N.; Rødningsby, A.; Hauglin, H.; Rødningen, T.; Dahlø, T. Jammertest 2022: Jamming and Spoofing Lessons Learned. *Eng. Proc.* **2023**, *54*, 22. https://doi.org/10.3390/ENC2023-15445

Academic Editors: Tom Willems and Okko Bleeker

Published: 29 October 2023

1. Introduction—What Was Jammertest?

Jammertest 2022 was an event held from the 19th through to the 23 September 2022 on the island of Andøya on the Norwegian coast, and was an exceptional opportunity for the international navigation community due to each of the locations selected, the data access policies enacted by the organizers, and the selection of the tests conducted.

The location, adjacent to the community of Bleik, was ideal for carrying out jamming and spoofing tests for a number of reasons. The first and primary beneficial feature was the high ridgeline which surrounded the test location on three sides. With peaks exceeding 400 m above sea mean sea level and lying close to the transmission site, this ridge line not only protected the mainland from the emitted signals but also prevented the signal from propagating into much of the airspace surrounding the island. Signals could only freely propagate within the test area and to the northeast out to the northern Atlantic.

The Jammertest data access policies were also ideal in that attendees were allowed to freely discuss and publish their observations and results. Typically, jamming and spoofing exercises, along with the data collected through these exercises, are considered to be sensitive, possibly due to the perceived potential for misuse. Given that both jamming and spoofing are widely discussed in publicly accessible papers in both technical and general media publications, the decision was made that the utility of allowing relevant industrial, governmental, research, and academic institutions to freely discuss the observed phenomena outweighed remaining concerns around publication. The specific tests carried out at Jammertest were numerous and are detailed in Section 3.

2. Test Site, Setup, and Selection

Jammertest made use of several locations on the island of Andøya for different purposes, including the hosting of the participants, static emission sites, static reception sites, dynamic testing areas, and ad hoc evaluation points (all shown in Figure 1). The map in Figure 1 is labeled with five zones that were used for different purposes during the week.

Figure 1. Modified map showing test and lodging locations with numbered locations one through five as described below. Original map from norgeskart.no, accessed on 1 April 2023.

Location 1 at the northernmost extent of the island was the local host community where the majority of test participants were housed.

Location 2 to the North of the community of Bleik and adjacent to the local cemetery was used as an equipment deployment and emissions site for the high-power jamming sources, as well as for the testing of helicopter navigation systems.

Location 3 at the Bleik community center was the primary meeting base camp, setup and equipment preparation point, and deployment area for static receiver testing. It was also used as the first low-power Personal Privacy Device (PPD) test area. A collection of PPDs used by the Norwegian Communication Authority (Nkom) during the test activities is shown in Figure 2.

Figure 2. Twenty-one assorted jamming devices of various designs used throughout the PPD tests.

Location 4 at Bauktuva was a roadside parking area on a low hilltop used for making safe turns for single vehicles and platoons of vehicles (participating in tests).

Location 5 at Grunnvatnet was protected from emissions by the high-power jamming sources by local topography and was used as a second low-power/PPD test area.

The testing carried out during the event was designed to expose participants to as many forms of signal interference as possible and in as many ways as possible to help evaluate navigation system behavior in conditions of interest to as many different user segments as practical. Since the most common form of jamming most navigation users will encounter is emitted either unintentionally or from PPDs, it was natural to include both an array of PPDs as well as custom-generated signals. Since many sources of unintentional Radio Frequency Interference (RFI) are narrowband in nature [1], it was decided that several of the sub-tests should include Continuous Wave (CW) signals.

In addition to the PPD and 'unintentional' signal-like CW sources, a number of other modulations and power profiles were used to help simulate other scenarios or to try to stimulate failure modes in receiving equipment which may not normally arise. One example of this approach includes the progressive jamming of multiple Global Navigation Satellite System (GNSS) signal bands and modulations where a new modulation was periodically added incrementally to the list of jammed signals before being removed in the reverse order. This so-called modulation 'pyramid' was intended to test the potential fallback behavior of modern multi-constellation multi-frequency receivers. Similarly, some tests were conducted with ramping power levels to better evaluate the sensitivity thresholds of various systems or, in other cases, persistent high-power jamming on one or more bands to provide both static and dynamic testing opportunities.

3. Scheduled Tests

In order to accommodate as many use cases as possible, the testing was split into multiple morning and afternoon sessions over the five days of testing at a primary site, in addition to periodic tests at a secondary site and the convoy testing of vehicles on the local roads. While it is not possible to list all of the tests carried out by all of the various participants here, a summary in the form of the transmission schedule used by the Norwegian Communications Authority, the Norwegian Defense Research Establishment, and the Norwegian Metrology Service for the primary test site has been reproduced for the purposes of this paper and is shown in Table 1.

Table 1. Primary site tests.

Time	Transmission Plan	Comments
Monday 14:00–14:45	Single-band PPD jammers	Sixteen one-minute tests of an assortment of single-band PPD jammers, including four with multiple individual jammers of the same model. These tests were first conducted with the jammers located inside a car, then repeated with the jammers moved to the roof of the vehicle.
Monday 15:00–15:30	Multi-band PPD jammers	Six one-minute tests of multi-band PPD jammers (repeated once with the devices placed inside a static test vehicle, then repeated with the devices on the roof of the vehicle). The dual-band jammers had two models, with two units of each model type, while the jammers with more than two bands of coverage had only single units of two different types.
Monday 15:30–17:45	High-power jammers	Signals emitted at 20 W Equivalent Isotropically Radiated Power (EIRP) from a directional antenna placed at location 2 directed towards location 3 with 15 min of test time per modulation. The modulations used were CW and PRN in combinations of L1 only, L1 + G1, L1 + G1 + L2 and L1 + G1 + L2 + L5.
Tuesday 9:00–12:45	Power ramp RFI	Signals generated commensurate with a 20 W EIRP transmission passed through a variable attenuator starting from 100 dB attenuation (2 nW EIRP) and stepping to 0 dB, then back to 100 dB attenuation in steps of 2 dB every 10 s. Tests were repeated for modulations CW and PRN on carrier combinations of L1, L1 + G1 + L2 + L5 and L2 + L5 + G2 + E5b, plus a test of only CW (no PRN) modulation conducted for the carrier combination of L1 + L5 + E5b.

Table 1. *Cont.*

Time	Transmission Plan	Comments
Tuesday 14:00–15:30	Sustained high-power jamming	Twenty-minute transmissions of 20 W EIRP jamming signals, first with CW modulation and then PRN modulation on the L1 only band, followed by the L1 + G1 + L2 + L5 band combination.
Tuesday 16:30–18:00	Modulation pyramid.	With 10 W of power and PRN modulation on each identified band, one modulation per step was added first, and this step was repeated at intervals of 3 min; then, one modulation per step was removed. The order of the bands added in steps was as follows: E5b, L5, G2, L2, B1I, G1, L1. These were then removed in reverse order.
Wednesday 9:00–10:30	Sustained high-power jamming II	A repetition of the sustained high-power jamming to allow vehicles to execute driving tests in the same environment.
Thursday 9:00–13:00	Simple spoofing	Numerous spoofing activities, some preceded by jamming, some including persistent jamming on non-spoofed signals. Various signals with stale ephemeris, synchronization at the tens of seconds level and large transmitted antenna position errors, each of which should have been easily detectable, were adopted.
Thursday 14:00–18:00	Advanced spoofing	Numerous spoofing activities, some preceded by jamming, some including persistent jamming on non-spoofed signals. Current ephemerides with synchronization at the ten nanoseconds level and accurate spoofed positions preceding dynamic spoofed positions.
Friday 9:00–13:00	Ad hoc testing	Various [1].

[1] The ad hoc testing on Friday was an opportunity to repeat or modify tests that attendees requested based on their observations during the previous days of testing (in this case, focusing on personal privacy device re-testing and mobile user evaluations).

4. Jamming Observations

The behavior of the receivers observed by the authors ranged from completely expected to entirely unexpected. Outcomes that were in line with the expectations of the authors included the relatively good resistance of mass-market receivers to CW interference, as several of these models are advertised to contain CW detection and or mitigation support in the receiver firmware. While the 20 W EIRP transmissions were still enough to cause loss of lock to these receivers, their resilience to one of the most commonly observed forms of RFI based on long term international monitoring [2] is encouraging.

A neutral observation from the jamming tests related to the relative behavior of survey receivers compared to mass-market devices when subjected to persistent strong jamming signals. When the high-end receivers are subjected to 'moderate' levels of RFI on all their tracked signal bands, their firmware will selectively halt the output of observables, with some models appearing to have a cut out at 36 dB-Hz. In comparison, mass-market receivers that come from product families formerly marketed as being 'high sensitivity' tend to continue outputting observables and position solutions at these and lower signal levels. This latter case led to multiple observations of a low-cost receiver continuing to generate a position solution even as the position error increased to hundreds of meters, as is shown in Figure 3. Appropriately, the receiver generated increased uncertainty estimates and appeared to consistently bound the actual position error, meaning that the generated information is not hazardously misleading if the reported uncertainty is used by the target application.

An unexpected observation that is reasonable in retrospect is that multi-band multi-constellation receivers can manifest problems with timing synchronization when a subset of their signal bands are jammed. In the context of positioning, these systems appear to fall back almost universally to remaining available signals when a subset of their tracked signals are denied by persistent jamming and continue to generate observables and position plus velocity information to the user; however, timing synchronization can encounter unexpected behavior. When the signals from the constellation selected for time scale synchronization are denied for an extended period, some receiver models appear to fail to maintain their synchronization to the selected timing reference and begin to rapidly drift in time while maintaining other outputs. While not expected at the time of the tests, this behavior does pose an interesting design question for receiver firmware as it is not immediately obvious what the 'correct' answer to this situation is. One potential answer is

that the receiver should rely on the data transmissions from other constellations, which include relative time offset information to indirectly track the selected time scale even when signals from the reference constellation are unavailable. Another potential approach is to simply halt outputting a solution as it is no longer possible to directly observe the selected time scale. Based on observed real-world behavior, it seems that some models of receivers have undefined or at least undocumented behavior with respect to their time scale synchronization when exposed to the jamming of the reference constellation, which could be more concerning to some users than a lack of outputs.

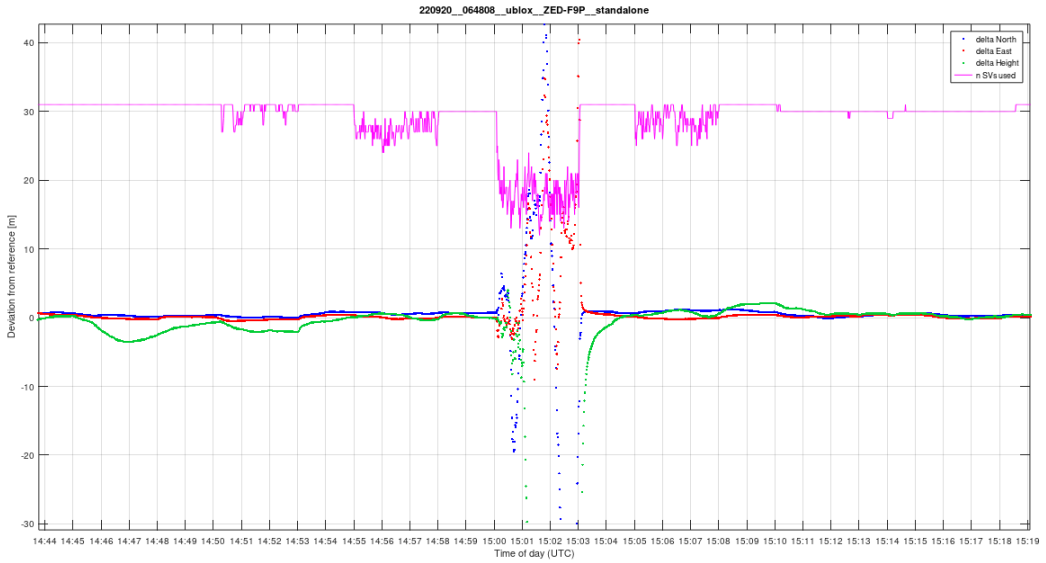

Figure 3. Number of tracked satellites and reported positional deviation of a static Ublox F9P receiver under jamming.

5. Spoofing Observations

The spoofing tests were physically arranged to allow as many participants as feasible to place their equipment under test within the line of sight of the transmitting antenna at a distance of less than approximately 20 m where possible. Based on this combination of criteria and the layout of the site in terms of where the spoofing signal generation equipment could be set up, the transmission antenna was placed in the middle of the front parking lot of the Bleik community center. One of the motivating factors for allowing users to operate as close to the transmission location as possible was the desire to minimize the amount of transmitted power required while also allowing the spoofed position information to be correct. The testing plan for the spoofing signal generation tests is included in Annex 1 for tests categorized as simple and Annex 2 for tests categorized as advanced.

Generating GNSS navigation signals that successfully masquerade as legitimately generated signals is difficult, with several publications indicating specific signal generation defects that can be used to aid in the detection of spoofed signals [3,4], including but not limited to time variation, correlation variation, position discontinuities, inconsistent observable data, incorrect ephemeris, or timing errors. In the Jammertest 2022 spoofing program, the distinction between the 'simple' spoofing tests and the 'complex' spoofing tests is the use of correct current ephemerides provided by the Norwegian Mapping Authority (Kartverket), together with the precise time keeping at the level of tens of nanoseconds for the latter. While the so-called simple tests could still entail careful pre-jamming, stable and high-fidelity signal generation, correct simulated ephemerides, and accurate initial position generation, the inclusion of precise synchronization enabled the evaluation of network timing receivers in addition to navigation-focused GNSS equipment. Attention to the generation of a representative and stable spoofing signal is particularly important given that some methods of potential spoofing investigation and detection might rely on the interaction of the produced signal with intentional antenna motion [5,6] or other

isolation techniques which may be complicated by an unstable signal source. This presents a challenge where the given signal would ideally be useful to everyone, which can be partly addressed through providing both 'simple' and 'complex' spoofing scenarios such as those provided at Jammertest 2022.

Some of the observations of note from the author's experiences during the test include expected results such as entry-level receivers (such as those integrated into the phones of the participants) being very quickly fooled by the spoofed signal. In one case, one of the participants took advantage of the spoofing tests to activate a fitness training app which happily believed the owner ran a distance of six kilometers (climbing over 450 m vertically) within six minutes and allowed them to post it to social media as a new 'personal best', indicating that the phone has no inertial sanity checking and that the app has no filtering for superhuman feats (Figure 4).

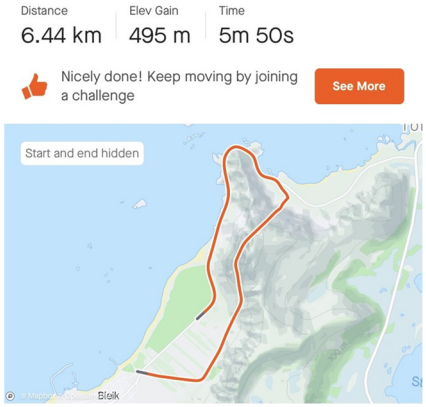

Figure 4. Screenshot from the Strava app showing a spoofed smartphone's reported superhuman run. Map data from Mapbox OpenStreet.

An unfortunate observation was that some high-end receiver systems supporting quadruple constellation triple frequency operation could be driven into apparently unrecoverable states via the single-frequency spoofing and multi-frequency jamming combinations of even the simple spoofing tests. Despite having an internal oscillator that is relatively stable, the receiver transitioned from tracking real signals to tracking the spoofed signals after only a short period of jamming but then would not recover after the removal of the spoofing and jamming. Instead, more than 40 min after the removal of the perturbing signals, the receiver reported that it was tracking only several GLONASS satellites and one QZSS satellite, stating that the receiver altitude was 1500 m higher than in reality and that it was slowly floating away ever higher.

A beneficial outcome of the spoofing tests was that even when the spoofing signals were generated with a power level approximately 20 dB (too weak to impact the assembled receivers), systems with in-band power level monitoring capabilities still noted significant and obvious changes in the level of their respective automatic gain control feedback states or measured in-band power levels. This is encouraging as it implies that even relatively low-cost receivers that generate Automatic Gain Control (AGC) level outputs have an additional avenue available to them for the detection and reporting of potential spoofing signals.

6. Unexpected Observations

The first of the notable unexpected observations was that on the morning of Tuesday 20th September, the scheduled power ramp test was apparently interrupted by multiple events of unintentional RFI. This test presented an opportunity for evaluating the detection thresholds of various pieces of equipment, including the Advanced RFI Detection Analysis and Alerting System (ARFIDAAS) monitoring system [2], which includes direct band power measurement instruments as part of its normal detection process. Monitoring using

the ARFIDAAS system started approximately three minutes before the designed test start time, and the system almost immediately began detecting and logging events. Over the three-minute period between the start of logging and the start of the test, three separate RFI events were captured. Since the test was scheduled to start with an extremely low EIRP of approximately 2 nW, it was initially thought that these detections implied that either an incorrect attenuator setting had been selected at the transmission site or that an unrelated project participant had mistakenly activated one of the test PPDs without permission; however, upon a closer inspection of the three events, none of them matched either the expected test signals or the known signals from the PPD selection. Upon further review, three distinct RFI signals of unknown origins had been captured coincidentally in the time prior to the start of the test and despite the remote nature of the test site. The first of these was a 'chirping' signal thought to be formed by self-resonant feedback in car-borne navigation or entertainment systems impacting the G1 band; the second was a pulsed CW source near the Beidou B6 center frequency, while the third was a continuously active 1200 MHz narrowband signal. A spectrogram of the unintentionally generated 'chirping' signal is presented in Figure 5. Here, it should be noted that while the modulation appears to be a form of chirp signal, the center frequency and limited bandwidth of the signal indicate that it would be a relatively ineffective jammer to use against GPS, Galileo, and Beidou signals, though might present difficulties for GLONASS reception.

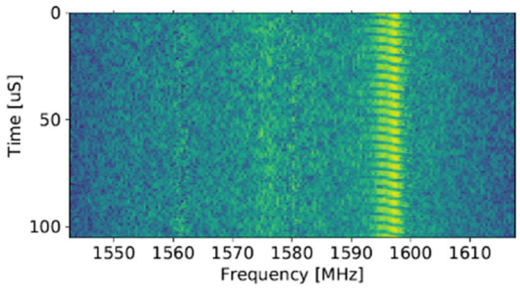

Figure 5. A time–frequency plot of a suspected unintentionally generated signal emitted from a car passing the test range just prior to the start of the low-power ramp test (detected using ARFIDAAS system hardware). Color encodes relative signal strength with lighter yellows indicating concentrated signal power.

A second unexpected observation was that some of the receivers used by the participants to evaluate Network RTK service performance during jamming and spoofing were disrupted by the RFI in a way that was not predicted to be a point of failure before the testing. In at least one receiver model, the loss of RTK performance was not caused by the degradation of the GNSS observables but instead by the disruption of the 2.4 GHz Wi-Fi-based data link between the receiver and the controlling computer acting as a correction relay to the receiver. It is unclear how much energy the jamming devices in question were leaking at or near the 2.4 GHz band used by the receiver's Wi-Fi link, but observations in the wild have shown the opposite situation, whereby malfunctioning Wi-Fi devices act as GNSS jammers by emitting at half of their expected operating frequency. This shows an additional danger of cheap jammer devices, in addition to their intended purpose the poor production value can cause additional interference in other, not-intended bands.

A third surprise came in the form of the difficulty encountered in calibrating the power level employed in spoofing the collected GNSS receivers. Before shipping the signal generation equipment to the venue, the selected scenarios were generated and tested in the Norwegian metrology service's (Justervesenet) lab to tune parameters such as the transmitted power level. However, after setting up on site and initial attempts were made to generate the spoofing signals for the test scenarios, none of the user receivers were initially captured by the generated spoofing signal. It was eventually necessary to increase the transmitted spoofing power by 20 dB relative to the starting point. Some of this difference was eventually explained by the use of a different cable assembly between

the signal generator and the transmitting antenna, but this is not thought to explain the entirety of the change power level requirement. Despite careful preparation, generating a realistic minimum power spoofing signal was demonstrated to be challenging once more.

A final unexpected observation was that some of the highest-end navigation systems evaluated had more significant problems as a result of the generated signals than their much lower-end counterparts. For example, one of the mass-market automotive platforms appeared to be unaffected in terms of reported position solution by the generated spoofing due to integration with a set of low-cost Micro Electro-Mechanical Systems (MEMS) inertial sensors, while one of the high-end navigation systems, which integrated a ring laser gyroscope-based Inertial Navigation System (INS), accumulated a kilometer-level navigation error during jamming tests and could not recover until power cycled. The assumption is that the automotive receiver was successfully leveraging Zero-velocity Update (ZUPT) detection while the high-end platform intended to operate in an airborne platform may not have supported this state detection, as this effect was not expected to be observed in normal operation.

7. Conclusions and Data Availability

One of the standout observations from the tests was that various pieces of receiver equipment manifested behaviors that could be considered naive or counterintuitive when faced with jamming and spoofing signals, which indicate that the device firmware does not appear to be designed to monitor for or guard against the impacts of these threats. For example, integrated systems such as smartphones or network-connected receivers make no observable attempt to mitigate spoofing attacks that utilize obviously incorrect timing information. While the timing and positioning gap is not as egregious as that observed during the spoofing incident at ION 2017 [7], even a modest cost quartz oscillator should not be fooled by jumps of several seconds after a short period of signal denial, but this was observed during Jammertest. Hopefully, in the coming years, manufacturers will continue to deploy anti-jamming and anti-spoofing technologies within their receivers that can leverage even simple AGC state behavior to mitigate the impacts of these threats, implement firmware that can exploit the diversity of timing sources such as network timing protocol servers to prevent gross errors, or, at least, adjust their firmware parameters to allow receivers to gracefully recover within an hour of spoofing termination if they insist on allowing their clock to jump by tens of seconds in the first place.

The activities at Jammertest 2022 were an invaluable opportunity for commercial, governmental, research, and academic organizations to observe the behavior of GNSS-dependent navigation and timing equipment under jamming and spoofing conditions. While other events of this nature have been held before, the policy of open data access sets this event apart and provides a chance for others to learn from the experiences of the attendees not just through abstracted publication but also through the direct sharing of captured data.

The authors of this paper are pleased to be able to make available selected subsets of the testing data captured at Jammertest 2022 from the primary site tests. These data include raw IF spectrum captures of the L1/E1/G1 band captured with 40 MHz complex sampling during the entirety of the spoofing tests, as well as other data captured by the ARFIDAAS monitoring station via SINTEF, ublox F9P receiver data captured during various jamming and spoofing tests throughout the course of the test plan (captured via Kartverket and a centimetric network), and RTK receiver data captured throughout the tests via Kartverket. For access to these data, please contact the corresponding authors.

Author Contributions: A.M.: primary document drafting. N.S.: primary document drafting and proofing. A.S.: contributed receiver position deviation results. N.G.: documentation of test setup and descriptions. A.R.: setup of jamming and power level descriptions. H.H.: description of spoofing test setup and considerations. T.R.: description of spoofing test setup and document proofing. T.D.: contribution of receiver spoofing position domain observations and discussions. All authors have read and agreed to the published version of the manuscript.

Funding: The authors would like to thank the European Space Agency NAVISP program for funding the development of the ARFIDAAS system (NAVISP3-EL3-015), as well as the Norwegian Council of Research (project number 305051) for funding the participation of the primary authors and data analysis activities. Authors H.H. and T.R. would like to thank the Norwegian Space Agency for funding through project 74GA2203.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: For data availability please contact the authors via email.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Rødningsby, A.; Morrison, A.; Sokolova, N.; Gerrard, N.; Rost, C. RFI Monitoring of GNSS Signals on Norwegian Highways. In Proceedings of the 33rd International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2020), Virtual, 21–25 September 2020.
2. Morrison, A.; Sokolova, N.; Swinden, R.; Musumeci, L.; Caparra, G. Advanced RFI Detection, Alert and Analysis System Design and Monitoring Campaign Results. In Proceedings of the NAVITEC 2022, Virtual, 5–7 April 2022.
3. Kujur, B.; Khanafseh, S.; Pervan, B. Detecting GNSS Spoofing using Temporal Behavior of Spoofed Signals. In Proceedings of the 34th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2021), St. Louis, MO, USA, 20–24 September 2021; pp. 3668–3682.
4. Turner, M.; Wimbush, S.; Enneking, C.; Konovaltsev, A. Spoofing Detection by Distortion of the Correlation Function. In Proceedings of the 2020 IEEE/ION Position, Location and Navigation Symposium (PLANS), Portland, OR, USA, 20–23 April 2020; pp. 566–574.
5. Psiaki, M.L.; Powell, S.P.; O'Hanlon, B.W. GNSS Spoofing Detection using High-Frequency Antenna Motion and Carrier-Phase Data. In Proceedings of the 26th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2013), Nashville, TN, USA, 16–20 September 2013; pp. 2949–2991.
6. Humphreys, T.E.; Ledvina, B.M.; Psiaki, M.L.; O'Hanlon, B.W.; Kintner, P.M., Jr. Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer. In Proceedings of the 21st International Technical Meeting of the Satellite Division of the Insitute of Navigation (ION GNSS 2008), Savannah, GA, USA, 16–19 September 2008; pp. 2314–2325.
7. Scott, L. Spoofing Incident Report: An Illustration of Cascading Security Failure. Inside GNSS Magazine—Global Navigation Satellite System Engineering Policy, and Design. Available online: insidegnss.com/spoofing-incident-report-an-illustration-of-cascading-security-failure/ (accessed on 28 April 2023).