engineering proceedings

MDPI

Proceeding Paper

Making a Good Thing Better: Jammertest 2023 Jamming, Meaconing, Spoofing, and Synchronization on the Norwegian Coast †

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

[1] SINTEF Digital, 7034 Trondheim, Norway; nadia.sokolova@sintef.no
[2] Nkom, 4790 Lillesand, Norway; nicolai.gerrard@nkom.no
[3] Justervesenet, 2007 Kjeller, Norway; hha@justervesenet.no (H.H.); thr@justervesenet.no (T.R.)
[4] Forsvarets Forskningsinstitutt, 2007 Kjeller, Norway; anders.rodningsby@ffi.no
* Correspondence: aiden.morrison@sintef.no
† Presented at the European Navigation Conference 2024, Noordwijk, The Netherlands, 22–24 May 2024.

Abstract: Jammertest is the largest known GNSS jamming, meaconing, and spoofing test event in the world, which has an open policy towards both user participation and user communication with no restrictions on the sharing of data or publication of results. The organizers implemented several changes and enhancements within the 2023 test campaign to further broaden the appeal and applicability of the tests for as many demographics of GNSS users as possible. More than 200 participants from 19 nations took part in person from 18 to 22 September at the test sites along the west coast of the Andøy island. This paper summarizes the design and motivation of the tests and test venue with particular attention to the efforts taken to provide users with precision timing and frequency references independent of the denied and disrupted GNSS signals. Aspects of surveilling and enforcing unintentional emissions, and real-time communication and coordination to the large number of distributed participants are also discussed.

Keywords: GNSS; jamming; meaconing; spoofing; interference; resilience; security

Academic Editor: Terry Moore

Published: 24 March 2025

Citation: Morrison, A.; Sokolova, N.; Gerrard, N.; Hauglin, H.; Rødningen, T.; Rødningsby, A. Making a Good Thing Better: Jammertest 2023 Jamming, Meaconing, Spoofing, and Synchronization on the Norwegian Coast. *Eng. Proc.* **2025**, *88*, 15. https://doi.org/10.3390/engproc2025088015

1. Introduction

Since 2021, Jammertest has been an annual exercise hosted in Norway by Norwegian authorities including The Public Roads Administration (NPRA), The Communications Authority (Nkom), The Metrology Service (JV), The Defense Research Establishment (FFI), and The Space Agency (NSA). In 2023, more than 64 organizations from 19 countries traveled to the island of Andøya in Northern Norway to evaluate positioning, navigation, and timing (PNT) systems under a plurality of test scenarios, including low- and high-powered jamming, meaconing, position spoofing, and time offset attacks over the five-day test period. This paper describes the details behind the extensive tests carried out at Jammertest 2023 from the point of view of the test organizers and operators. In addition to describing the setup, scenarios, and equipment used, particular emphasis will be given to describing the ways in which precise time and frequency information were provided to both spoofing transmission and user receiver equipment within the affected zone of the test area throughout the campaign.

Three test locations were set up on the western side of the island, with the primary test site centered at the community of Bleik with the secondary and tertiary sites south

of the town. The areas were selected to provide test locations mutually shielded from each other by terrain and distance to allow independent simultaneous testing at each individual site while also using the natural geography of local mountain ridges to protect the mainland and mainland airspace from the high-powered emissions. The primary site hosted fixed transmission equipment for both jamming and spoofing, while the secondary site was dedicated to personal privacy devices (PPD) both statically and mobile between the secondary and tertiary sites. The tertiary site focused on mobile jamming and spoofing from SDR-based spoofers.

Jammertest is a special resource for the positioning navigation and timing (PNT) community in that it is the only known jamming, meaconing, and spoofing event that has policies of both open participation and open communication. Similar events that include high capability jamming and spoofing signals require either invitation, non-disclosure agreements, or both and, therefore, limit the portability of the lessons learned at the events, while Jammertest has a policy of open communication and data sharing between participants, and the public. There are signs that this aspect of Jammertest has encouraged other test operators to begin opening the terms of participation in their events, which is a welcome development. Additionally, the test site of Andøya allows testing on the ground, in the sky, and at sea.

2. Test Venue and Planned Activities

The testing venue comprised three locations along the western shore of Andøya, a map of which is shown in Figure 1.

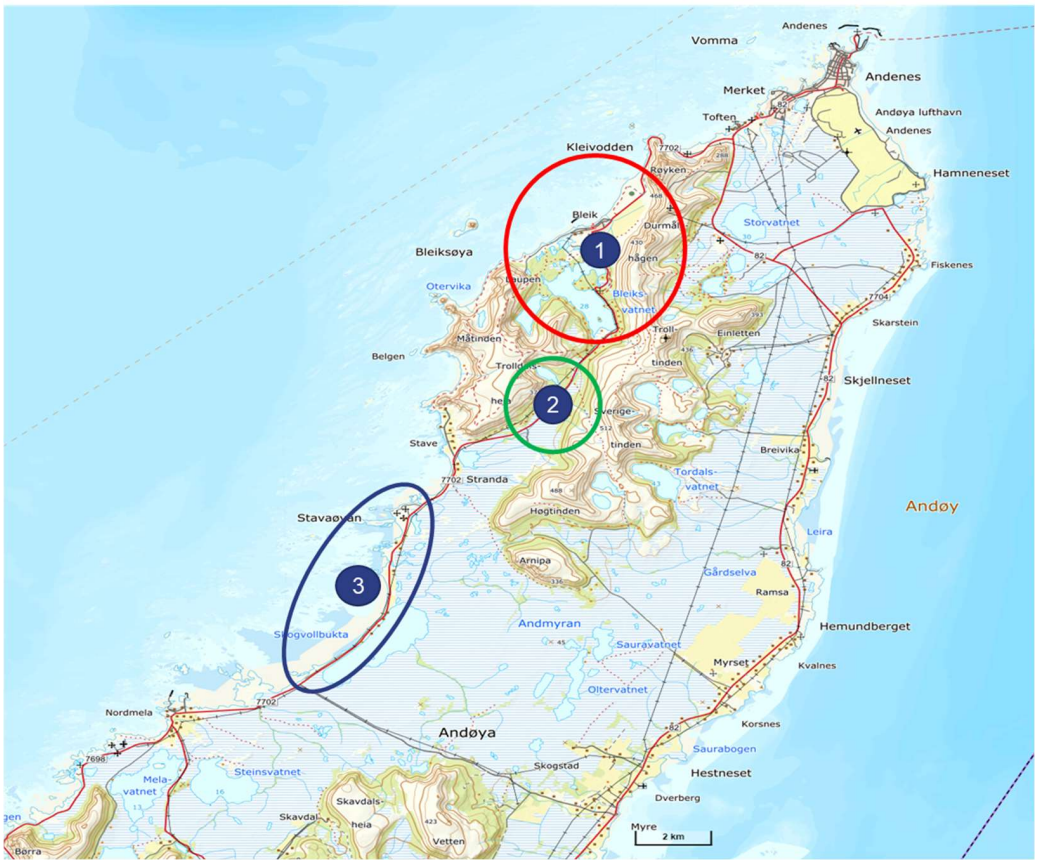


Figure 1. Topographical map of the Northern extent of Andøya Norway showing the three test locations along the Northwestern coast facing the Atlantic Ocean (base map is retrieved from Norgeskart.no). Location one was the community house at Bleik, with locations two and three lying to the south.

At the primary test site signals were generated using both custom and consumer off the shelf (COTS) devices depending on the active test scenario. High and low powered jamming signals were transmitted by directional antennas from lowland fields by Bleik (point A in Figure 2) and at the top of the local mountain ridge overlooking the lowlands (point B in Figure 2) to optimize the coverage area, allow directional jamming with different elevation angles, and to allow for meaconing transmission (minimize the chances for a feedback loop).

Figure 2. Topographical map of test location 1 (Bleik). Point A is the location of the jamming equipment at the lowland fields of Bleik, point B is the location of the jamming and meaconing equipment at the mountain ridge and point C is the basecamp (Bleik proper) and location of the spoofing equipment. (base map is retrieved from norgeskart.no).

An array of eight antennas and amplifiers were used to produce these signals on the mountain top allowing individual band control and power level for numerous signals targeting different sections of the L-band independently. An additional vertically mounted transmission antenna was placed at the Bleik community house (point C in Figure 2) in the center of the test area from which spoofing and additional jamming signals were generated. These spoofing signals were generated by Ettus x300 radios [1] fed by Safran Skydel simulator software version 23.5.4 [2]. The antenna array on the mountain as well as the antenna set on the roof of the community center below are both shown in Figure 3.

At the secondary and tertiary test sites, signals were generated with PPDs for the jamming and with a SDR for the spoofing. These two test sites were shielded from high power transmission from test site 1 by the local topography and from each other by distance and limits to the transmission power.

Comparing the tests carried out in previous years, the number, variety, and precision of the tests were all enhanced to provide users with as broad an array of opportunities to collect as relevant data as possible. As listed in Table 1, a focus on user directed testing was emphasized at test sites 2 and 3 during Jammertest 2023, allowing participants to define the details of test scenarios they wished to carry out in coordination with the test organizers.

(**a**) (**b**)

Figure 3. The primary test site at Bleik employed multiple antennas and antenna arrays to transmit the jamming, meaconing, and spoofing signals over the test area: (**a**) The array of transmission antennas used for the execution of jamming and meaconing tests at test site 1 positioned high on the adjecent mountain ridge to optimize coverage of the test area, etc. (**b**) the set of antennas installed on the Bleik community house within test site 1 from whichposition spoofing and timing attacks were transmitted, and the RF environment monitored by Nkom.

Table 1. Test activity schedule from Jammertest 2023. Gray highlighted fields indicate activities, which were customizable to the needs of attending users and made available on a reservation basis.

	Test Site 1 Activities	**Test Site 2 Activities**	**Test Site 3 Activities**
Monday AM *	User setup	User setup	User setup
Monday PM	High power stationary jamming	User directed tests (reserved timeslots)	User directed tests (reserved timeslots)
Tuesday AM	Power ramp (0.1 µW to 20 W), High power stationary jamming	User directed tests (reserved timeslots)	Motorcades with stationary PPDs
Tuesday PM	Meaconing (0.1 W and 10 W)	User directed tests (reserved timeslots)	Motorcades with moving PPDs
Wednesday AM	Incoherent stationary spoofing, synthetic and true ephemerides	User directed tests (reserved timeslots)	Motorcades with stationary PPDs
Wednesday PM	Coherent stationary spoofing, true ephemerides	User directed tests (reserved timeslots)	Motorcades with moving PPDs
Thursday AM	Incoherent time spoofing, synthetic ephemerides	Multi-jammer scenarios User directed tests (reserved timeslots)	Vehicle borne SDR based spoofing
Thursday PM	Coherent time spoofing, true ephemerides	User directed tests (reserved timeslots)	Vehicle borne SDR based spoofing
Friday AM	PPD jammers and high-power jamming	User directed tests (reserved timeslots)	User directed tests (reserved timeslots)
Friday PM	Packing and cleanup	Packing and cleanup	Packing and cleanup

* The morning tests ran from 09:00 until approximately 13:00, while the afternoon tests ran from 14:00 until 18:00.

3. On-Site Synchronization

One of the primary challenges to the execution and evaluation of spoofing, meaconing and precisely controlled time-offset attacks was the need to have accurate timing for

both the test operators and test participants throughout the duration of transmissions, independent of the local GNSS signal environment. Without a ground truth reference for time and frequency, measuring the impact on the time estimates of receivers when exposed to meaconing and spoofing attacks cannot be gauged. To achieve this reliable reference, the hosts exploited the local geography of the island as well as Norwegian infrastructure to provide two sources of timing information throughout the test sessions. The first of these was GNSS over a fiberoptic connection from the Andøya space facilities, which were within 5 km of the primary test location but masked from all test sites by the local mountainous terrain. This remotely captured GNSS signal was fed to a novel prototype PPP disciplined clock [3], which was compensated for the fiber and other delays in the distribution network. The second was a remotely located Cs-clock backed Enhanced Primary Reference Time Clock [4] routed to the site over the multi-hop precision timing protocol [5] distribution chain shown in Figure 4, where other important elements are marked including: (i) >100 km of Norwegian operator Telenor's core timing network; (ii) 120 km high accuracy White Rabbit [6] PTP link using dedicated channels in the dense wavelength division multiplexed (DWDM [7]) network operated by the academic network provider Sikt; (iii) 5 km bidirectional link over dark fiber. At the test site these timing signals were used to provide PTP network timing as well as precise 10 MHz signals and pulse per second (PPS) markers through distribution amplifiers for test operators and participants alike.

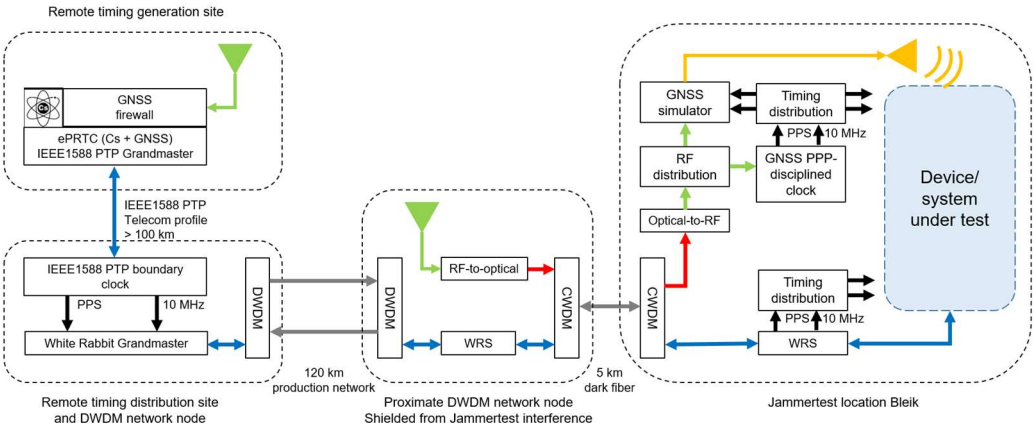
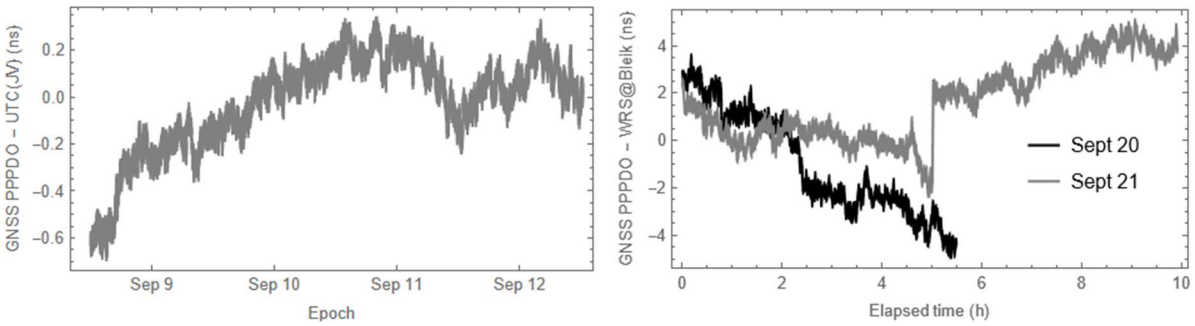


Figure 4. Setup for distributing reference timing to Jammertest.

At the primary test site, timing was exposed on two separate interfaces from the two implemented sources. The absolute and relative performance achieved by these time and frequency references is shown in Figure 5.

The left-hand plot indicates the level of synchronization between the locally provided time synchronization and the UTC timescale maintained by Justervesenet in Norway. The system was characterized prior to the Jammertest activities and maintained a full range of less than a nanosecond over a five-day period.

The right-hand portion indicates the level of timing synchronization employed by the GNSS simulator used for spoofing purposes during Jammertest relative to the white rabbit protocol distributed synchronization signal, which was provided to users at the Bleik (test site 1) test venue.



(**a**) (**b**)

Figure 5. The performance of the provided reference time and frequency was evaluated over the course of the Jammertest events in terms of both synchronization relative to the UTC(JV) reference and between local distribution methods: (**a**) The performance of the local GNSS PPPDO relative to the UTC timescale maintained by Justervesenet in Norway was evaluated over several days prior to the week of Jammertest; (**b**) the level of disagreement between the two locally generated time and frequency references monitored over the final two days of Jammertest 2023.

The motivation for ensuring tight synchronization between the transmitting simulator and the national time scale was to ensure that the coherently generated spoofing and timing attacks were generated with the closest feasible time alignment to the live GNSS timescale. The motivation for providing the synchronization signal to the users was slightly different in nature and was directed at solving the implied problems of reliance on GNSS for synchronization purposes when GNSS itself is the target of intentional disruption. Many modern systems rely implicitly on GNSS availability for precise time and frequency control via GNSS disciplined oscillators creating a chicken-and-egg data dependency between the effectiveness of the attack and the quality of the data produced by these instruments. Provision of precise time and frequency by Justervesenet to the test participants thereby turns the white rabbit synchronization protocol into a metaphorical timing easter bunny, providing the precise timing without local reliance on GNSS.

4. Description of Jamming and Spoofing Signal Sources

The three test sites were picked to satisfy different use cases:

- Test site 1 allowed high power transmissions without unacceptable impact on other parts of Andøya and Norway, and it also provided areas fit for flying UAVs, fields with long (further than 1 km) line-of-sight, a village giving opportunities to test with buildings and inhabited areas, access to a harbor and to the sea, terrain where the interference signals could naturally be blocked, and signals generated here did not overlap with signals generated at the other two test sites.
- Test site 2 was far enough away from test site 1 to be used in parallel without worrying about causing disruptions for each other. Furthermore, it was remote and flat, with access to both a large parking lot and a road, meaning one could do tests with UAVs, vehicles and on foot.
- Test site 3 was chosen to create another low power transmission test area, this one with a focus on automotive tests and tests requiring vehicle-born test beds to be driven over longer distances. Within the transmission power regulations, this test area and test site 2 could be used in parallel, significantly increasing both the number of test subjects, the number of tests, and the use of the areas outside of Bleik.

4.1. Test Site One Equipment

The high-power jammer used on the mountaintop at test site one can provide jamming signals with up to 200 W EIRP simultaneously on eight GNSS bands. The jammer uses two USRP X410 SDRs from Ettus Research [1] as signal generators. Each SDR had four output channels covering the frequency range of 1 MHz to 7.2 GHz, with maximum 400 MHz instantaneous bandwidth. The SDRs have an internal gain range of 60 dB in 1 dB steps. Each of the output signals are fed to the corresponding channel of the programmable 10-channel step-attenuator with an individual attenuation range of 95 dB in 0.25 dB steps. The output signal from the attenuators is then fed to eight individual power amplifiers. These amplifiers are further connected to eight individual antennas via lengths of 10 m plus 20 m coaxial cables. The antennas are directional helical antennas with right hand circular polarization (RHCP) and approximately 10 dB gain.

A PC running Linux controls both SDRs and the step-attenuators. The software on the PC allows the jammer to automatically execute the individual tests described for the high-power jammer and supports all jamming signals described therein.

Spoofing signals generated at the community house using Safran Skydel simulation software in combination with two USRP X300 transmitted through FFI supplied amplifiers and roof-mounted antennas as shown in Figure 6. To ensure that the signals were properly synchronized the timing signals for the USRPs were provided from a rubidium oscillator synchronized through the timing solution described in Section 3. In addition to this Skydel requires information from a connected GNSS receiver to synchronize the simulation start time to the live sky GNSS signal. For this purpose, a u-Blox M8T [8] receiver was used, with the signal provided over fiber from a remote location as part of the system described in Section 3.

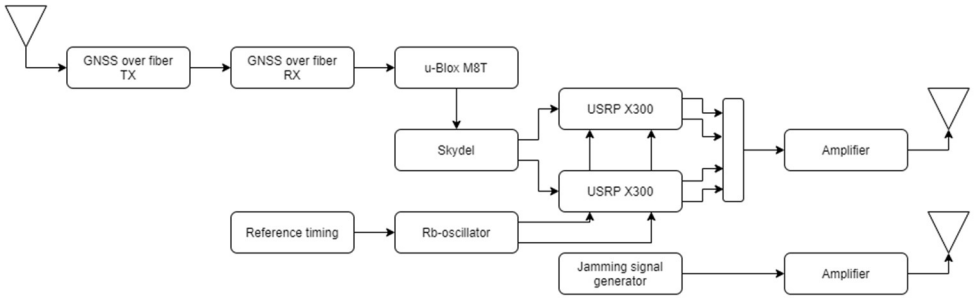


Figure 6. Setup for spoofing signal generation and transmission.

When transmitting a combination of jamming and spoofing signals the jamming signals generation was split between the "upper" and "lower band". The jamming signals transmitted in the "upper band" was generated by Skydel, while jamming signals in the "lower band" were generated by external FFI equipment and transmitted from a second antenna.

The ephemeris data used when generating the spoofing signals came from two sources, Hourly RINEX V2 GPS Broadcast Ephemeris from NASA's crustal dynamics data information system (CDDIS) [9], and for Galileo the Norwegian mapping authority provided the information from the reference station on Andøya. The incoherent ephemeris data used in some scenarios was generated by propagating several-years-old ephemeris data in the simulator. The low-power jammers employed at this test site were a subset of the PPD variety employed at site two as described below.

4.2. Test Site Two Equipment

At test site 2, a total of 28 jammers were in play. Most of these jammers were of the PPD variety, meaning they are produced for (illegal) sale to private citizens who usually use them for privacy purposes (although their entire span of use is much wider). All jammers had been given technical characteristics such as bandwidth, estimated max power output, sweep rate and what GNSS bands could potentially be afflicted by which transmission.

4.3. Test Site Three Equipment

The portable spoofing transmitter used at test site three comprised a bladeRF x115 from Nuand [10], a low-noise amplifier with 45 dB gain, and a dipole antenna. The antenna was mounted on the top of a test car. During the mobile spoofing tests the test car with spoofing antenna was in the middle of the convoy, and the distance between the vehicles were kept as small as possible to have enough spoofing signal power to reach all vehicles in the convoy, even with more than eight vehicles participating. The low power jammers employed at this test site were of the PPD variety as discussed above.

5. Discussion of Unexpected Transmissions

A practical consideration when bringing many users operating experimental electronic devices into proximity is that unintentional transmissions are more likely than not to occur. Since these spurious emissions could frustrate the efforts of other test participants to conduct a well-controlled evaluation of their devices, an effort was made to continuously monitor the spectrum. In events where anomalous emissions were detected by the central monitoring or reported by users, a member of Nkom with mobile source search equipment would proceed to the reported location to attempt to locate and identify the source of the unintentional emissions.

While there were thankfully no serious disruptions to the official tests encountered at Jammertest 2023, there were three interesting events that highlight the value of the monitoring and control activities. First, a group of participants who were testing digital beamforming techniques using COTS (Commercial Off-The-Shelf) hardware proved to be the source of spurious emissions in the GPS L1 band when their receiver was powered. The source of the emissions was determined to be the low-cost patch antennas in use with their receiver that unfortunately became self-resonant when driving the inputs of their SDR devices. A compromise was reached in this case that allowed this group to move away from the main building to a distance where their low-level spurious emissions were no longer visible to other test participants. A second source of spurious emissions was eventually localized to a RADAR transmitter within a test vehicle owned and operated by one of the automotive test participants, with the test RADAR emitting a low magnitude but observable rake signal (see, e.g., [11]) into the L-band when in operation. This vehicle was allowed to continue to test but was kept away from other operators during testing.

Despite the best efforts of the test operators and the active hunt for spurious signals, one subtle case of spurious emissions was not identified until test participants had begun to process their event data and noticed inconsistencies therein. During the meaconing tests, the intention was that the spectrum around the GPS/Galileo/Beidou L1 frequency be re-transmitted with GLONASS G1 filtered out. Due to the combination of the level of gain used and the roll-off of the filtering in the meaconing equipment, a subset of the GLONASS satellites were unintentionally re-transmitted at a power level comparable to the live-sky signals resulting in selective disruption of the GLONASS observables generated by some receivers. Ultimately, this is an interesting scenario worthy of testing but also a deviation from the intended transmission plan.

6. Potential Improvements for Jammertest 2024

The Jammertest organizers strove to make the 2023 Jammertest event not only the biggest Jammertest event so far, but also the best in terms of both the tests conducted and the accuracy with which this information was communicated to the participants in real time. Small deviations in the test plan are inevitable over the full week of intensive testing, and while 2022's event made use of an RSS [12] feed and teams chat groups for event status communication, it was found that these were not fully satisfactory in terms of function and reliability. To address this, the event operators secured a license to transmit a low-power FM radio signal during the test events and used this to broadcast a Jammertest radio station that carried definitive test updates including a warning of test starts and termination. This radio station made it much easier for outdoor and mobile users to keep track of the current state of the test plan than the chat solution alone achieved, though a messaging and chat client was also used as a secondary communications channel. In parallel, fiber optic connectivity was routed to the test venue to facilitate the provision of precise timing information but to also greatly improve the reliability of internet connectivity, which in previous years had been limited, forcing users to rely on expensive and sometimes slow cellular data coverage.

Looking forward to 2024, there are a few areas, which may be pursued to further enhance the quantity, quality, and reliability of the test scenarios such as turning a bug into a feature via extending the range of frequencies passed by the meaconing tests to cover the entire GLONASS band or by installing additional filtering to prevent the partial retransmission of the G1 band observed at Jammertest 2023. Additionally, the offer of precise time and frequency information to participants proved more popular than expected, particularly in the case of the UTC aligned PPS signal. The provision of additional ports for the time reference signals will, therefore, be pursued by the organizers.

Author Contributions: Conceptualization, A.M. and N.S.; writing—original draft preparation, A.M., N.S., N.G., H.H., T.R. and A.R.; writing—review and editing, N.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research was partially funded by the Research Council of Norway, grant number 332528 and the Norwegian Space Agency grant number 74GA2307.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Selected data available from test participants and paper authors. Please contact the corresponding author for more information.

Acknowledgments: The authors would like to thank the Bleik community and community house members for their hospitality and help.

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

References

1. Ettus Research™: USRP X Series. Available online: https://www.ettus.com/product-categories/usrp-x-series/ (accessed on 15 February 2024).
2. Safran Federal Systems: GNSS Testing and Simulation. Available online: https://www.safranfederalsystems.com/gnss-testing-and-simulation (accessed on 15 February 2024).
3. Fugro: Time Synchronization Service Fugro AtomiChron®. Available online: https://www.fugro.com/expertise/other-expertise/atomichron (accessed on 15 February 2024).
4. *G.8272.1/Y.1367.1*; Timing Characteristics of Enhanced Primary Reference Time Clocks, ITU-T Recommendation. International Telecommunication Union (ITU): Geneva, Switzerland, 2016.

5. He, K.; An, C.; Hui Wang, J.; Li, T.; Zu, L.; Li, F. Multi-hop Precision Time Protocol: An Internet Applicable Time Synchronization Scheme. In Proceedings of the NOMS 2022–2022 IEEE/IFIP Network Operations and Management Symposium, Budapest, Hungary, 25–29 April 2022; pp. 1–9. [CrossRef]
6. Lipiński, M.; Włostowski, T.; Serrano, J.; Alvarez, P. White Rabbit: A PTP application for robust sub-nanosecond synchronization. Proceedings of ISPCS 2011, Munich, Germany, 12–13 September 2011.
7. Brackett, C.A. Dense wavelength division multiplexing networks: Principles and applications. *IEEE J. Sel. Areas Commun.* **1990**, *8*, 948–964. [CrossRef]
8. u-blox: NEO/LEA-M8T Series: U-blox M8 Concurrent GNSS Timing Modules. Available online: https://www.u-blox.com/en/product/neolea-m8t-series (accessed on 15 February 2024).
9. NASA CDDIS: GNSS Orbit Products. Available online: https://cddis.nasa.gov/Data_and_Derived_Products/GNSS/orbit_products.html (accessed on 15 February 2024).
10. Nuand: BladeRF x115. Available online: https://www.nuand.com/product/bladerf-x115/ (accessed on 15 February 2024).
11. Sokolova, N.; Morrison, A.; Diez, A. Characterization of the GNSS RFI Threat to DFMC GBAS Signal Bands. *Sensors* **2022**, *22*, 8587. [CrossRef] [PubMed]
12. RSS.com. How Do Really Simple Syndication Feeds Work? Available online: https://rss.com/blog/how-do-rss-feeds-work/ (accessed on 22 February 2024).