Statens vegvesen
Norwegian Public Roads Administration

Norwegian Communications Authority

FFI Forsvarets forskningsinstitutt
Norwegian Defence Research Establishment

Justervesenet

Jammertest 2022

Report on jamming and spoofing of GNSS equipment and GNSS based systems performance at Andøya, Norway, in 2022

June 2023

Summary

Jammertest 2022 was carried out between the 19th and the 23rd of September 2022 at Andøya, Norway. The purpose of the test gathering was to offer a test area to industry, academia, defence actors and the public sector, where the participants could be exposed to jamming and spoofing of GNSS in a controlled environment.

This report reviews the arrangement; the background, the purpose, an overview of the performed jamming and spoofing attacks and gives a high level, observational summary of the results of the test. At the end, a recommendation on a future Jammertest (‘*Jammertest 2023*’) is put forward.

Table of Contents

1 Background

Jammertest 2022 was a gathering that grouped industry, the defense sector, academia and the public sector together so that they could expose their equipment, systems and procedures and/or routines to GNSS jamming and spoofing in a controlled environment. This was carried out between the 19th and the 23rd of September 2022 at Andøya in Northern Norway.

The background for conducting the array of jamming and spoofing attacks, collectively known as tests, was ideas developed in a government discussion forum in 2019 and 2020, which led to the arrangement Testfest 2021, a small-scale version of Jammertest done in Skibotndalen in Troms in 2021.

The organisers of Jammertest 2022 were the Norwegian Public Roads Administration (NPRA), the Norwegian Communications Authority (Nkom) and the Norwegian Defence Research Establishment (FFI). The Tromsø-based company Testnor was hired for on-the-ground practical support, project lead and communication. In addition to this, the Norwegian Metrology Service assisted the organisers with technical expertise and implementation of the spoofing attacks.

Definitions:

- GNSS – Global Navigation Satellite System. Satellite systems that provide position, navigation and time on a global scale. There exists four such systems; the American *GPS*, the Russian *Glonass*, the Chinese *Beidou* and the European *Galileo*.
- Jamming – electromagnetic noise at specific frequencies or in a specific frequency band, intended to disrupt the legitimate wireless services using these frequencies. Typically designated as a denial-of-service attack.
- Spoofing – tricking a receiver by sending signals simulating the service one would want to copy, with the intention of making the receiver process these false signals instead of the actual service signals (in the case of GNSS, from the satellites). Usually termed as a deception-of-service attack.
- High effect jamming: Jamming transmissions originating from a stationary signal generator with a fixed directional antenna, with a transmitted power of maximum 20 W.
- Low effect jamming: Jamming transmissions originating from handheld jammer equipment (with isotropic antennas) available from the Internet, with a output power below 1 W.
- RFI – Radio Frequency Interference, external signals (or noise) that interfere with the radio frequency service in question.

2 Purpose

The purpose of Jammertest 2022 can be divided into three parts:

- To offer test areas for large scale GNSS jamming and spoofing in real world environments, in a controlled manner in surroundings with roads, diverse terrain, buildings (village level), etc. The participants would by this be able to test the accuracy, availability and resilience of their equipment, systems, new solutions, etc. By making these test cases available in an open and inviting environment, the organisers wanted to facilitate the innovation of new and more robust GNSS based or dependent technology.
- To raise the level of competency, awareness and understanding of the negative consequences of illegal GNSS jamming and spoofing, performed by private individuals as well as state actors, and to demonstrate vulnerabilities and resilience by portraying or refuting theoretical issues.
- To contribute to increase the visibility of proactive cooperation across authorities in the Norwegian government about a complicated problem (GNSS jamming and spoofing), in addition to display Norway as a country that accepts and confronts the challenges posed by jamming and spoofing, and a country where industry and others can conduct tests they not easily can do in other countries.

“Jammertest is an arena for experimentation. The arena gathers problem owners and problem solvers and will contribute so that industry and others are challenged to solve this important societal challenge. This should be done in close cooperation with the problem owners, the authorities, so that Jammertest can aid in closer future collaboration, attract relevant communities and assist in increased commercialisation of resilient technology.”

- Tomas Levin, Senior Principal Engineer, NPRA

Through exploring for example how jamming in different compositions (of radiated power, frequency bands and signal modulations) affect different technologies and technology stacks, one can investigate the different connections in the underlying systems and discover which parameters give what indications for which attacks.

The purpose of organising Jammertest 2022 at Andøya in particular, is the very special mountain formations here, creating very favourable conditions for minimising signal exposure to unwanted areas. It is also slightly remote, so that the tests cause minimal disruptions to air traffic and normal civilians.

An additional benefit of Jammertest was that by gathering as many as possible at Andøya, the need for other GNSS jamming tests other places in Norway would be reduced, thus diminishing the disruption to the society that such tests normally cause and the amount of bureaucratic work needed for them.

2.1 Norwegian PNT strategy (2018)

In the Norwegian government's strategy for PNT (2018), areas such as

- "exploit new opportunities and take care of Norwegian interest internationally",
- "contribute to raise awareness about PNT dependencies",
- "contribute to prevent disturbances and failures in PNT dependent systems",

and

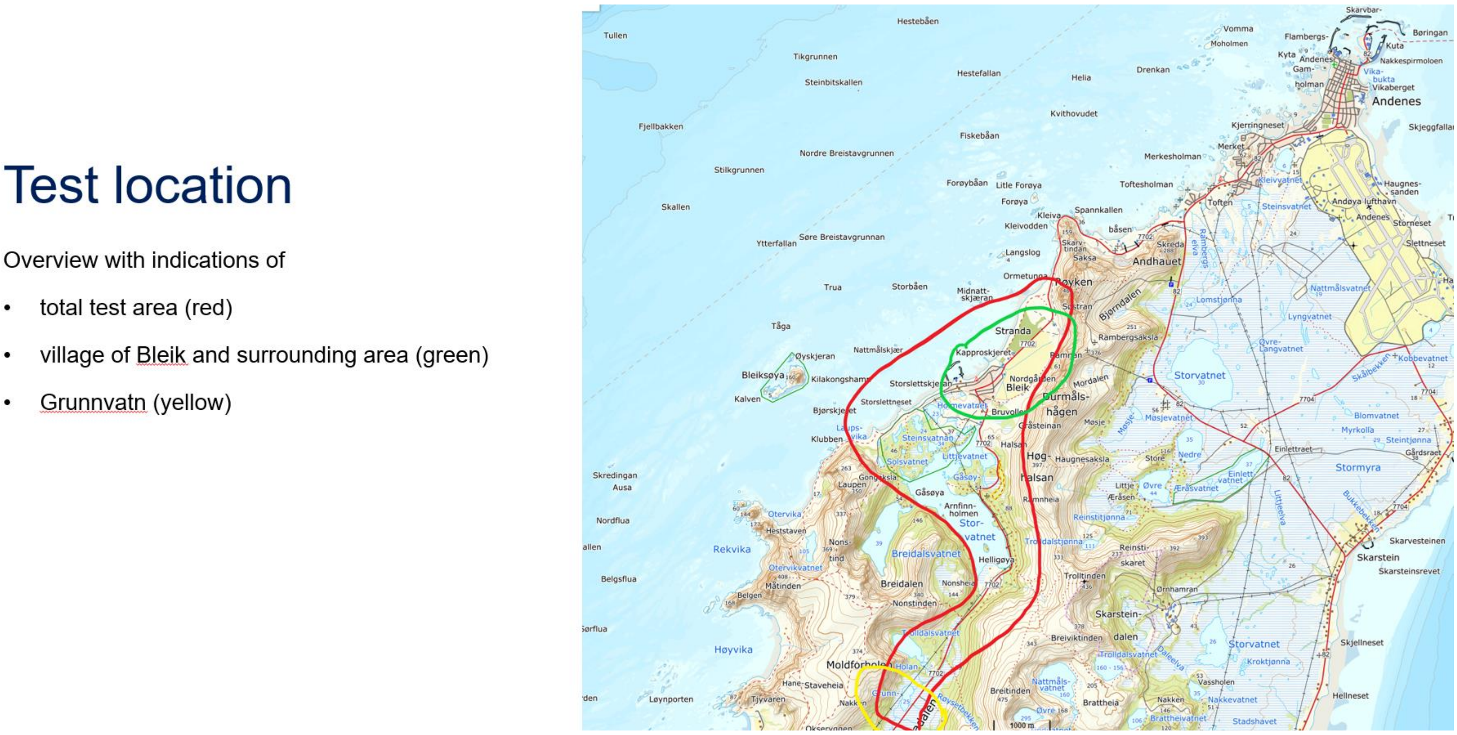
- "contribute to make sure that failures in PNT services don't propagate to cause critical outages in national infrastructure",

are all purposefully indicated as topics that both the government and the ministries wanted Norway as a nation to work on.

Jammertest 2022 contributes to achieving these goals through creating international cooperation on testing of already existing and new potential technological possibilities. This is done by communicating about the testbed's purpose and results, and aiding in the development of new and/or more robust PNT/GNSS solutions, making the nation and the world better at withstanding disturbances and failures in PNT based systems and services.

3 Overview of the test week activities[1]

3.1 Overview of test areas



Test location

Overview with indications of

- total test area (red)
- village of Bleik and surrounding area (green)
- Grunnvatn (yellow)

Figure 1: Map showing where at Andøya the tests were conducted.

As shown in Figure 1, the tests were conducted around the village of Bleik at Andøya in Northern Norway. The test area, where GNSS interference could be transmitted, is indicated with red. Within this area, the transmission equipment was mainly at two locations:

- The main test area (green), centered at Bleik graveyard and Bleik Community House.
- The secondary test area, by Grunvatn (yellow).

Additionally, vehicles were allowed to drive in the entire red area, while flying (mainly UAVs) were restricted to Bleik.

[1] For more information on jamming and spoofing attack methods, see Appendix 1.

3.2 Test program

Day	Activities
Monday (19th)	Part 1 (main test area): - Reference tests of low effect jammers (brought by Nkom and FFI); jammer 1 until jammer 14. - Reference tests of high effect signal types (generated by FFI); L1, G1, L2 and L5 in combinations of CW and PRN modulations (e.g. L1+G1 PRN). Part 2 (secondary test area): Long time jamming with a low effect jammer.
Tuesday (20th)	Part 3 (main test area): - Power ramp tests (sensitivity tests) with the high effect jammer, in different combinations of frequency bands and modulations. - Long time jamming with the high effect jammer and with the same reference setups as in Part 1. - Pyramid jamming with the high effect jammer. Part 4 (secondary test area): Jammers not in use in the main test area could be used "freely" by participants, under the guidance and supervision by a representative of the organisers.[2]
Wednesday (21st)	Part 5 (main test area): - Vehicle motorcade tests during long time jamming with the high effect jammer. - Vehicle motorcade tests with low effect jammers in and around the vehicles. Part 6 (secondary test area): Jammers not in use in the main test area could be used "freely" by participants, under the guidance and supervision by a representative of the organisers.

[2] Transmission of signals in frequency bands allocated for GNSS (satellite-to-earth-reception), or to needlessly disturb frequency use where GNSS share spectrum with other services, is illegal in Norway. Exceptions can be given to the armed forces or the Police, and then only with a granted frequency license from Nkom. During Jammertest 2022, FFI was legally allowed to conduct transmissions, since FFI was the holder of the frequency permission from Nkom. FFI delegated this legal right and responsibility to the other organisers' representatives in the field when a FFI representative was unavailable.

Thursday (22nd)	Part 7 (main test area): - Spoofing tests, with coherent and incoherent transmissions, with different combinations of initial and continuous jamming from low effect jammers. The spoofing tests targeted both position and timing. Part 8 (secondary test area): Jammers not in use in the main test area could be used “freely” by participants, under the guidance and supervision by a representative of the organisers.
Friday (23rd)	Part 9 (main test area and secondary test area): - Repeat of some previous transmission cases (such as low effect jammers and spoofing test). - New ideas, such as several low effect jammers at the same time in different setups in the terrain, new motorcade tests and jamming from the high effect jammer towards AIS-satellite (to test satellite detection capabilities).

Table 1: Summary of the activities conducted at Jammertest 2022, divided by day.

In addition, specific transmissions were done for the benefit of the one of the helicopters from the Norwegian Air Force’s SAR service.

4 Results

This chapter sums up some high-level observations from the tests, in addition to giving some examples of reported results. It does not give a complete description of all of the results from all the tests that the participants were able to conduct. However, it intends to give an impression of what types of results and experiences the participants brought with them back home after the test week. Additionally, it aims to give ideas to the reader on what kind of tests they themselves can run, or how the reader could research their own systems, to see if they experience the same type of problems.

The first subchapter, 4.1, aims to give some insight into the high-level observations. The two following subchapters, 4.2 and 4.3, gives two concrete, but anonymised, examples. Subchapter 4.4 is experiences not fitting into the previous subchapters and subchapter 4.5 gives contact information to some participants possessing measurement data they are willing to share.

– *Both users and industry get to test their navigation equipment in a realistic environment, where signals from GPS and other satellite navigation systems are disturbed, deceived or completely unavailable,* Anders Rødningsby (FFI) summed up for Inside Telecom 2022. [3]

4.1 High level observations

On a very superficial level one could say that it is quite obvious that some systems are much better prepared for jamming and spoofing attacks than others. Participants got some indications on what makes some systems more robust, and especially what the systems that were easily spoofed are missing. For example, by counterfeiting GNSS-signals – spoofing – cars that were parked on flat ground by Bleik started to show they drove around at the nearby mountain peaks. When the cars then started to drive, one could see the systems sensing something was wrong by trying to correct the map viewing, causing this to jerk and jitter, before (some car systems) reverting to the spoofed GNSS signals and continued showing the false, spoofed route.

One of the abovementioned indications were that some navigation systems are vulnerable because they rely too heavily on GPS than other GNSS. Systems that should be able to gain information from other satellite systems than GPS, and on other frequency bands than the ones jammed and/or spoofed, often weighted the GPS signal much more than the others, so that it could be deceived by for example only spoofing GPS (instead of for example having some sort of logical protection measures based on comparisons between all systems). Occasionally, the systems depended on satellite fix on at least one GPS satellite to be able to able to use the other non-jammed/-spoofed, not-GPS signals. Sometimes this was an embedded vulnerability, sometimes it was because of the system settings (where other settings than default could fix this). As one participant uttered: «If multi-constellation receivers are designed to be "reliant on" GPS L1, this is a serious matter that might reduce the resilience, making the use of multi-constellation receivers [somewhat] pointless». It should be noted that other multiband receivers did

[3] https://www.insidetelecom.no/artikler/omfattende-jammetester-pa-andoya/522377

default to non-spoofed signals when for example GPS L1 was jammed, so this seems to be equipment and system dependent.

In summation, one could say that multi-constellation receivers do give an increase in the robustness of the receiver in regards to RFI, yet it does not automatically give the safety that many maybe instinctively think, even towards simple GPS L1 jamming and spoofing. This will depend on the implementation choices made by everyone from the chip producers to the ones using the receivers in their systems.

Another interesting observation was that some receivers desperately try to keep GNSS-fix in RFI environments. This resulted in inaccuracies that could, for example, reach tens of kilometres, because the receivers rather tried to keep fix than to decide to not use the satellite signal in a non-healthy RF environment. Such results could be interpreted as spoofing, yet they are only a consequence of internal receiver processing. Additionally, the recuperation time for different receivers (and the systems they were implemented in) varied wildly. This mean that how much time they spent on regained fix after the RFI was turned off varied, and the variation was all over, from almost instantaneously, to a few minutes or never (a reboot was required to regain fix).

When it came to the two types of spoofing attacks, incoherent spoofing quickly turned out to be quite ineffective without the assistance of jamming, while coherent spoofing deceived most receivers (almost all unless they had protective measures from either smart implementation of other sensors or specially designed “firewalls”). Interestingly, many phones (also those with multi-GNSS chip sets) survived incoherent spoofing attacks as long as the A-GPS function (augmentation function to use cellular base stations to improve TTFF or accuracy) was activated. By deactivating this function, they were deceived by simple incoherent GPS L1&Galileo E1-only spoofing signals. If the spoofing was done coherently, the phones were deceived immediately, even with A-GPS activated. Variations were also observed in how fast receivers started to follow the spoofed signals (if at all), particularly as a function of the pre-existing RF environment, meaning how they were affected by initial jamming.

When it comes to timing, it was observed that simple GNSS controlled time servers would accept whatever spoofed GNSS signal they were fed, with variations in how much time it took for the different servers to lock onto the spoofed signal. More sophisticated equipment, with logical control mechanisms and/or comparisons towards other sources, would detect the spoofing and go into holdover (only use and trust an internal oscillator), meaning they survived the spoofing attack. Differences between equipment would appear here as well, as for example the same attack would affect the equipment differently, especially in the different phase transitions.

Another observation came when comparing high precision equipment, such as very sensitive geodetic surveying kits with more normal (and much cheaper) receivers, standalone or integrated in systems (like cars). The high precision equipment could be much more sensitive to RFI, caused maybe by the cheaper receivers being part of sensor fusions, or that cheaper receivers often accept a certain compromise with accuracy vs availability, while high precision equipment has the opposite tendency. Such compromises are often seen in phones, although those participants testing phones did experience that even low effect jammers could be surprisingly effective.

The same tendency between high precision equipment and cheaper receivers was also observed in regards to receivers’ ability to restore true PVT-solutions after a spoofing attack. Some receivers were pushed into irreparable conditions after the spoofing, for example causing one multi-GNSS receiver to slowly drift upwards after the spoofing was ended, never gaining fix on more than five Glonass satellites even several hours all jamming and spoofing had ended. This indicates that some receivers that (at least) do (have the technical possibility to) perform 'sanity checks' do not have a conceptual understanding of 'insanity checks'. Meaning that even though the RFI attack itself only lasted a few minutes, the effects of the attack can last hours(?), days(?) or until the system is completely rebooted(?).

The results of the Jammertest were also included in a government Concept Study on future road tolling models (such as GNSS road pricing), where relevant observations pointed out were[4]:

- A jammer onboard a vehicle will hinder GNSS signals for the evaluated onboard solutions, and additional positioning possibilities are therefore necessary.
- A jammer in a vehicle positioned in front or behind the test vehicle in question would not hinder the GNSS signals for the evaluated onboard solutions.
- A jammer in a vehicle passing in the opposite direction of the test vehicle in question does only cause disturbances in a short period of time, depending on speed, but usually only a few seconds.
- Spoofing of evaluated onboard solutions is considered so technical demanding (and proliferate so little) that it is not a relevant issue at this point in the Study.

As previously mentioned, jamming in and of itself can cause large position and timing inaccuracies, as the signal reception and processing is affected. The same observations were made when starting up or ending spoofing. When this was studied a bit further, it became obvious that the RFI phase transitions could cause unexpected results. Different phases in the attack can produce different results, and the results can linger even long after the RF environment is healthy again (and in some cases receivers never recovered). These transitions phases can be very unsafe places for GNSS receivers, even if they have well designed protection measures. The transitions happened between the phases 'no RFI' and 'RFI':

- The transition from no RFI to RFI → Initiating RFI
- The transition from RFI to no RFI → Discontinuing RFI

The issue seemed to be that many of the implemented protection measures were designed for the binary case *no RFI vs RFI*, and did not sufficiently work during the transitions. For example, it is not a given that GNSS controlled oscillators will enter holdover in a controlled manner when they start to experience RFI. In the transition period before protection measures has handled the RFI, instabilities and discrepancies could occur. If even short-lived instabilities or discrepancies are unacceptable, this could cause dangerous situations. Interestingly, this observation means that in some cases, weak jamming signals could be much more dangerous than stronger jamming signals, as they could prolong the transition period before protection measures and holdover conditions are properly enabled.

One observation that was made throughout, was that a lot of receivers equipped with jamming and spoofing protection measures could withstand many of the low effect jammers, but results varied quite

[4] https://www.skatteetaten.no/contentassets/343a9f921ade437c81482661e96320de/2022-11-5-3-vurdering-av-tekniske-losninger.pdf

a bit when it came to the effectiveness of these measures when they were presented with the high effect jammer.

For time servers, position spoofing was relatively unproblematic, but time spoofing could, to a varying degree, be quite drastic. This was especially true for more sophisticated attacks, like injection or removal of leap seconds. It was also observed that some protection measures could be fooled if the jamming and/or spoofing was active for a long enough time. One hypothesis for this behaviour is that the protection mechanisms started to perceive the disturbed RF environment as the new normal (since it had been active for a while), and the spoofing would then be seen as the new true signals. This way, the spoofing could spoof receivers even though the spoofing was detected (and stopped) in the beginning. Interestingly, some systems had to be rebooted after this affected them, since they never started to trust the real satellite signals again.

4.2 Example of observations

The following subchapter is a collection of examples of observations made by one participant, as they drove around in a vehicle with units made of GNSS modules and MEMS sensors. The units were from the same producer, with one of them being from the newest generation of GNSS receivers and the other from the previous generation.

When driving in a motorcade column with a L1 only jammer in another car and testing the newest unit, some degraded user experience was observed, but nothing major (it was a small drift in the movement track while the jammer was turned on, but the movement after that followed the correct movement, just shifted from the real track).

When meeting a L1 only jammer in a truck and testing the newest unit, all GNSS-reception disappeared for a few seconds, but no great PVT-accuracy loss was observed.

When driving with a L1 only jammer inside the vehicle and testing the newest unit, all GNSS reception was lost, and after around six minutes the inaccuracy had built up to around 150-200 metres. Further testing with other jammers inside the vehicle indicated results dependent on the different start up criteria, and especially dependent on the MEMS sensors being initiated or not. In one case, the unit managed to regain some GNSS fix and a PVT-solution, but with a degraded signal. In another case with another jammer, no GNSS fix was possible, but the PVT was still available thanks to the other sensors. This means, as already mentioned, that different jammers will (of course) results in different results.

The units were also exposed to spoofing. The vehicle was then parked in the vicinity of the spoofer antenna and the “goal” antenna (for coherent spoofing). When the two units, with GNSS fix and initiated sensors, was exposed to incoherent spoofing, the newest unit remained unaffected, while the older unit was spoofed (interestingly, the inaccuracy became very large during the transition period until successfully spoofed, see Figure 2 a)). If the car started moving, the newest unit remained on true track, while the older experienced inaccuracies in the beginning, which became very large before the it in the end ended up following the spoofed track (see Figure 2 b)). The early inaccuracies might also be from the spoofing being initiated with jamming. When the coherent spoofing started up while the vehicle was stationary, both units experienced some initial inaccuracy before being spoofed and followed the spoofed track. While moving, the newest unit was barely affected at all, while the older unit had different experiences depending on there being initial jamming or not: if initial jamming, it started to follow the spoofed track, while if no initial jamming, the track turned out to be a mix of the true and the spoofed movement (yet either not at the true or at the spoofed movement track).

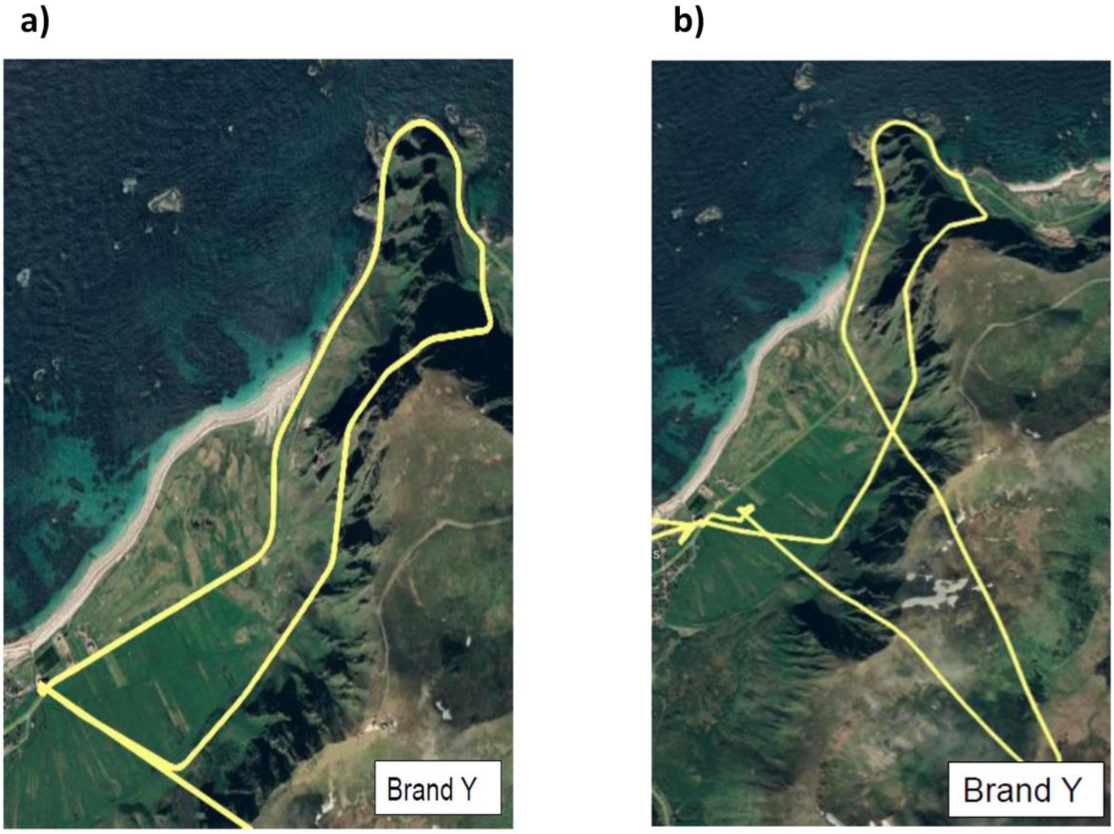


Figure 2: Older unit during a spoofing attack, with all MEMS sensors initiated before the attack. A) is when the vehicle is standing still, and b) is when the vehicle is moving. The spoofed track is clearly visible in a), expect for the straight line at the bottom.

This participant also made some assessments on detection: Jamming is easily seen in the spectrum, like in Figure 3. Spoofing is much harder, and there exists a lot of variation depending on what parameters are used in the detection algorithm (for example, the "spoofing detected" parameter from the GNSS chip did turn up when the spoofing started, but it disappeared long before the spoofing was turned off), and how long the spoofing was active (in the end, some detection mechanisms are fooled to believe that the spoofed environment is the new, healthy environment). Two receivers connected by a fixed distance is also an effective way to detect spoofing. Another observation was that AGC can be a useful parameter to detect spoofing, even though it is not as useful to detect jamming.

Some other thoughts on detection were well summarized by Harald Hauglin from the Norwegian Metrology Service: «*Basic spoofing signals used satellite data very different from those transmitted by the actual satellites and ought to be flagged as fake by sufficiently alert receivers. Advanced spoofing* *signals used data/ephemerides identical to those transmitted by the actual satellites and for some synchronized scenarios gave insignificant changes in position and timing at the target location. Even these more advanced spoofing signals may be detectable by fairly basic consistency checks (e.g. two antennas with a known displacement should not report the same position), robust multisensor fusion, RF spectrum analysis or by new authentication mechanisms such as Galileo OSNMA»*[5].

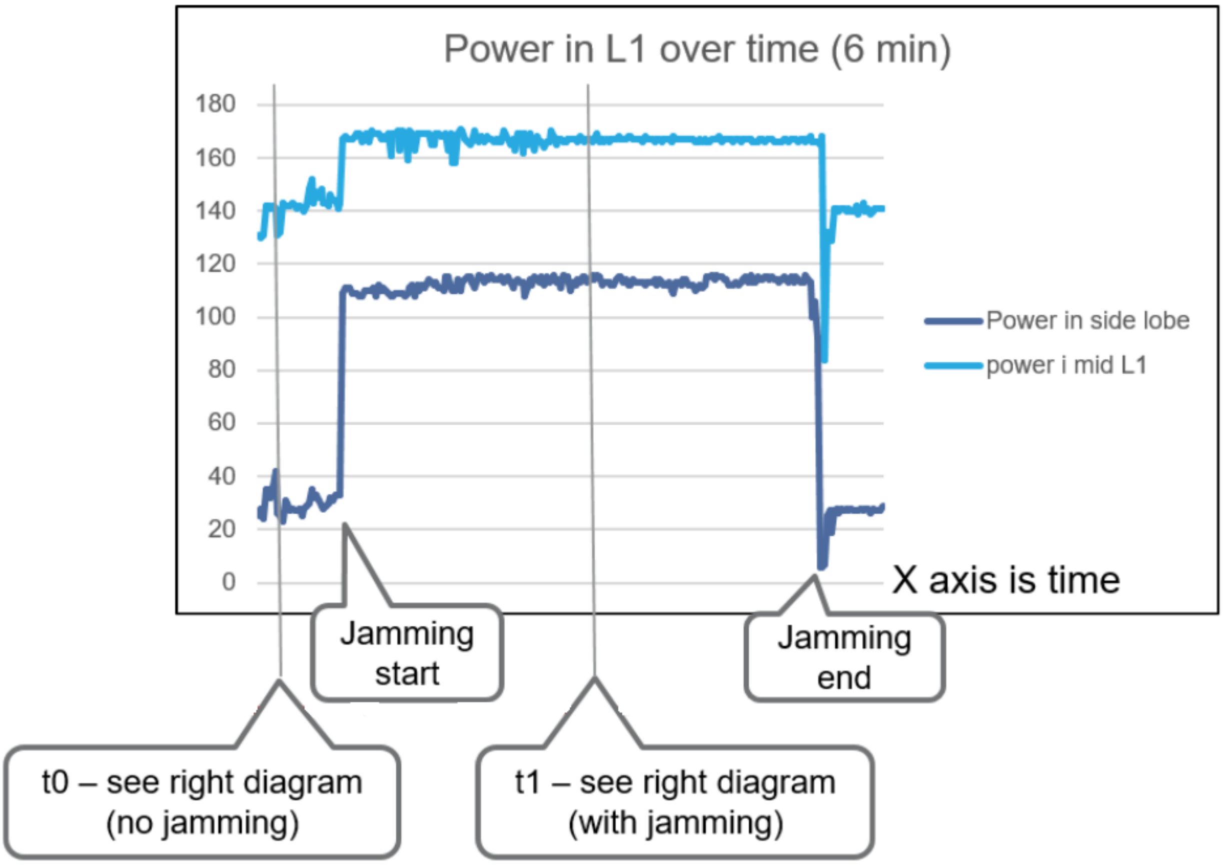


Figure 3: Spectrum measurement from a built-in spectrum analyser in the newest unit.

4.3 Example of tests on detection equipment

One participant tested commercially available GPS interference detection equipment from Chronos; CTL3510 and CTL3520. The units are designed to detect interference in a 20 MHz wide frequency band centred on 1575 MHz. Both units reacted well to being used to detect both jamming and spoofing, with all different modulations (like chirp, CW, PRN). What follows is a summary of the participants experiences from trying out this equipment during Jammertest 2022.

«CTL3510 is a user-friendly handheld, yet compact and versatile detector. Tests shows a practical range of approximately 50 meters if a 10 mW low-cost "eBay jammer" is used inside a car. It will record and

[5] https://www.linkedin.com/posts/harald-hauglin-3140a610_jammertest2022-galileo-osnma-activity-6979791066744934400-kAs0/?originalSubdomain=no

time stamp the measured levels to an internal file which can be downloaded through USB. The graph can be used later to document if jamming or spoofing signals were present at a certain time. A LED bar graph for relative signal strength indication is provided, as well as a switchable vibrate/alert function. Use cases may be covert operations and intelligence, or if carried by a public servant on everyday basis. CTL3510 has limited range but the value to the user is instant response if being near to a source.

During the high-power sessions, the CTL3510 triggered and showed approximately a half-scale level reading at the community house, 1100 meters away from the jamming transmitter site.

The CTL3520 was valuable to locate and eliminate any jammer, spoofing or noise signal on GNSS frequencies. With or without experience in radio direction finding, the product is quite intuitive in operation.

The received relative signal strength will be indicated through a LED bar graph. When approaching successively to the signal source, the built-in attenuator must be increased on the go to facilitate a max/min reading to properly determine the direction. The current attenuator setting is always visible.
By rotating and holding the locator vertically, it is possible to find the elevation in a higher structure or building. In one actual case, we found that the jammer was located inside a truck cabin, elevated only 2 m meters above ground level. Knowing the elevation will reduce the time used when locating a source.

Several ‘hide-and-seek’ of hidden jammer scenarios were carried out, and we were able to locate the hidden jammer in each case. The smaller CTL3510 was engaged in some of the tests, giving the user extra confidence in the locating process. Even during the high-power jamming sessions, we could apply the attenuation needed to determine the direction.

Tests show that the CTL3520 has a quite sensitive receiver. At maximum sensitivity, it is possible to determine the direction of an incoming signal from a 10 mW “eBay-jammer” at about 1 km. If the source is airborne, a significantly larger range applies.»

4.4 Other

Some defence industry participants could not share their results and experiences, yet as an example that the tests performed were useful for them as well, Teledyn Flir provided the following remark: «*The tests we were able to conduct at Andøya directly contributed to a new software that improved GPS denied and spoofing performance for the Black Hornet 3. The Black Hornet 3 with that software is being actively used in Ukraine.*»

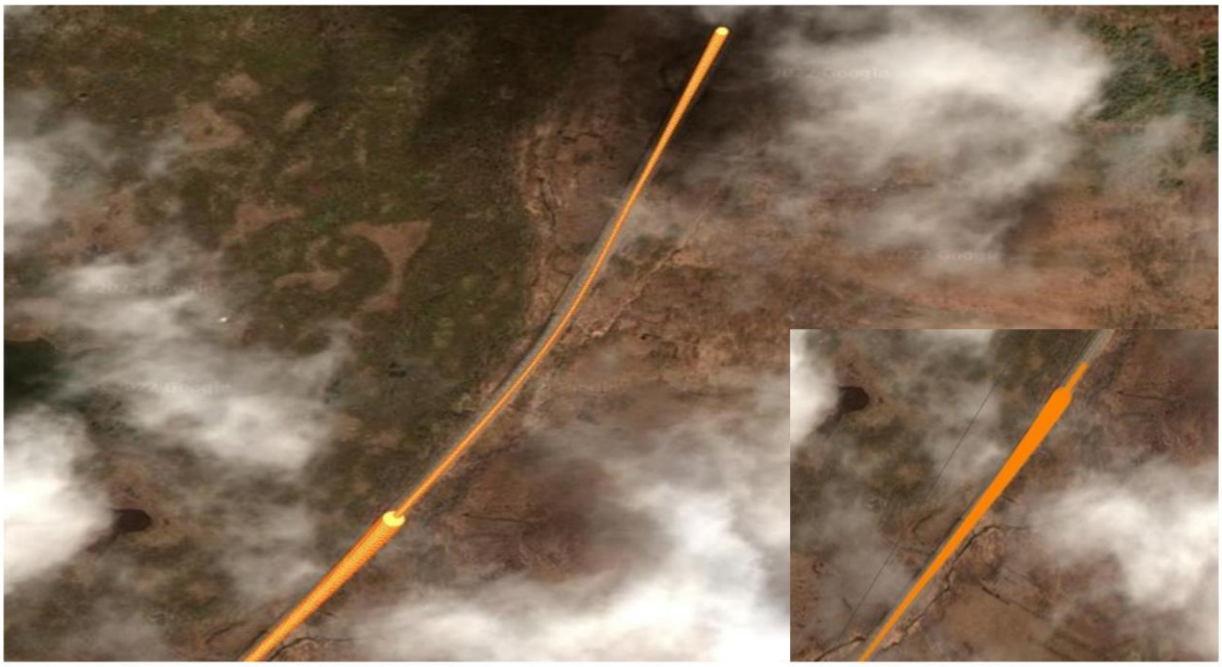


Figure 4: Example on how INS sensor inaccuracy accumulates over time when GNSS is lost, here in a vehicle driving along a road.

Additionally, the data capture campaigns carried out by some of the participants could potentially be very useful for others, in for example developing increased sensitivity when exposed to incoherent spoofing, improve false positive spoofing detections (the false movement being from jamming rather than from spoofing) and data on real jammers and on many different jamming signal types.

Some results from Jammertest 2022 are covered in the articles and posts described in Table 2.

Sak	Sted	Dato	Lenke
Interessante resultater: Nkom håper jammetesten på Andøya kan bli årlig	InsideTelecom	26.9.2022	Interessante resultater: Nkom håper jammetesten på Andøya kan bli årlig - Inside Telecom
Nyttige resultater etter jammetest	Nkom	28.9.2022	Nyttige resultater etter jammetest

Alle fikk problemer, så de var veldig fornøyde	vegvesen.no	28.09.2022	Alle fikk problemer, så de var veldig fornøyde
Nyttige resultater etter jammetesten	Security worldmarket	29.9.2022	Nyttige resultater etter jammetesten
World's Largest Jammer Test Held in Norway: Awaiting results	Resilient Navigation and Timing Foundation	28.9.2022	World's Largest Jammer Test Held in Norway: Awaiting results
First Results – World's Largest Jammer (& Spoofing) Test	Resilient Navigation and Timing Foundation	29.9.2022	First Results – World's Largest Jammer (& Spoofing) Test
JammerTest 2022: Unauthorized Jamming, Accidental Spoofing – GPS Patron discusses the event & results	Resilient Navigation and Timing Foundation	11.10.2022	JammerTest 2022: Unauthorized Jamming, Accidental Spoofing – GPS Patron discusses the event & results
JammerTest2022 Norway	GPSPatron	10.10.2022	JammerTest2022 Norway
Testet jamming og spoofing av navigasjonssignaler	Norsk Romsenter	21.10.2022	Testet jamming og spoofing av navigasjonssignaler
GNSS/GPS jamming and spoofing tests under actual conditions	Ublox	08.03.2023	GNSS/GPS jamming and spoofing tests under actual conditions
Norsk øvelse afslører at simpel GPS-jamming slår helikoptere og skibe ud af kurs	Ingeniøren	03.02.2023	Norsk øvelse afslører at simpel GPS-jamming slår helikoptere og skibe ud af kurs
Impact analysis of spoofing on different-grade GNSS receivers	IEEE	08.06.2023	Impact analysis of spoofing on different-grade GNSS receivers
Mitigating Jamming and Spoofing with Grit	Hexagon	2023	Mitigating Jamming and Spoofing with Grit (page 50 and onwards)

Table 2: News stories and posts on sites like Linkedin and company webpages on results from Jammertest 2022 (in Norwegian, English and Danish).

4.5 Access to measurement data sets

4.5.1 Nkom

The Norwegian Communications Authority (Nkom) has spectrum measurements (effect over time) of most of the high effect jamming signals, most of the low effect jammers and some of the spoofing signals. For access to these measurements, contact Nicolai Gerrard, nge@nkom.no.

4.5.2 Sintef

Sintef monitored and made recordings of most of the signals transmitted around the Community house. For access to their data set, contact Senior Research Scientist Aiden Morrison, aiden.morrison@sintef.no.

4.5.3 GPSPatron

GPSPatron did monitoring from several probes, where all their measurements are collected in their cloud. Their data set is available to everyone from https://jammertest2022.gp-cloud.io/, and access is given through this link: https://forms.gle/Wgjdu7WE4kASLamJ6.

5 Conclusion

Jammertest 2022 offered a civil, unrestricted, and open area for larger field tests of GNSS jamming and spoofing, something that is offered in few other places in the world (and then usually organised by the military). The tests and investigations made available possibilities to increase ones understanding and knowledge of GNSS RFI effects on systems and technology stacks, to discover new challenges not previously thought of or analysed, and to give a unique opportunity to do measurements and data capture of GNSS jamming and spoofing, in real environments.

Based on the feedback from participants, all the abovementioned possibilities were fulfilled, and with a strong wish (from more or less everyone participating) to repeat such tests in the future, for example with the motivation to test the measures implemented based on the results from 2022.

Such tests also allow government authorities to take more active steps towards ensuring the safety of GNSS from jamming and spoofing, more than just doing monitoring and notifications; the Jammertest concept facilitates the development of solutions more robust to ill-willed attacks, thereby enabling both industry and the sector as a whole to handle more RFI cases without the assistance from governmental entities (like Nkom). Additionally, Jammertest was a unique learning opportunity for authorities and participants, where insights into such things as vulnerabilities and system response were among the most prominent. The networking done and the learning arena made by the participating engineers, scientists and sector professionals turned out to also be extremely rewarding.

The organisers are of that opinion that the associated costs and work to arrange Jammertest was justified, compared to the advantages made for their own organisations, the Norwegian nation and for future GNSS equipment and systems.

A poll on the need and wish for a Jammertest 2023 was done twice, first during the Jammertest 2022 week and later as part of a digital evaluation. The response from the participants was in unison, they wanted a new Jammertest.

The organisers are therefore recommending repeating Jammertest in 2023, and that work should be done to make this a regular occurrence each year, as it obviously complies with a need expressed by industry, academia, government and important GNSS users (e.g. SAR).

5.1 Summary of observations

The satellite navigation systems in board a vehicle behave very differently from for example precise time servers. As both the margin of error and the consequences for the different systems differ, the GNSS implementation in the tech stack and the system response make it hard to say anything on a general basis. However, some high-level observations are to be considered:

- Multi-GNSS systems can be dependent on a reference constellation, so that attacks against this constellation alone can degrade the PVT-solution, even with other healthy constellations, and in some cases completely deny service.
- Jamming can cause spoofing like symptoms, illustrating that some receivers have very high fault tolerance (fault tolerance vs satellite fix).
- Different phases in the attack can produce different results, and the results can linger even long after the RF environment is healthy again (and in some cases receivers never recover). These transitions phases can be very unsafe places for GNSS receivers, even if they have well designed protection measures (usually made for the jamming/no jamming cases). The transitions are:
    - the transition from no RFI to RFI → Initiating RFI,
    - the transition from RFI to no RFI → Discontinuing RFI
- Incoherent spoofing works when systems have no or bad security barriers, and/or in combination with jamming.
- Coherent spoofing attacks work very well, and often did not need any jamming to succeed. Also, some multi-GNSS systems dependent on a reference constellation was completely spoofed by only spoofing that constellation, even though other constellations (and frequencies) were healthy and available.
- Even what looked like successful security measures could be spoofed if the spoofer was active for long enough (the new spoofed RF environment became the «real» environment, and when the healthy RF environment came back, this was seen as a new attack).

Appendix 1 – Jamming and spoofing attack methods

Jamming

The jamming conducted at Jammertest 2022 was from an assortment of low effect jammers (of the kind available online) and with a high effect jammer (SDR and directional antenna). The low effect jammers jammed GNSS frequency bands in the following combinations: GPS L1, GPS L1+L2, GPS L1+L2+L5, where all of them had an isotropic antenna and varying output power. The high effect jammer was a signal generator, capable of jamming all GNSS bands, with a right hand circular polarised directional antenna. The maximum output power from the signal generator was 20 W, and the modulations used where CW (Continuous Wave), and PRN (Pseudo Random Noise) with a P-code, BPSK (undefined satellite number) modulation. All these jamming signal possibilities were used in the activities described in Chapter 3. The frequency specifications for the PRN modulations are given in Table A1.

Jamming signal	Centre frequency (MHz)	BPSK modulation rate (MHz)
L1	1575,42	10,23
L2	1227,6	10,23
L5	1176,45	10,23
G1	1602	5,11
G2	1246	5,11
E5b	1207,14	10,23
B1I	1561,1	2

Table A1: Frequency details for the PRN BPSK modulated jamming signals.

Spoofing (as explained by Harald Hauglin of The Norwegian Metrology Service)

«The main difference between the spoofing activities of the session before lunch (‘basic spoofing’) and the session after lunch (‘advanced spoofing’) was the satellite data used (ephemeris data).

Basic spoofing (incoherent) uses other satellite data (meaning information on where the satellite is and what time the satellite clock is giving) than what a receiver would receive from real satellites. This means that the simulated satellites in the spoofed signals sent out other data that the real satellites did at the time of transmission (of the spoofing signal). This will create a “jump” in the receivers PVT-solution when it starts to lock onto the spoofed signals instead of the real satellite signals.

Advanced spoofing (coherent) simulated satellites sent out the same data about themselves that the real satellites sent out at the time of transmission. For some of our spoofing scenarios, the time stamp from the satellite (the time from the satellite clock) was synchronised with GPS system time, and the delays in our simulation chain was corrected to an error of only some tens of nanoseconds. For receivers close to our “goal antenna” [the antenna used to get an accurate starting spoofed position], this results in our simulated signals and the real signals containing more or less the identical information and are received with some tens of nanoseconds of each other. The aforementioned “jump” will now be essentially gone, and eventual built-in spoofing detection algorithms would be much more challenged to stop this kind of attack than an incoherent one.

We simulated only GPS L1 C/A and Galileo E1. »