Jammertest: The biggest open GNSS vulnerability test in the world

What is GNSS, why is GNSS important for road authorities, and, why in the world would anyone attack a service that we have come to depend upon?

Figure 1: Person blinded by a flashlight while looking up at the sky (AI Generated Copilot)

Sjefingeniør Tomas Levin,

Statens vegvesen

BACKGROUND

Global Navigation Satellite Systems (GNSS) is a common name for several satellite navigation systems which can tell users on the ground their exact position and time for the cost of a simple receiver casting around €200 or less. There are several varieties of GNSS systems; GPS the American system, Galileo the European system, GLONASS the Russian system and the Chinese BeiDuo.

As an oversimplification one can think of GNSS systems as super exact atomic clocks flying around in space, sending a simple message down to earth: I'm here (coordinates in space) and my time is X (accurate to 60-nanosecond range). By triangulating these signals based on the time and the location of the transmitting satellites, it is possible for the user to calculate their location in three dimensions1. The strength of the radio signal emittet can be compared to placing a 60-watt lightbulb at the distance of the moon and standing on earth looking up to see the light bulb. It is quite clear that a small light source on earth will quickly overpower the lightbulb in the sky. Shining a torch at someone who is looking up at the sky for the lightbulb is an example of jamming. The same can be done with the radio signals from the satellites.

But why should road authorities care about GNSS and potential vulnerabilities?

The answer lies in the digitalization of the road transport sector. In-vehicle navigation is one example, knowing where you are on the map is crucial for navigation. Micromobility services use GNSS so that riders can find the e-bikes, and for calculation of the cost of trips. There are also traffic safety related applications; Intelligent Speed Assistance (ISA) is a part of the type approval for new vehicles and allows for usage of speed limit data taken from maps. It requires that at least the Galileo systems must be used 2. Also E-call uses GNSS to establish where the vehicle is when the automatic emergency call is initiated 3. There are also many more applications that depend on GNSS to find the location of road vehicles: fleet management, road traffic monitoring, road user charging 4 just to mention a few.

In 2016, the Norwegian Public Roads Administration (NPRA) conducted an experiment using a consumer grade GNSS receiver to monitor interference close to the north bound lanes on E6 Moholtlia. The data showed evidence of jammers on Norwegian roads. The results were presented at the 2017 Posisjon conference in Oslo. In parallel, the Norwegian Communication Authority (Nkom) and Norwegian Defence Research Establishment (FFI) were doing similar but more advanced experiments along a different part of the E6. The Nkom and FFI study concluded that there is radio interference present on our road network 5.

Figure 2 Slide documenting GPS/GNSS jamming on E6 Moholtlia

The afore mentioned studies proved the presence of jamming on Norwegian roads. But little was known about the effect jammers may have on systems that use GNSS. The NPRA adhere to Vision Zero, meaning that no person should be killed or severely injured in the road transport system. Could jamming of GNSS cause deaths or serious injury? And is it possible to build knowledge and reduce vulnerabilities at the same time?

EARLY TESTING

On the 25th of October 2018, the NPRA, FFI and Nkom conducted a small-scale low power jamming experiment at E39 Øysand near Trondheim. According to Norwegian law, only Police and the Norwegian Armed Forces are allowed to transmit radio interference. This also means that industry actors have to tag along with the police or the military to test their equipment.

Figure 2: The first experiment where the NPRA was intentionally jammed

The results from the 2018 test at Øysand was inconclusive, to say the least. A total of three receivers were used. The navigation unit in the Skoda Superb, and two identical ublox M8 recievers, on placed on the vehicle in line of sight of the jammer and one in the building in the shadow of the jammer. The devices showed very different behavior. The built in receiver in the Skoda was quickly affected by low power jamming, most notably it reported being 318 meters under the surface before it stopped working. The receiver on the vehicle also quickly stopped working, not noticing much drift in location. The device on the building in the shadow of the jammer, traveled more than 6 million meters to the south before giving up. Different wave forms were also used, 2 of the 3 wave forms made the GPS give strange results. The data from the receiver indicated that it was not jammed while we were jamming it.

THE JAMMERTEST CONCEPT IS BORN

In September 2021 the first ever Jammertest was arranged on the E8 in the Skiboten vally. The learnings from 2018 was that GNSS applications, like the navigation unit in a car, should be seen as a complete software and hardware stack. And that at every level there is the possibility for something to go wrong. Hence, testing just a receiver is not enough. During 2 days at Jammertest 2021 three vehicles were subjected to jamming and GPS spoofing. All vehicles were successfully jammed and spoofed. Only one vehicle informed the driver that GNSS was lost or unreliable. But there were differences between how hard it was to make the vehicles loose their location or have them accept the false locations. One challenge was the low power used, under 1 Watt. The reason for the low power was that the broadcasted radio signal would reach into Swedish and Finnish airspace. The signal spreads upwards like a funnel, where the transmitting antenna is at the bottom. If more power was used the signal would reach into Swedish and Finnish airspace at an altitude of 30 000 feet.

Jammertest is a testbed where the authorities enable industry actors and other government agencies to test their systems under live sky combined with different jamming, spoofing and meaconing scenarios. The transmission of the signals is done by the authorities, and is a combined effort of FFI and the Norwegian Metrology Service (Justervesenet). The participants are given a test catalog and a transmission plan in advance. The test catalog contains all possible tests, while the transmission plan contains the time and location where a selected set of tests will be run. The test catalog and testplan are freely available on GitHub: https://github.com/NPRA/jammertest-plan The participants must plan their data collection and tests in accordance with the transmission plan.

For Jammertest 2022, 2023 and 2024 the location was shifted to Bleik at Andøya. The mountains east of Bleik are near vertical and stops the signal from penetrating eastwards. In the westerly direction the nearest country is Greenland, but the distance is so great that it will not be affected by high powered jamming of 200 watt. The island of Bleik also offers an extended stretch of roads that will be affected as well as stretch of sea were boats and vessels can navigate. For the NPRA having a road stretch that spans 7 kilometers with sharp turns and bumps that also drops in and out of the jammed area allows us to see how well vehicle manufacturer can use inertial navigation as a backup.

Jammertest last for 5 days, Monday to Friday, starting with simple jamming attacks on Monday and gets into advanced and novel timing attacks on Thursday. Friday is reserved for spare tests that need to be rerun due to issues during the other days. In 2023 a total for 247 tests were conducted. The number of tests in 2024 was lower due to request for longer test and longer grace periods between test to allow equipment to recover. Some equipment requires a complete power cycle to get back on line.

We choose to categorize the participants into three groups: industry, research and government. Figure 4 shows the logos of all participants in 2024, it is worth noting that industry actors range from GNSS chip manufacturers, to integrated products that use GNSS chips and end users of products that contain GNSS functionality. As part of the application process to participate we try to balance the actors to get a good mix of actors. In 2024 we had more than 300 applications to join Jammertest, 237 were allowed to take part.

Figure 3 Logos of organizations participating in the 2024 edition of Jammertest

RESULTS FROM JAMMERTEST

Jammertest in not unique in the world, there is NAVFEST conducted in the US by the United States Air Force (6,7), the uniqueness lies in that Jammertest is an open event with few requirements placed on the participants in relation to publishing of results. The Jammertest partners encourage sharing of results, talk and interact with other participants to promote learning in the whole GNSS community. This is reflected in the 4 points from "Jammertest code of conduct":

- We want this to be a week of working together, learning and having a good time !
- No requirement to share findings, but we strongly encourage you all to share as much as possible during Jammertest, and also, publishing your results
- Friendly, inclusive and informal atmosphere; be friendly, respect each other's boundaries, be curious and, last but not least, help each other, we are quite close to the end of the earth
- Taking photos is generally allowed, but if you take pictures with persons or equipment in focus ASK first!

On Thursday evening there is an evening of "sharing is caring", where participants are invited to share heir exiperiance, learnings and anything

else. In 2024 a total of 102 slides were provided to the organizers.

WHAT HAS THE NPRA LEARNED SO FAR?

The first takeaway from Jammertest is that equipment behaves in different ways when subjected to the same attacks. A typical pattern we have seen in low-end GNSS recievers based on own tests and talking to other participantes is that position error increases when subjected to jamming and lasts a while after attacks, as illustrated in Figure 5. On some maritime recievers we have also seen a need for a compleat power-cycle to the GNSS recievers online after being subjected to jamming.

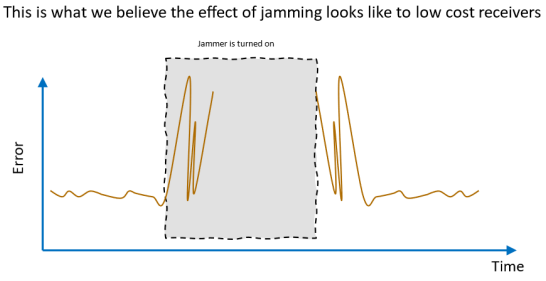

Figure 5 Effect on errors when subjected to jamming

Jammertest is a cat and mouse game where industry, research and government agencies have to continuously improve to catch up or be ahead of those that do not wish us well. Hence there is a need for Jammertest in the years to come. How Jammertest is run and organized is expected to change with time in relation to existing threats and the geo-political environment. At the moment parts of Norway being jammed is the new normal (8). And there was also an incident at Jammertest 2024, where one of the cables used by Jammertest was damaged and is being investigated by the Norwegian police (9,10). The 6 partners behind Jammertest believe that Jammertest is a good contribution to making GNSS usage more robust and in the end, even safer.

For more information on Jammertest see: Jammertest.no.

BIBLIOGRAPHY

1. Zogg, J. M. & U-Blox. GPS: Essentials of Satellite Navigation : Compendium : Theorie and Principles of Satellite Navigation, Overview of GPS/GNSS Systems and Applications. (U-Blox, 2009).

2. Regulation (EU) 2021/1958. Commission Delegated Regulation (EU) 2021/1958 of 23 June 2021 Supplementing Regulation (EU) 2019/2144 of the European Parliament and of the Council by Laying down Detailed Rules Concerning the Specific Test Procedures and Technical Requirements for the Type-Approval of Motor Vehicles with Regard to Their Intelligent Speed Assistance Systems and for the Type-Approval of Those Systems as Separate Technical Units and Amending Annex II to That Regulation (Text with EEA Relevance)Text with EEA Relevance. (2021).

3. Regulation (EU) 2015/758. Regulation (EU) 2015/758 of the European Parliament and of the Council of 29 April 2015 Concerning Type-Approval Requirements for the Deployment of the eCall in-Vehicle System Based on the 112 Service and Amending Directive 2007/46/EC. OJ L vol. 123 (2015).

4. European Global Navigation Satellite Systems Agency. EGNOS and GALILEO for ITS and ROAD TRANSPORT. (2017).

5. Gerrard, N., Rødningsby, A., Morrison, A., Sokolova, N. & Rost, C. GNSS RFI Monitoring and Classification on Norwegian Highways – An Authority Perspective. in 864–878 (St. Louis, Missouri, 2021). doi:10.33012/2021.17952.

6. GNSS, I. NAVFEST: 20 Years of Cost-Effective GPS NAVWAR Testing. Inside GNSS - Global Navigation Satellite Systems Engineering, Policy, and Design https://insidegnss.com/navfest-20-years-of-cost-effective-gps-navwar-testing/ (2024).

7. GNSS, I. NAVFEST: As Real as it Gets - Inside GNSS - Global Navigation Satellite Systems Engineering, Policy, and Design. NAVFEST: As Real as it Gets - Inside GNSS - Global Navigation Satellite Systems Engineering, Policy, and

Design https://insidegnss.com/navfest-as-real-as-it-gets/.

8. Svendsen, M. Sluttet å registrere GPS-forstyrrelser i Finnmark: – Uønsket normalsituasjon. https://www.forsvaretsforum.no/andoya-finnmark-jamming/sluttet-a-registrere-gps-forstyrrelser-i-finnmark-uonsket-normalsituasjon/395824 (2024).
9. Staalesen, A. Military experts suspect sabotage at Andøya. https://www.thebarentsobserver.com/security/military-experts-suspect-sabotage-at-andoya/166701.
10. Svendsen, M. Mistenker sabotasje på stor sikkerhetstest: –Bekymra for at det kan skje igjen. https://www.forsvaretsforum.no/andoya-ffi-forsker/mistenker-sabotasje-pa-stor-sikkerhetstest-bekymra-for-at-det-kan-skje-igjen/394932 (2024).