

Jammertest - concept, plans and some results

Anders M. Solberg, Norwegian Mapping Authority (NMA).

Credits for content to the Jammertest partners (listed on the last slides).

NKG Summer School, Tartu, 28 August 2025.



Kartverket

Outline

1. The Jammertest concept – background and philosophy
2. High-level technical information about Jammertest
 - Test areas
 - Attack vectors applied
 - Technical documentation
 - GNSS reference data
 - General findings from previous Jammertest events
3. Some NMA results from a low-cost Multi Constellation Dual Frequency receiver (2023) (presented at NNF seminar, Oslo, 12 June 2024)

Jammertest

«An open GNSS interference test arena to accelerate the development of resilient GNSS applications»



Statens vegvesen

Justervesenet



Norsk Romsenter
Norwegian Space Agency



Kartverket



Nasjonal
kommunikasjons-
myndighet

FFI Forsvarets
forskningsinstitutt
Norwegian Defence Research Establishment

TESTNOR

AVINOR

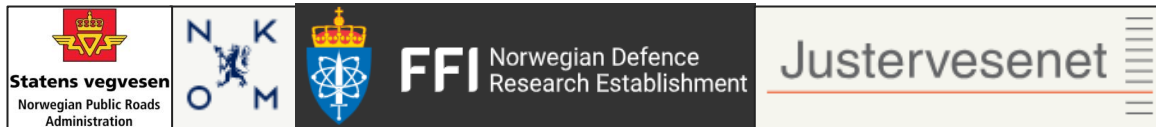
Background

- GNSS is a fantastic PNT enabler, but its radio signals are weak → Vulnerable to RFI
- PNT information is often an “invisible” resource, used in other systems → a lot of dependencies of GNSS in different sectors
- The needs for testing were expressed in discussions in a forum of Norwegian authorities through the years 2018-2020

→ Pilot test event in 2021



- Promising results and feedback from the pilot test event
→ Jammertest, September 2022: Full week of of operative GNSS interference testing at Andøya (4 organisers)



- Success and growing interest. Jammertest repeated in 2023 and 2024 with a rapidly growing number of participants, and eventually with some more organising institutions.



The philosophy of Jammertest

Jammertest is founded on the following “key values”:

- Facilitation
 - Offer a location where GNSS RFI signals can be transmitted in orderly forms without large disadvantages for society
- Transparency and openness
- Cooperation
- Resilience building over time
- An alternative to strict regulation



Photo: David Jensen

Facilitation

Regulation and enforcement of signal transmissions in GNSS frequency bands for anything else than space-to-earth radionavigation is (fortunately) extremely strict. In most countries, only very few exceptions are made, and then mainly for military exercises.



→ Lack of testing opportunities

+

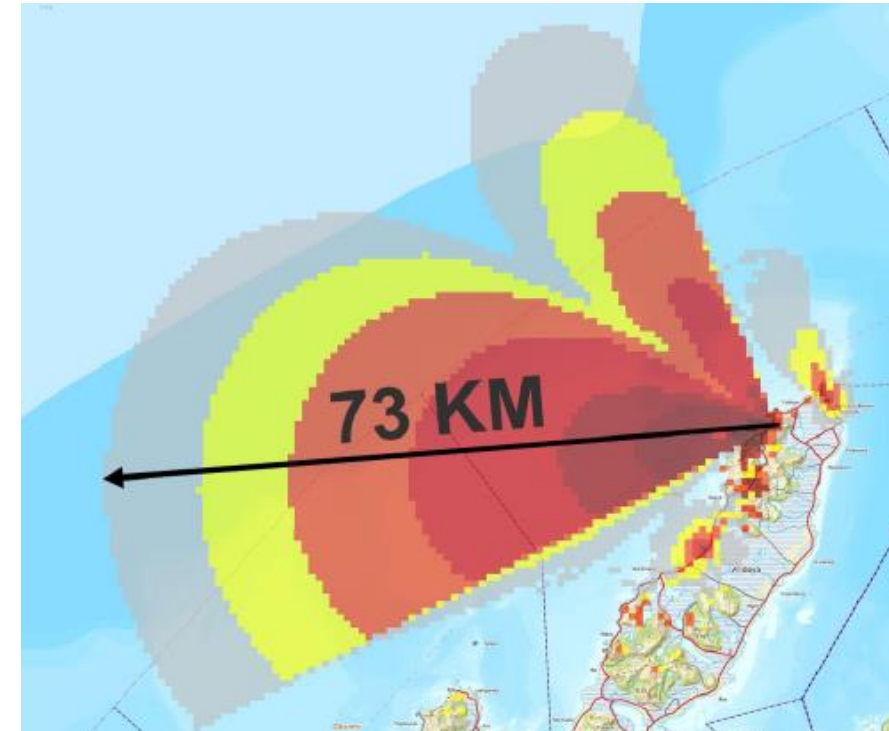
Growing need for testing. Lab testing is sometimes too clean/synthetic, and/or too physically restrictive (e.g. driving cars, flying helicopters).



=

Motivation for a test event.

Need for a location where GNSS RFI transmissions can be done with minimal disadvantages for society, while the location is still fairly accessible (travel, accommodation, HQ building, electrical power, internet, mobile phone coverage).



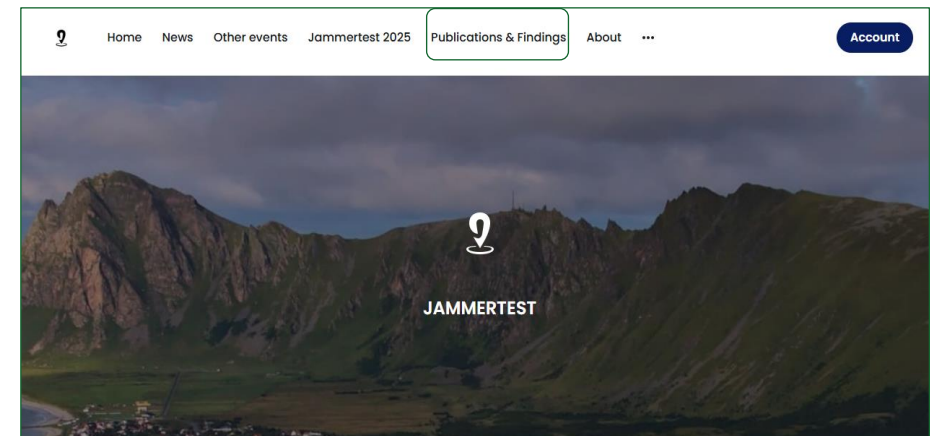
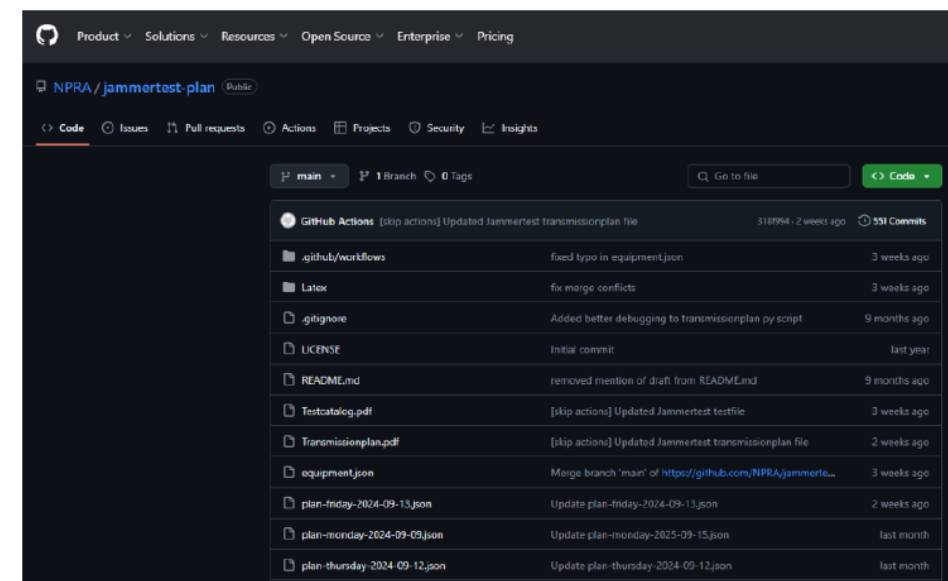
Why Andøya?

- Mountains to the east of the village of Bleik → mainland Norway shielded
- > 900 km to nearest neighbour to the west across the ocean (Jan Mayen)
- Tourist destination in summer (accommodation available in September)
- Airport available
- Local inhabitants are used to military and restrictive activities (e.g. rocket launches)



Transparency and openness

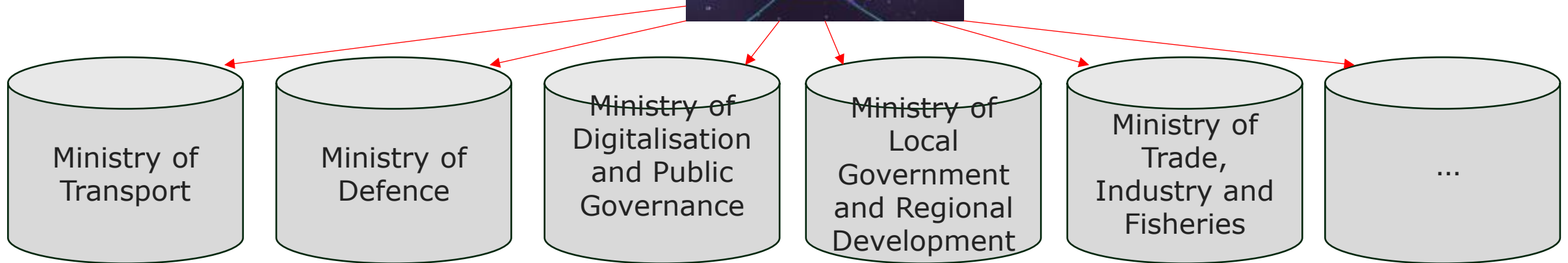
- All test-related information (technical and practical) is first shared with participants, then archived on the official website <https://jammertest.no>
- The development of the Test Catalogue (TC) and Transmission Plan (TP) is public, with documents available in both JSON and PDF formats on the Jammertest GitHub.
- The planning process is open to contributions, and after each Jammertest, technical details like the TP, TC, and logs are published.
- Participants are free to use their own recorded data without restrictions. While sharing is encouraged to support the broader community, only acknowledgements in publications are requested.
- A library of public results is also maintained on the official website.



Cooperation

Governance of many countries is sector based.

Vulnerabilities of PNT systems can affect several sectors, but who should take action to mitigate the risks?



- Jammertest raises cross-sectorial awareness of RFI threats against PNT systems.
- Organic development of roles and responsibilities, aligned with each organiser's strengths and expertise
- Participants' contributions are also important (requests/ideas for new/modified tests, ...).

Resilience building over time

- Being an annual event where several tests are repeated year after year, Jammertest provides the opportunity to test and validate improvements to equipment, systems and algorithms against the same RFI environment, so that the value of these improvements can be assessed.

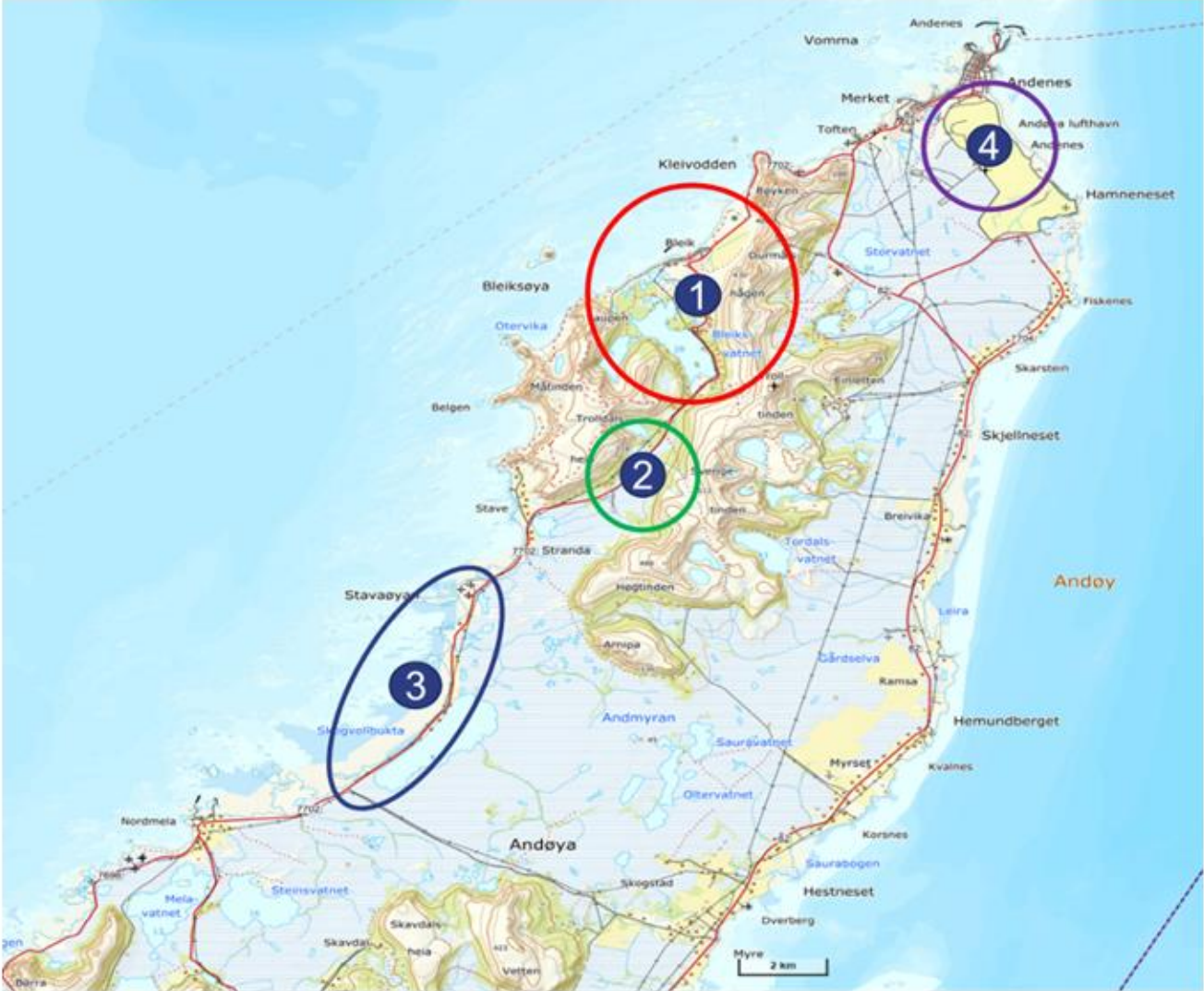
An alternative to strict regulation (of receivers)

- Strict regulation of receiver equipment → Difficult for legislation to keep up with the technical innovation speed.
- Some overall goals of Jammertest:
 - There should be no place in the market for devices and services that are not resilient to GNSS RFI.
 - It should be a main selling point that your product has survived Jammertest.

Outline

1. The Jammertest concept – background and philosophy
2. High-level technical information about Jammertest
 - Test areas
 - Attack vectors applied
 - Technical documentation
 - GNSS reference data
 - General findings from previous Jammertest events
3. Some NMA results from a low-cost Multi Constellation Dual Frequency receiver (2023) (presented at NNF seminar, Oslo, 12 June 2024)

-




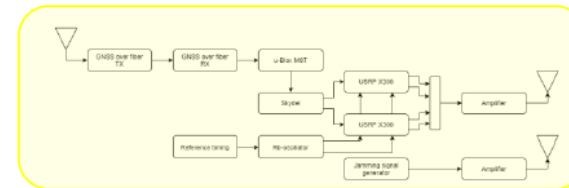
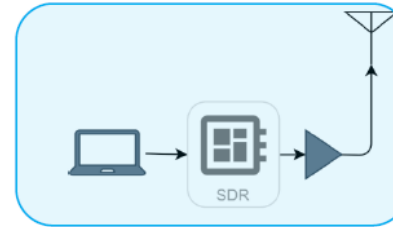
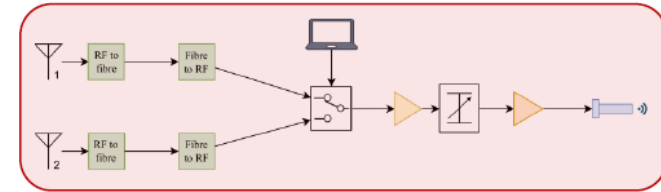
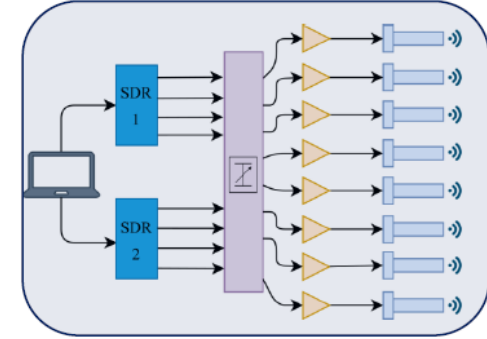
Attack vectors at Jammertest

GNSS RFI transmissions

Transmission group
<i>Stationary high-power jamming</i>
<i>Stationary low-power jamming</i>
<i>Mobile low-power jamming</i>
<i>Stationary spoofing</i>
<i>Stationary meaconing</i>
<i>Mobile spoofing</i>

Generated with:

- Porcus Major – The big jammer
 - Porcellum – The meaconing system
 - Mobile SDR Spoofer
 - “Low-power” jammers
 - Stationary Spoofer
- 



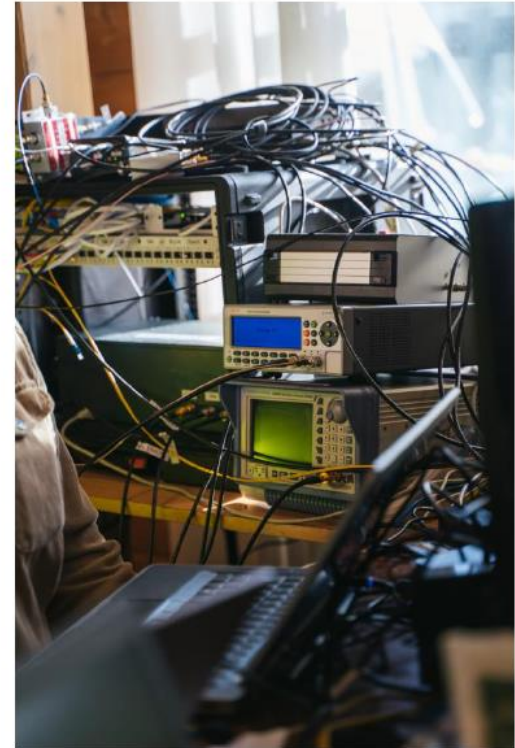
Attack vectors at Jammertest

GNSS RFI transmissions

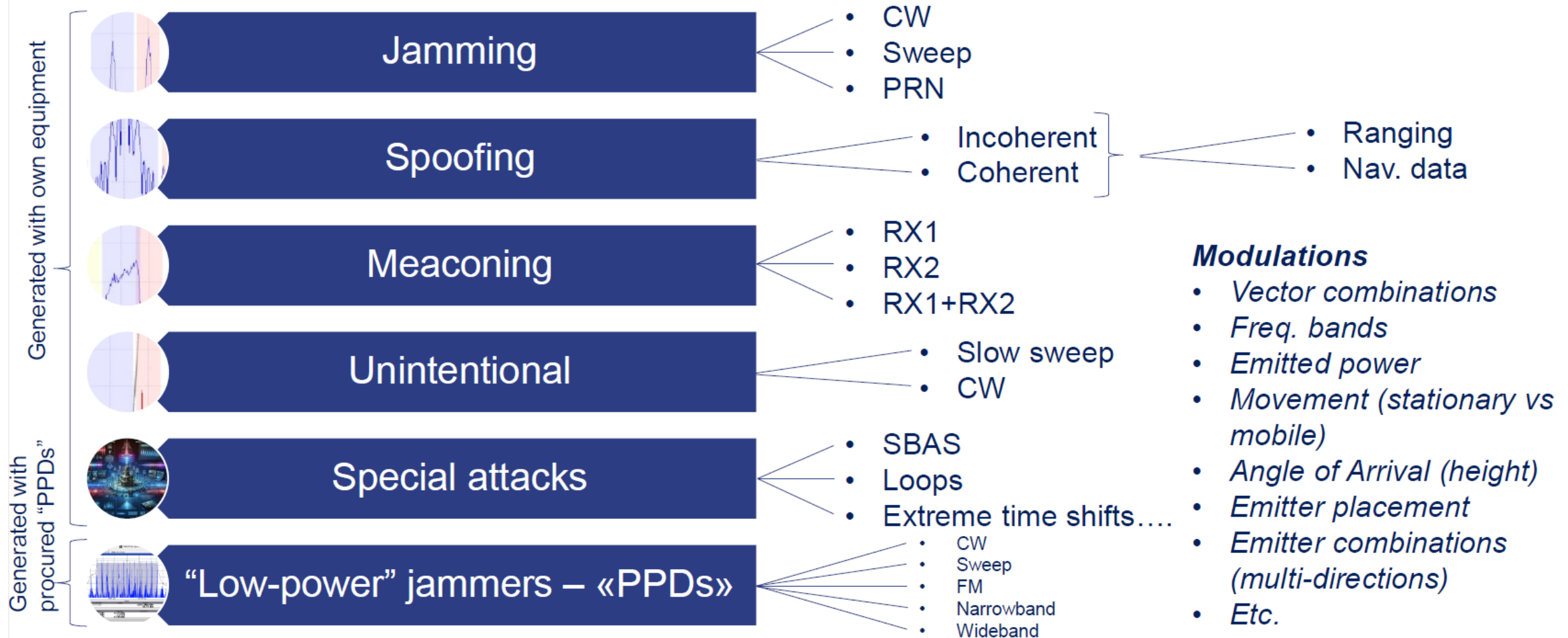
Transmission group
<i>Stationary high-power jamming</i>
<i>Stationary low-power jamming</i>
<i>Mobile low-power jamming</i>
<i>Stationary spoofing</i>
<i>Stationary meaconing</i>
<i>Mobile spoofing</i>



Photo: David Jensen



The Attack Vectors



Jammertest: Test catalogue, transmission plan and test log

Test catalogue of GNSS interference scenarios

2.4: Incoherent time spoofing from stationary spoofer using synthetic ephemerides	92
2.4.1 Time offset 15 minutes from real time. GPS L1 and Galileo E1 only, with power ramp	93
2.4.2 Time offset 15 minutes from real time, with power ramp	93
2.4.3 Time offset -3 minutes from real time, with power jump	94
2.4.4 Static + Frequency step. GPS L1 only	94
2.4.5 Static + Frequency step. GPS L1 and Galileo E1 only	94
2.4.6 Static + Frequency step. GPS L1 and Galileo E1 only, with initial and continuous jamming	95
2.4.7 Static + Frequency step	95
2.4.8 Static + Frequency step, with initial and continuous jamming	96
2.4.9 Static + Pseudorange error. GPS L1 only	96
2.4.10 Static + Pseudorange error. GPS L1 and Galileo E1 only	96
2.4.11 Static + Pseudorange error. GPS L1 and Galileo E1 only, with initial and continuous jamming	97
2.4.12 Static + Pseudorange error	97
2.4.13 Static + Pseudorange error, with initial and continuous jamming	98

A subset of catalogued tests are actually transmitted



Transmission plan 2024

09:00	09:00-09:25 - 2.4.2 Time offset 15 minutes from real time, with power ramp Power: 0.0316W Contact: Nicolai Gerrard (NKOM)
	09:40-09:55 - 2.4.3 Time offset -3 minutes from real time, with power jump Power: 0.0316W Contact: Nicolai Gerrard (NKOM)
10:00	10:10-10:25 - 2.4.12 Static + Pseudorange error Power: 0.0316W Contact: Nicolai Gerrard (NKOM)
	10:40-10:55 - 2.4.13 Static + Pseudorange error, with initial and continuous jamming Power: 0.001W Contact: Nicolai Gerrard (NKOM)

Test documents are machine readable (.json + .xls) to help automated data collection and analysis



Log of actual transmissions

2.4.13	Static + Pseudorange error, with initial and continuous jamming	2024-09-12	10:50:08	10:50:21	Initial jamming (E6, L2, E5b, L5)
2.4.13	Static + Pseudorange error, with initial and continuous jamming	2024-09-12	10:50:21	10:55:19	Jamming of L1, G1, B1I activated
2.4.13	Static + Pseudorange error, with initial and continuous jamming	2024-09-12	10:55:19	10:55:23	Spoofing activated. Spoofing power different than TP
2.4.13	Static + Pseudorange error, with initial and continuous jamming	2024-09-12	10:55:23	10:55:24	Jamming of E5b deactivated
2.4.13	Static + Pseudorange error, with initial and continuous jamming	2024-09-12	10:55:24	10:55:25	Jamming of L5 deactivated
2.4.13	Static + Pseudorange error, with initial and continuous jamming	2024-09-12	10:55:25	10:55:26	Jamming of L2 deactivated
2.4.13	Static + Pseudorange error, with initial and continuous jamming	2024-09-12	10:55:26	11:05:21	Jamming of L1 deactivated. Time error of 9 ns/s. A total accumulated time error of 6 µs

New features at Jammertest 2025



- More high-power tests that include jamming of the E6 frequency band
- High power jamming from two different locations (and therefore different elevation and azimuth angles) at the same time
- Spoofing tests in Test Area 2
- Jamming tests designed for drones in Test Area 2
- Tests with drone with jammer onboard in Test Area 2 (DTU conducted a related special test in 2024)

GNSS reference data

NMA (Kartverket) provides GNSS reference data based on geodetic grade receivers free of charge for participants during the Jammertest week.

2 options for RTCM formatted real-time data:

- CPOS (NRTK service). Requires NMEA input from user equipment.
- RTCM data streams from individual GNSS reference stations nearby the test areas (distances \sim 10-60 km)

Stored data for post-processing:

- RINEX (v3.05) files from individual GNSS reference stations nearby the test areas (distances \sim 10-60 km)
 - 1 Hz data rate
 - Choose between 1hour and 24hour files

Important findings from Jammertest

- Many defense mechanisms are based on insufficient assumptions
 - E.g. a too “binary” handling of interference → Transition phases (from undisturbed to disturbed or vice versa) can cause problems
- Source dependencies in sensor fusion (GNSS weighted too heavily) → problems, even though non-GNSS sensors are also used
- Some attack vectors are fairly simple, but have been totally overlooked by industry
- GNSS RFI can have effects looking like cyber attacks (licences can be outdated etc.)
- Lots of learning when problem owners and problem solvers are gathered
- The systems need to be tested! Assumptions and manufacturers’ statements regarding their products can sometimes be defective.

*Text taken from “Trusselens omfang” (eng.: “The extent of the threat”). Nicolai Gerrard, NKOM.
Presented at FFI breakfast meeting, Oslo, 18 March 2025*

Outline

1. The Jammertest concept – background and philosophy
2. High-level technical information about Jammertest
 - Test areas
 - Attack vectors applied
 - Technical documentation
 - GNSS reference data
 - General findings from previous Jammertest events
3. Some NMA results from a low-cost Multi Constellation Dual Frequency receiver (2023) (presented at NNF seminar, Oslo, 12 June 2024)

NMA at Jammertest 2023

People:

Carl H. Ellingstad and Anders M. Solberg

Equipment:

- Geodetic GNSS receiver: Leica GR50 with LEIAR20 antenna
- **2 mass market GNSS receivers:**
 - **u-blox ZED-F9P standalone SPP**
 - **u-blox ZED-F9P connected to CPOS NRTK service**
 - **Both using the same u-blox ANN-MB-00 antenna**
- GNSS antennas, tribrachs, 5/8" adapters, tripods, antenna cables → Static data collection
- Indoors storage and operation of the receivers
- High-effect jammer located about 1.1 km away



U-blox ZED-F9P



17.0 mm x 22.0 mm x 2.4 mm

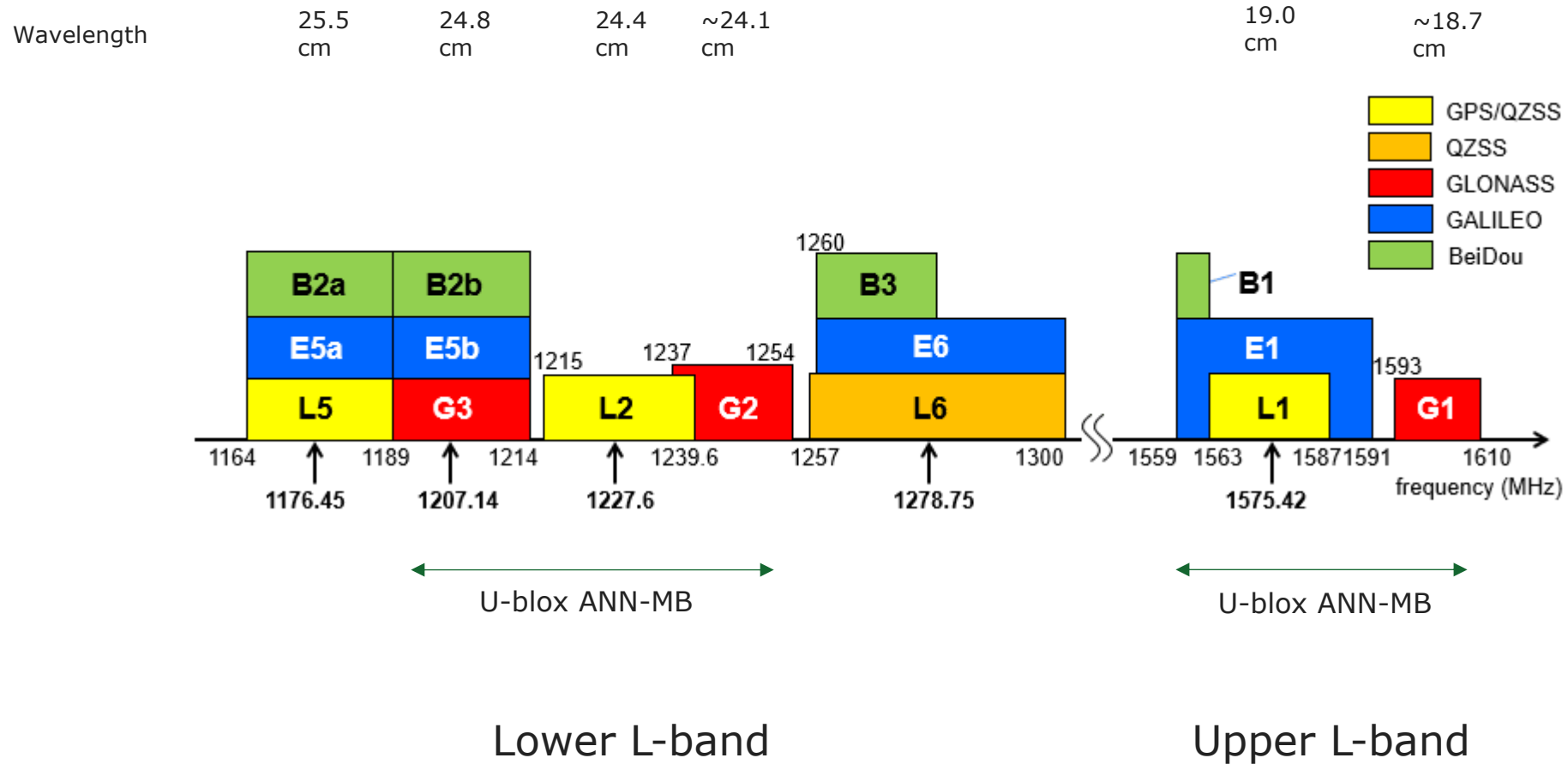


Antenna:
U-blox ANN-MB
82 mm x 60 mm x 22.5 mm

Multi-frequency GNSS receiver which track signals from all the big 4 GNSS (~2 frequencies per GNSS)

- GPS, GLONASS, Galileo, BeiDou
- L1C/A, L2C, L1OF, L2OF, E1-B/C, E5b, B1I, B2I
 - Restrictions on the dual-frequency capability:
 1. Only 24 out of 31 GPS satellites transmit L2C (Sep. 2023)
 2. B2I (old signal type) is only transmitted by the quite few BDS-2 satellites
- Able to track SBAS signals
- Able to work as an RTK rover
- Able to use the U-blox' own SSR service PointPerfect, or other SSR services that transmit data in the SPARTN format
- Maximum of 32 satellites at a time are used for PVT computation (not really a problem).

GNSS signal frequencies



Effects on U-blox F9P positioning, JT 2023

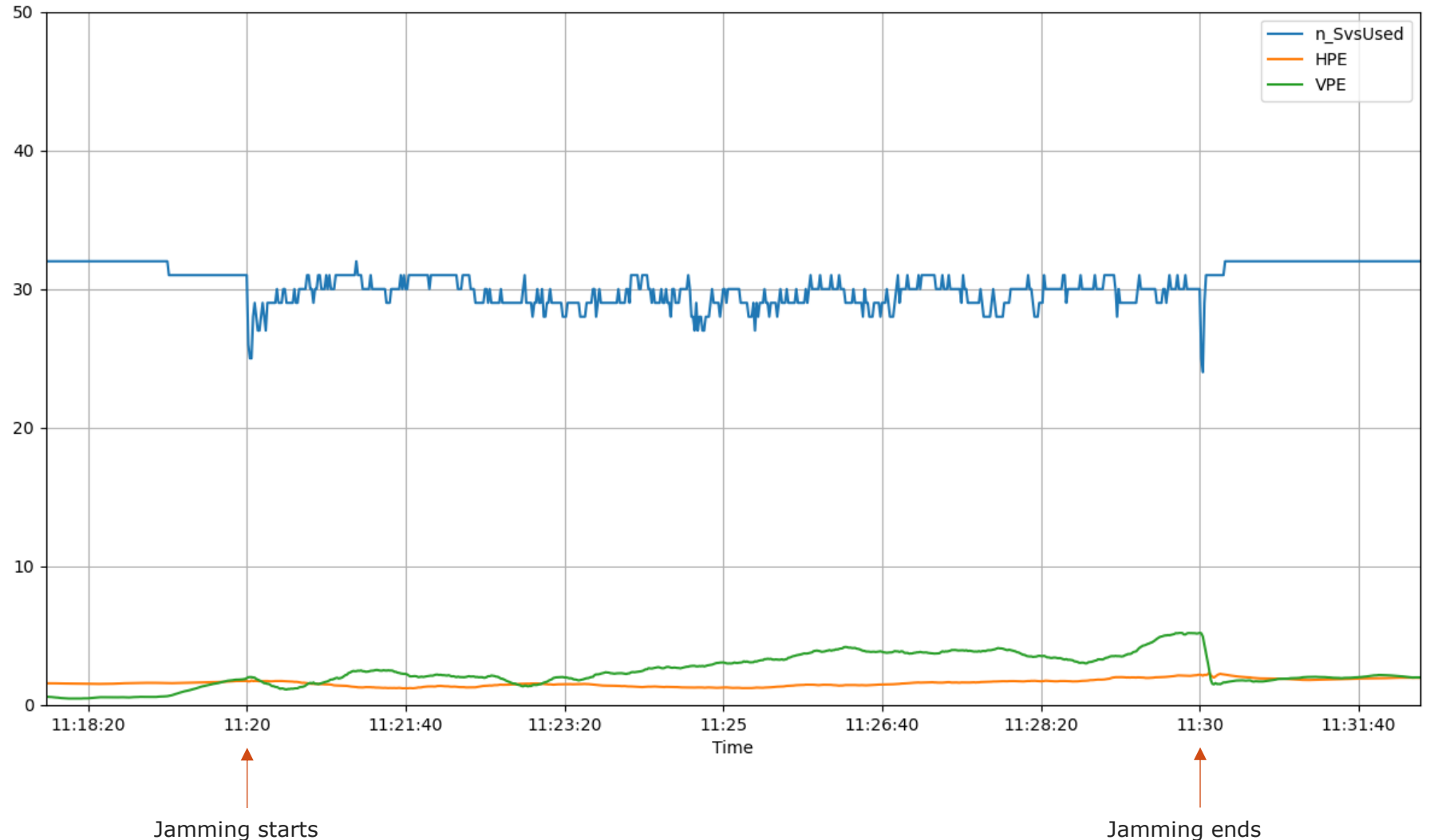
- On the following slides, example results from the U-blox ZED-F9P standalone receiver are shown.
- This receiver type is assumed to be relevant for automotive applications.
- U-blox outputs text (NMEA 0183) formatted positioning data and metadata together with binary data in .ubx files (a bit messy in my opinion)
- We have focused on the NMEA 0183 data.
- Very simple analysis:
 - Plotting time series: Position deviations, number of satellites used in positioning
 - Looking for abnormal behaviour
 - Inspecting metadata (estimated standard deviations etc.) if necessary
- All position deviation numbers in the following plots are in the unit **meters**

High-power jamming 20 W, 1.1 km away (page 1)

18 Sep, 11:20 – 11:30 UTC

CW jamming of L1, G1, L2 and L5

- More articulated (but moderate) effect than in 2022. A bit surprising.
- However: Different physical receiver in 2023 (perhaps different firmware installed)

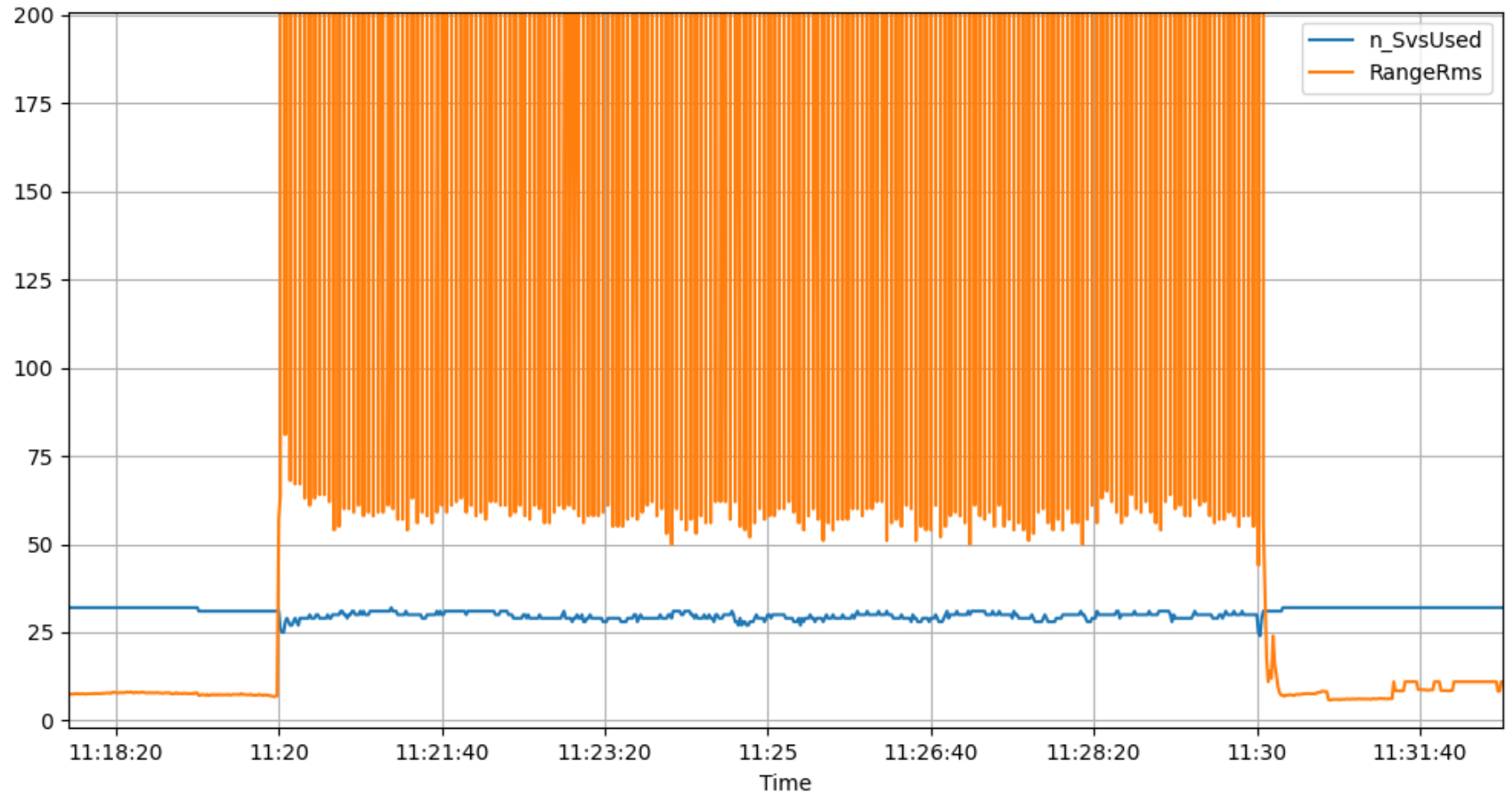


High-power jamming 20 W, 1.1 km away (page 2)

Range RMS from position computation in the F9P (taken from GST sentences) seems very sensitive to interference. This is the case for many of the tests (not only this one).

“Traditional” equation for such RMS:

$$RMS_{measurements} = \sqrt{\frac{\mathbf{e}^T \mathbf{W} \mathbf{e}}{n - p}}$$



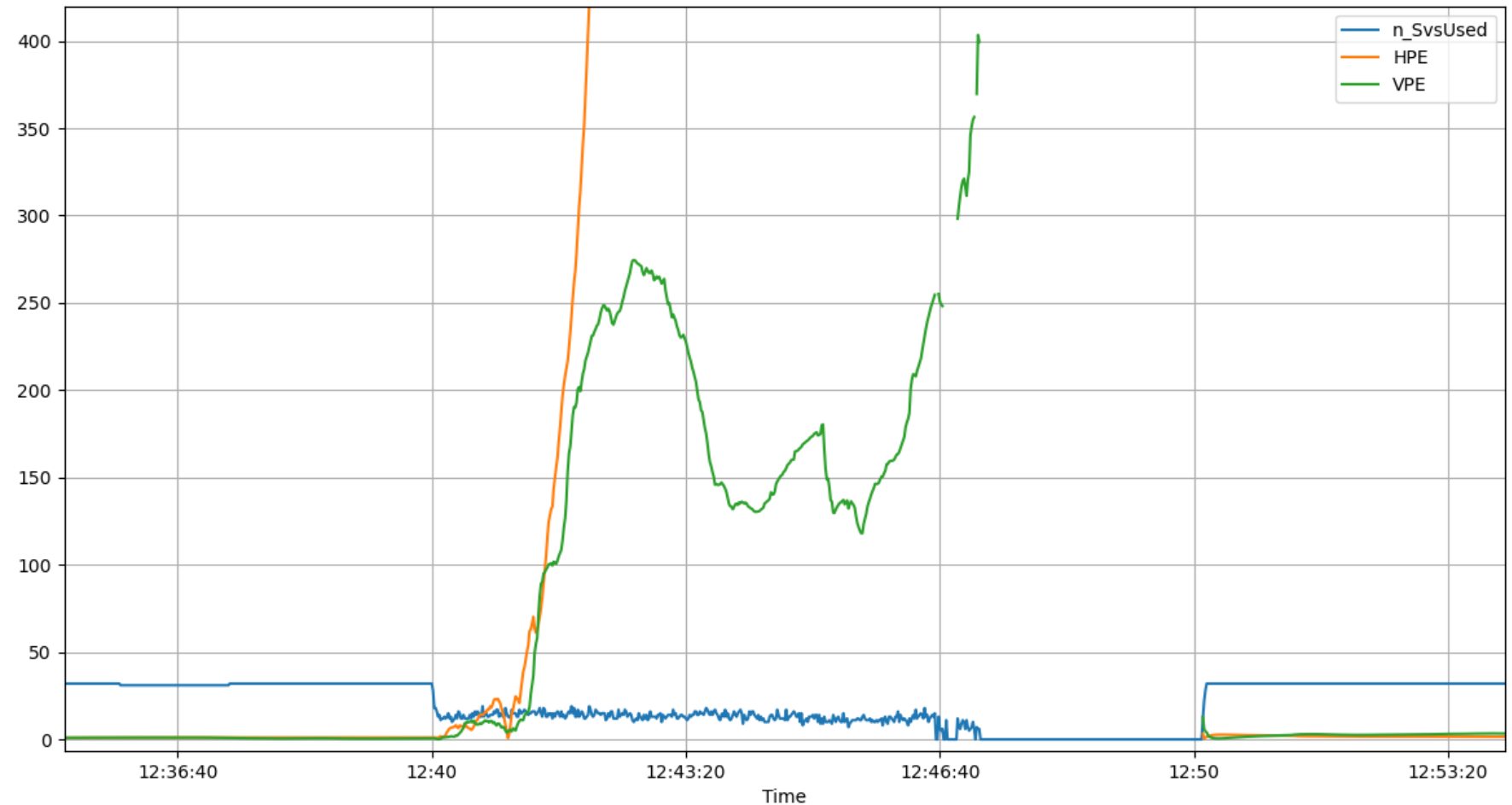
High-power jamming 20 W, 1.1 km away

18 Sep, 12:40 – 12:50 UTC

PRN-code jamming of

L1, G1, L2 and L5.

Caused extreme position drift, especially in the horizontal plane. At 12:47 positioning was lost.



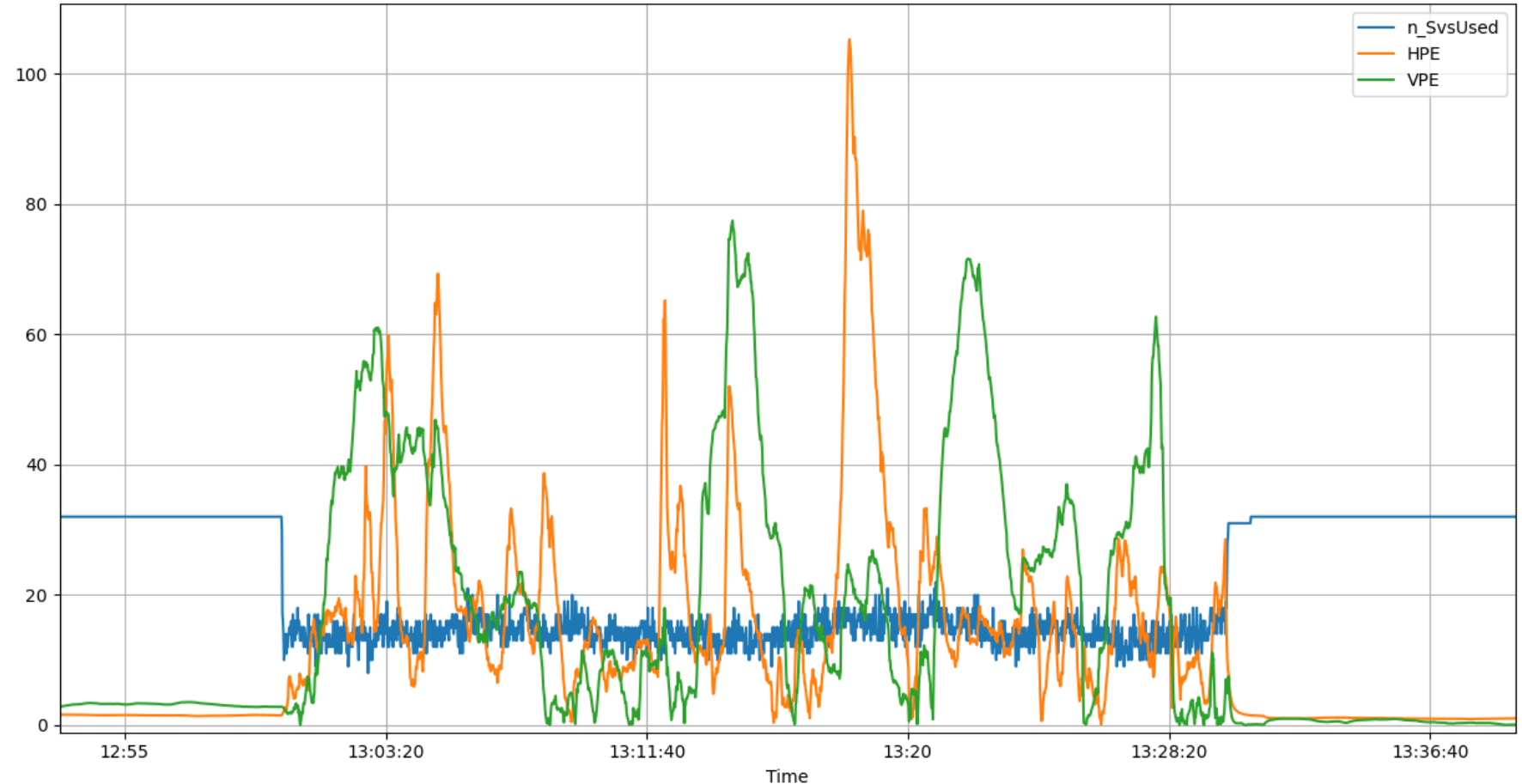
High-power jamming 20 W, 1.1 km away

18 Sep, 13:00 – 13:30 UTC

PRN-code jamming of

L1, G1, L2 and L5.

Caused large position drift (but not as extreme as in the previous case). Receiver threshold for SNR was changed from 0 to 25 dBHz at 13:15, but this had no visible effect.



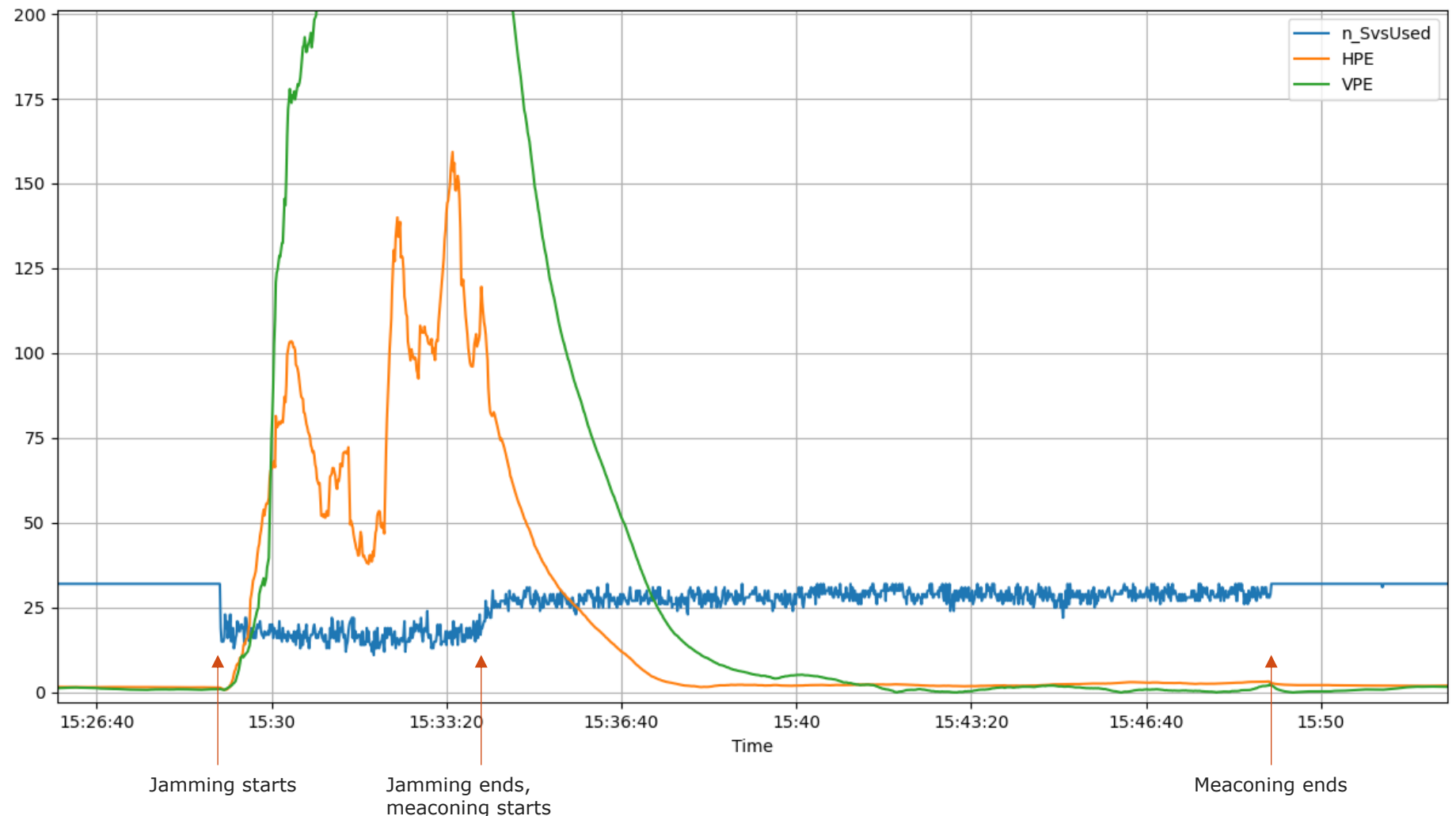
Meaconing 10 W, GPS L1 & L2, 1.6 km away

The 5-minutes jamming period (before the meaconing started) caused extreme position drift.

The meaconing itself caused less problems: The positioning converged back to a normal state within 6-7 minutes.

Probably more signals must be meaconed to fool the receiver ☺

Deeper analysis needed to find out exactly which signals/frequencies that kept the positioning OK during meaconing.



Simple spoofing attack example 1

20 Sep, 07:03 – 07:23 UTC

Incoherent spoofing. Large position and time jump, gradually increasing signal strength.

Spoofed position 70°N, 10°E

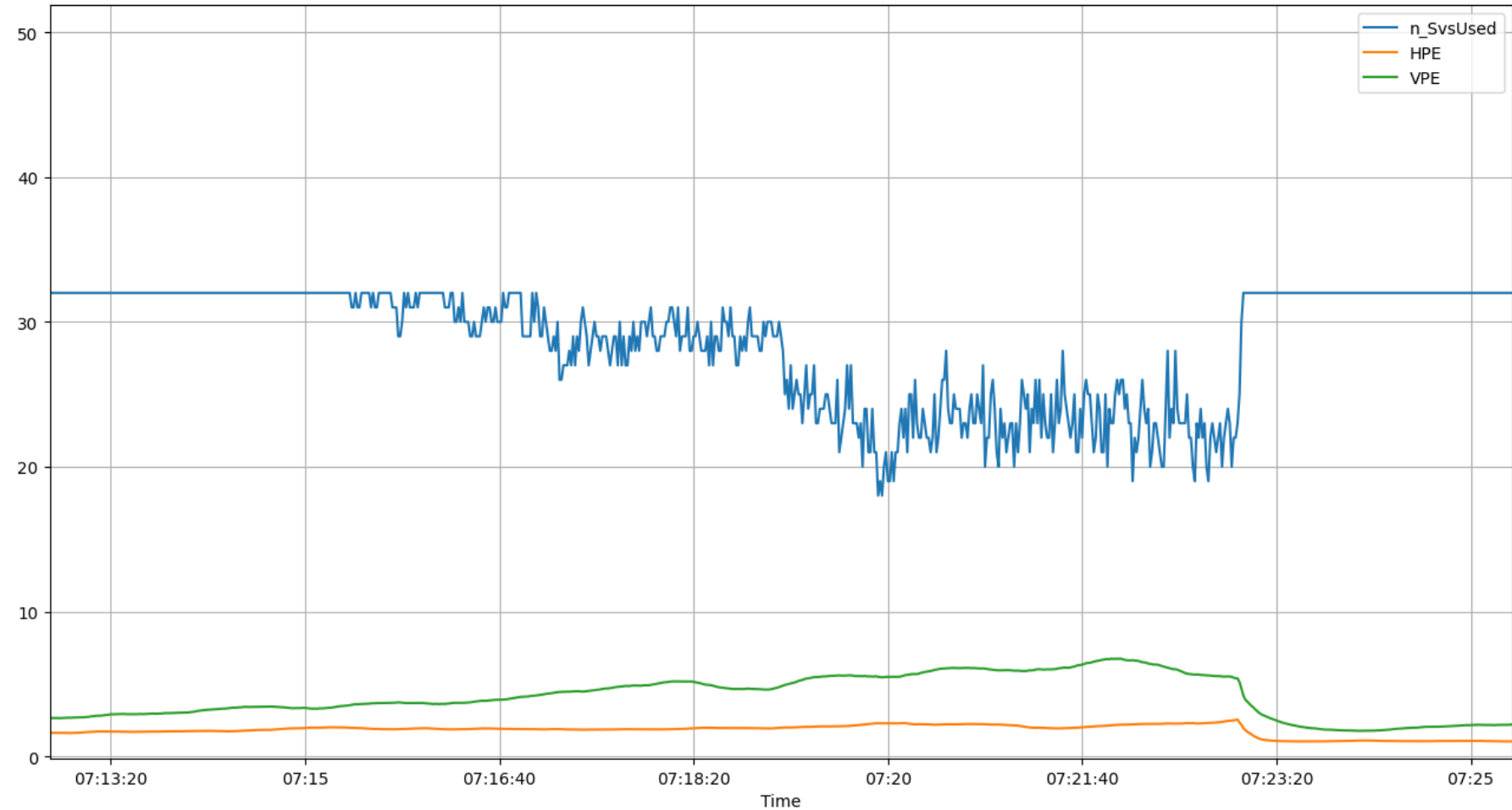
Spoofed start time 01.10.2023
12:00

No jamming.

Spoofed signals:

- GPS L1C/A, L2C, L5
- Galileo E1, E5a, E5b, E5AltBOC

Attack resisted by the receiver but positioning accuracy somewhat degraded.



More advanced spoofing attack example (page 1)

Coherent spoofing using true ephemerides.

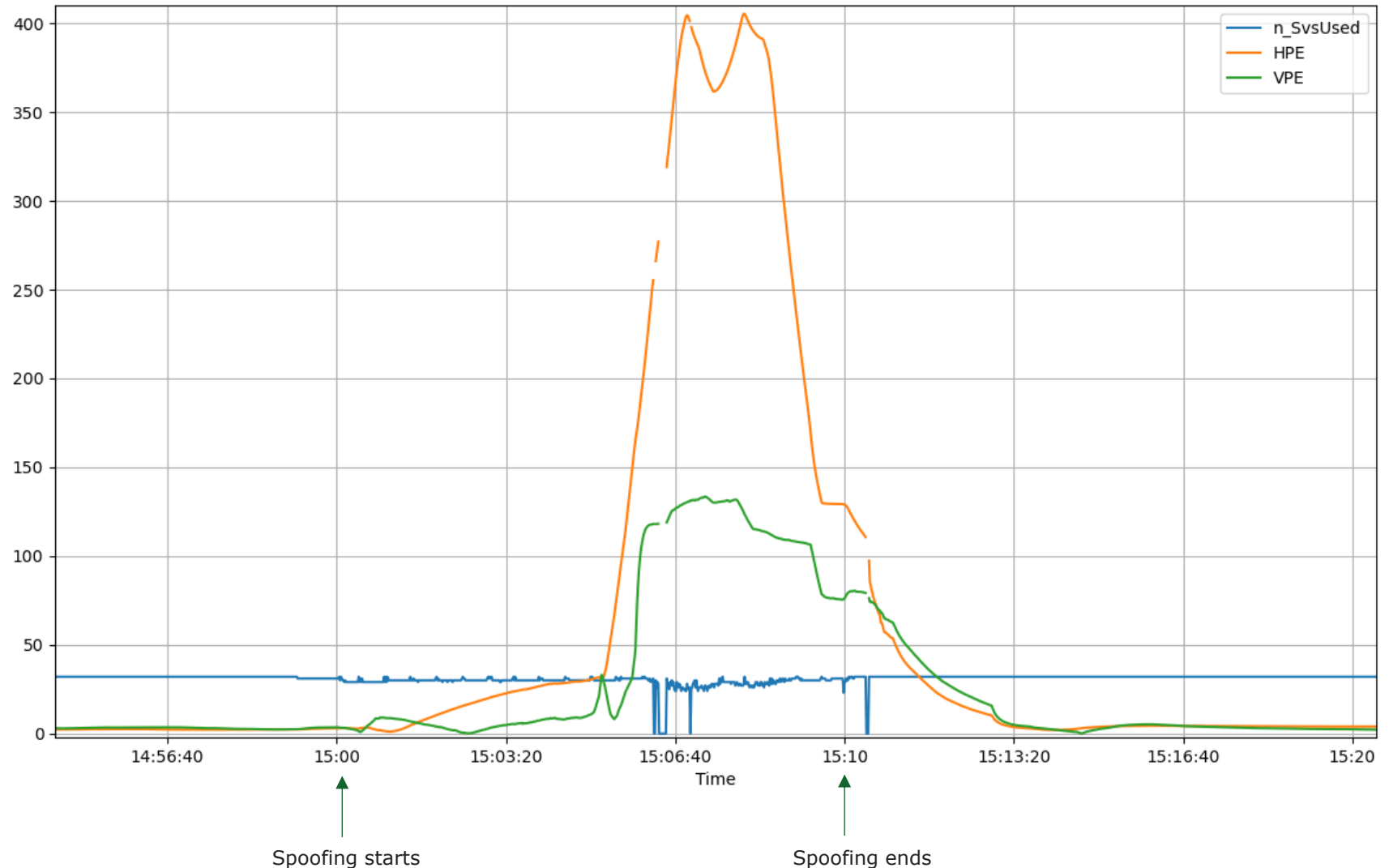
Spoofed route: Flying (“drone scenario”).

No jamming.

Spoofed signals:

- GPS L1 C/A, L2C, L5
- Galileo E1, E5a, E5b, E5AltBOC

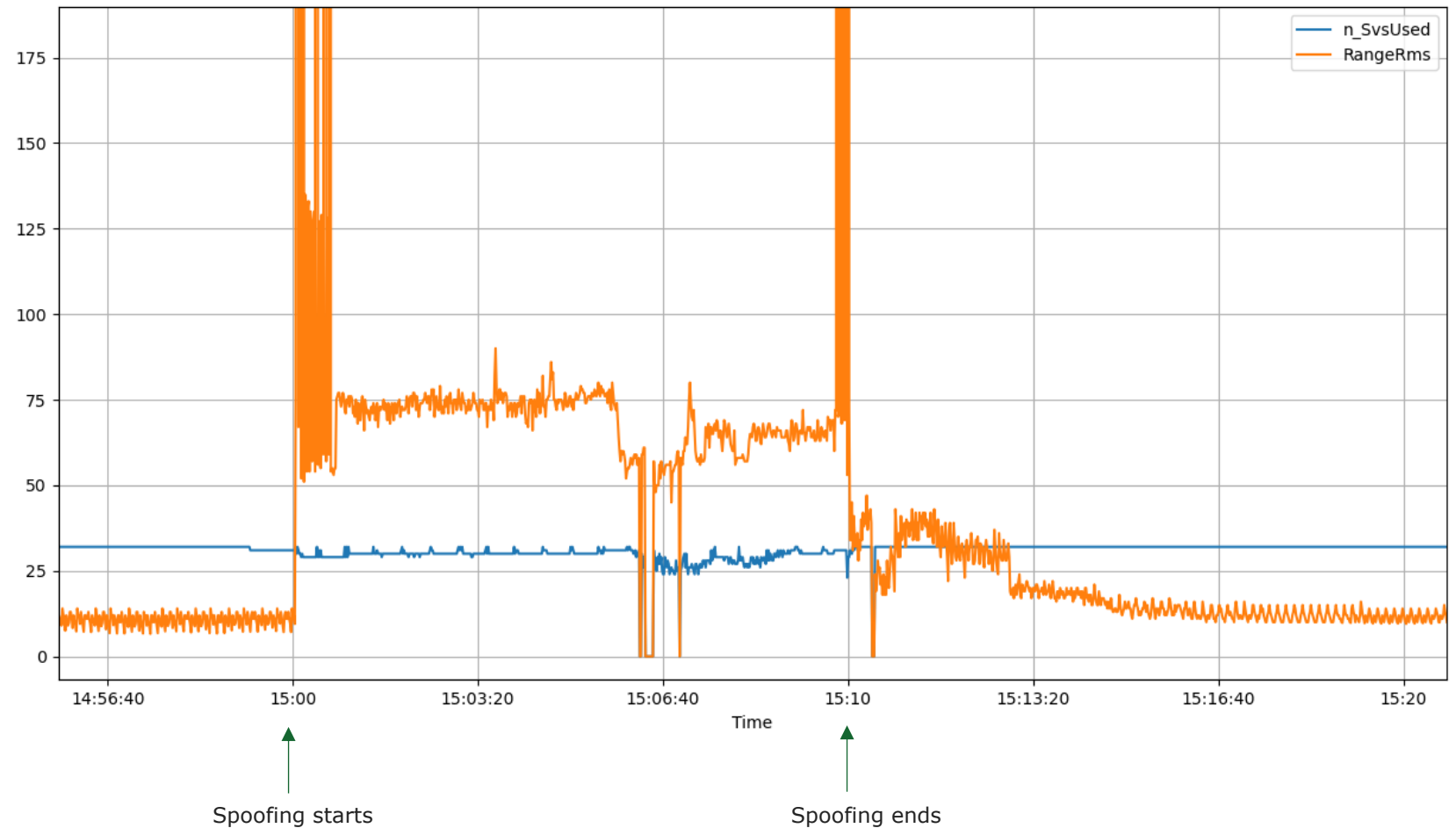
Spoofing attack “successful”, even if no jamming is performed (neither beforehand nor during spoofing), and even if the receiver uses GLO and BDS satellites as well. But see next page.



More advanced spoofing attack example (page 2)

Range RMS from position computation.

- “Normal” level: 10-15
- Level during spoofing: 60-80, maybe due to the discrepancies between false GPS & Gal measurements and true GLO & BDS measurements.
- Receiver seems to accept the increased RMS level, at least most of the time.



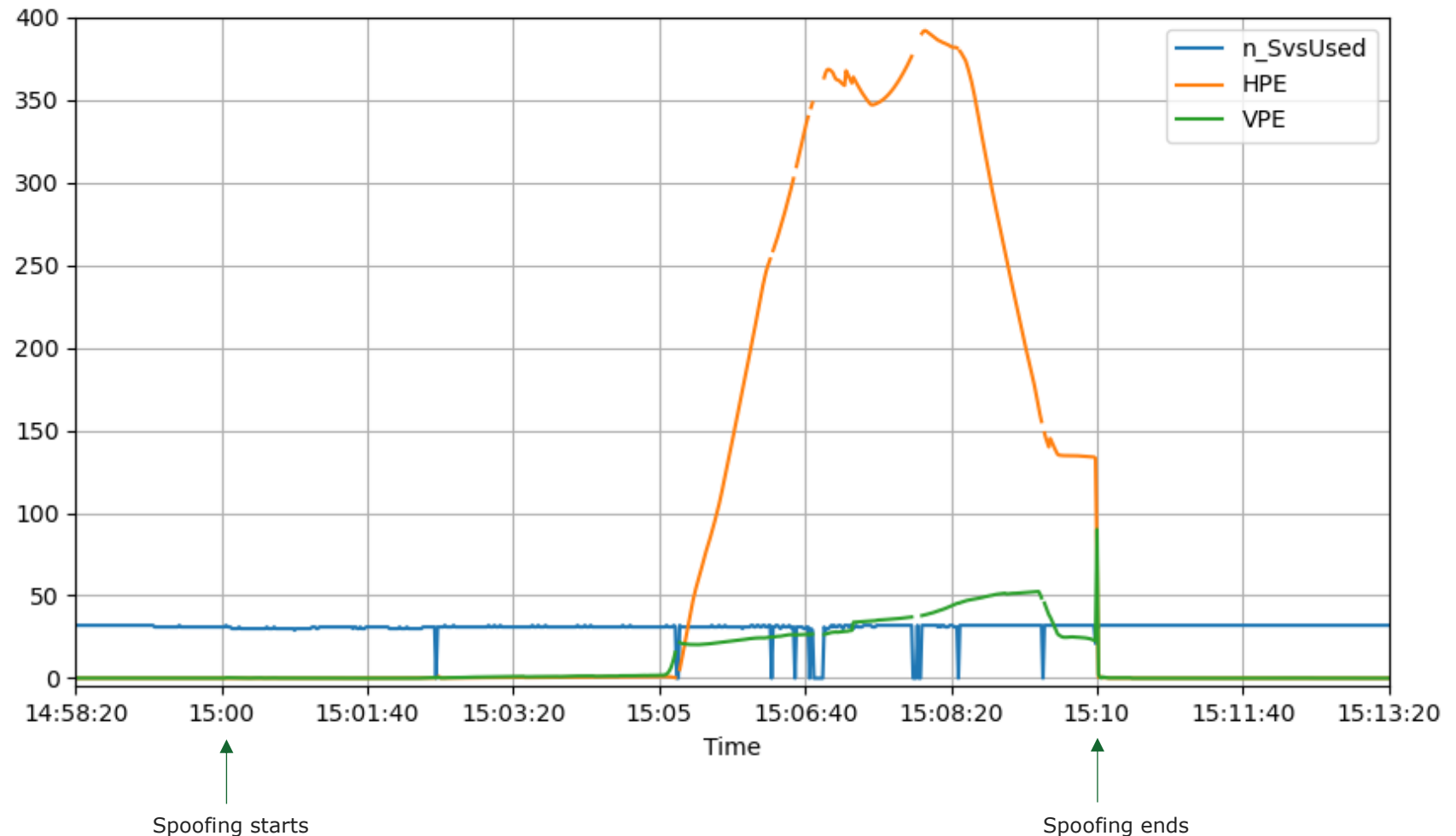
What about using CPOS NRTK service? (page 1)

Same advanced spoofing test as above ("drone scenario"). Results from U-blox receiver using CPOS.

Ground track of experienced trip is almost (but not totally) the same as in the standalone case. Experienced flying height is very different.

Between 15:02:33 and 15:10:08: No fixed (integer ambiguity resolved) RTK solution. Float RTK or code-based diff. solutions in this period.

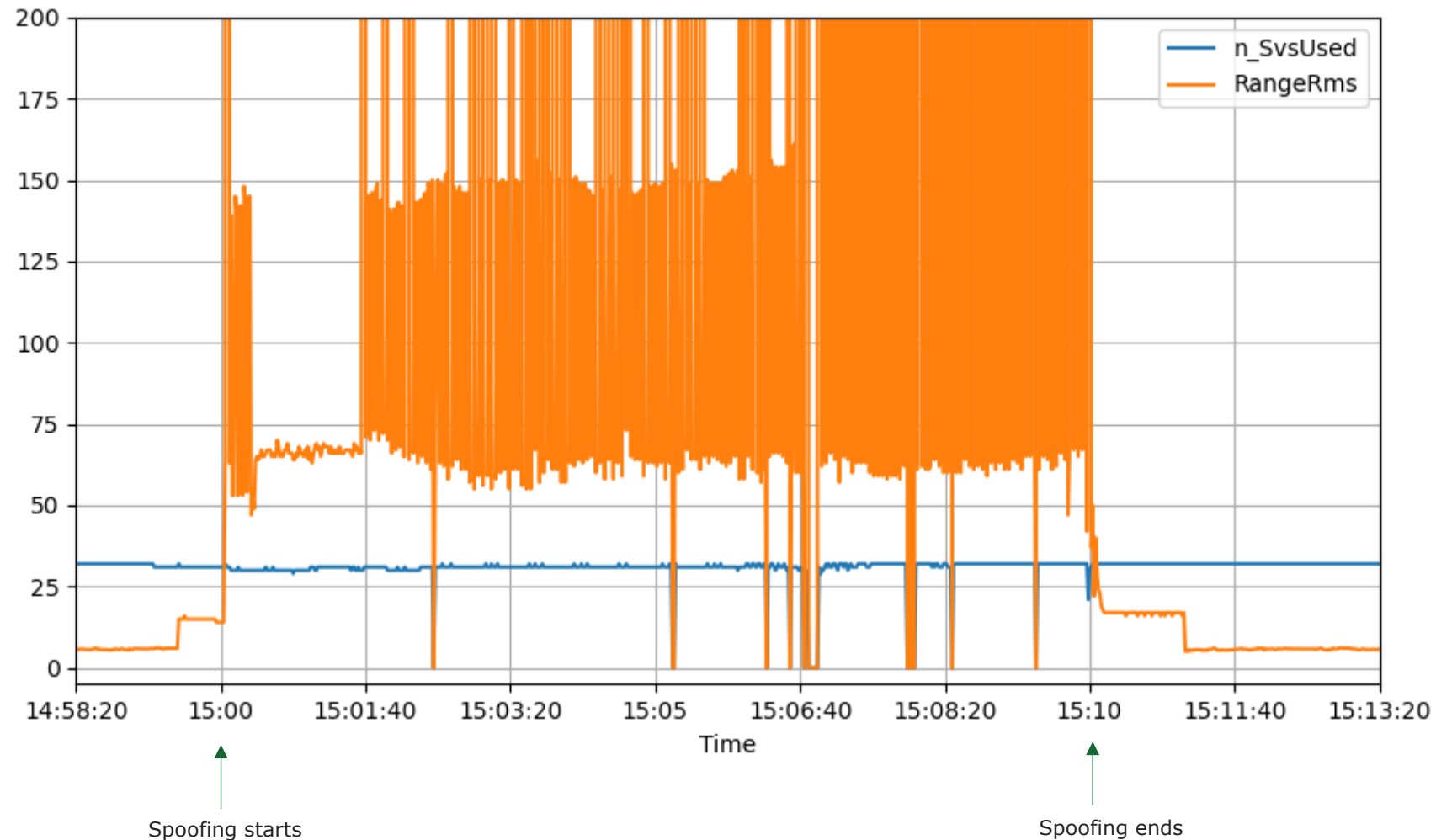
Faster return to a normal state when spoofing ends at 15:10, maybe due to differential positioning which aims at ambiguity fixing(?)



What about using CPOS NRTK service? (page 2)

Range RMS from position computation.

- “Normal” level: 5-15
- Level during spoofing: 60 to extremely high, maybe due to the discrepancies between false GPS & Gal measurements and true GLO & BDS measurements.
- Receiver seems to accept the increased RMS level, at least most of the time.



Conclusions, U-blox F9P positioning at JT 2023

Jamming:

- + : Effective fallback to using undisturbed frequency bands
- : The receiver seems very eager to use signals even if they are weak (and it seems difficult to prevent this by setting an SNR threshold) + filtering method & settings in PVT algorithm
 - = strong position drift under heavy jamming

Meaconing:

- + : Quite resistant to the meaconing attacks performed (the meaconing signals are experienced as jamming).
 - But some uncertainty about how many constellations/signals have been meaconed.

Spoofing:

- + : The receiver resists the simplest spoofing attacks. Some attacks are experienced as noise. Notice: No GLO or BDS spoofing attacks were performed, so the receiver may have been helped by correct GLO & BDS measurements.
- : The receiver is spoofed in several cases. This may happen also if initial jamming is not performed.

Credits (1)

A large part of this presentation is extracted from the article

“Jammertest: An open GNSS interference test arena to accelerate the development of resilient GNSS applications”. Nicolai Gerrard¹, Tor Atle Solend², Anders Rødningsby², Øystein Karlsen¹, Tomas Levin³, Harald Hauglin⁴, Kristian Svartveit⁵, Christian Berg Skjetne³, Anders Martin Solberg⁶, Thomas Rødningen⁴ and Øystein Borlaug². Proceeding paper from ENC 2025, Wroclaw, Poland.

1. Norwegian Communications Authority (NKOM – Nasjonal kommunikasjonsmyndighet)
2. Norwegian Defence Research Establishment (FFI – Forsvarets forskningsinstitutt)
3. Norwegian Public Roads Administration (Statens vegvesen)
4. Norwegian Metrology Service (Justervesenet)
5. Norwegian Space Agency (Norsk Romsenter)
6. Norwegian Mapping Authority (Kartverket)

Credits (2)

PowerPoint presentation “Jammertest”.

Presented by Nicolai Gerrard (NKOM) at ENC 2025, Wroclaw, Poland, May 2025.

Credits (3)

Trusselens omfang (eng.: The extent of the threat”).

Nicolai Gerrard, NKOM.

Presented at FFI breakfast meeting, Oslo, Norway, 18 March 2025

Credits (4)

General credits:

Norwegian Public Roads Administration (Statens vegvesen)

Norwegian Communications Authority (NKOM - Nasjonal kommunikasjonsmyndighet)

Norwegian Defence Research Establishment (FFI – Forsvarets forskningsinstitutt)

Norwegian Metrology Service (Justervesenet)

Norwegian Space Agency (Norsk Romsenter)

Avinor AS

Testnor AS



Questions?

Contact information

→ Anders M. Solberg

→ anders.martin.solberg@kartverket.no

<https://jammertest.no>



Kartverket