Testing various GNSS receivers at Jammertest

Anders M. Solberg, Carl H. Ellingstad

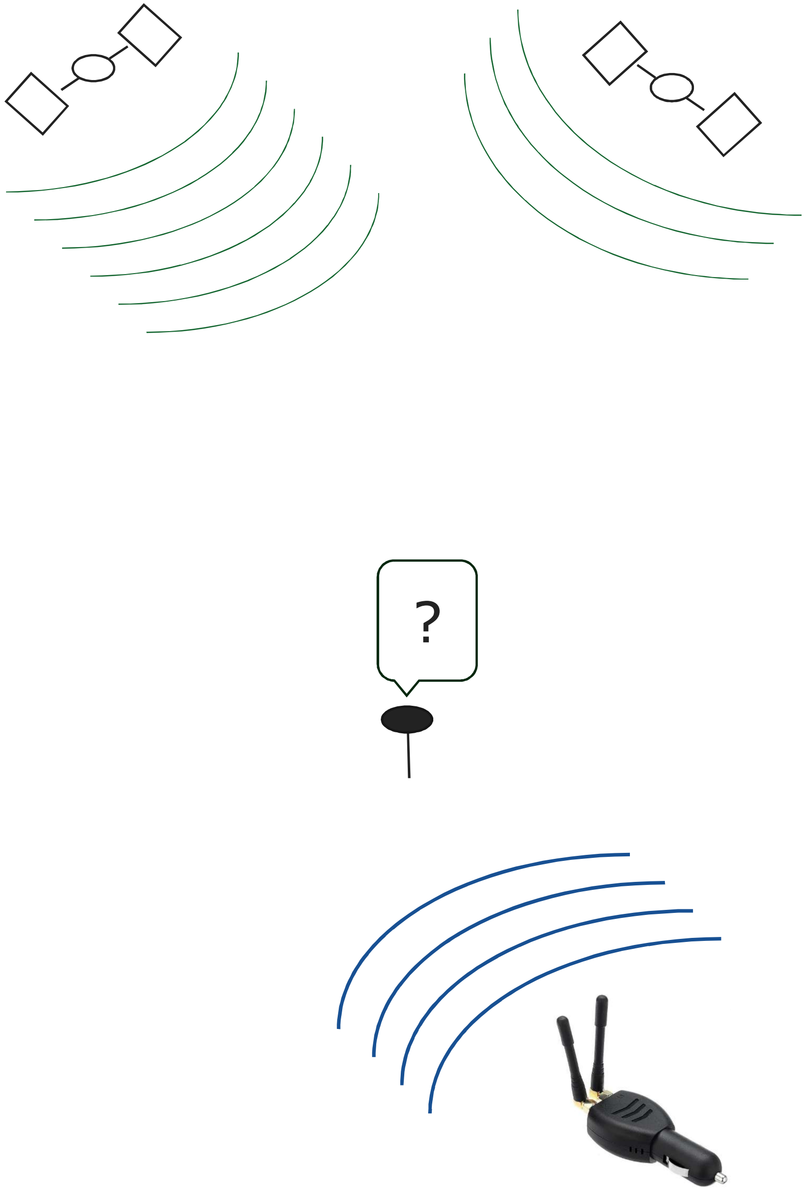
Kartverket

14.03.2024

What is GNSS jamming?

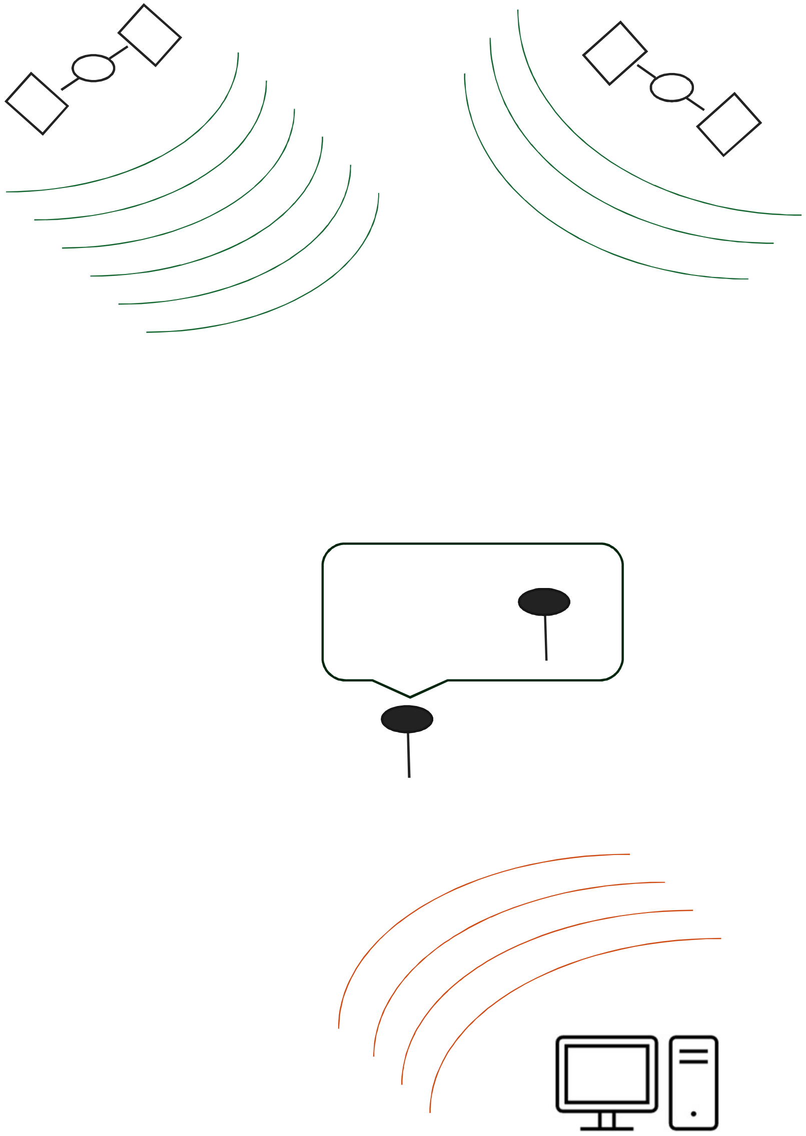
Transmission of radio signals to minimize the ability of the GNSS receiver to receive the radio signals that are transmitted by the GNSS satellites

- The perhaps most well-known result: The GNSS receiver is unable to compute its position
- But jamming can also lead to other effects…



What is GNSS spoofing?

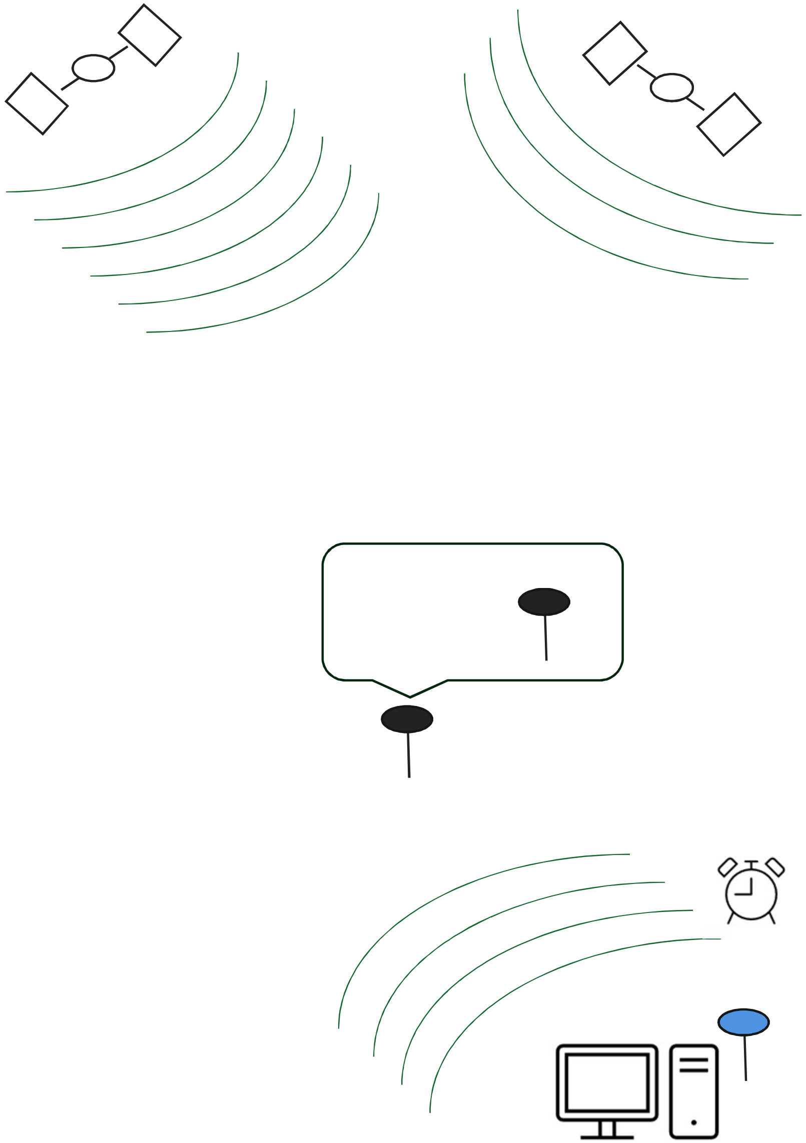
Transmission of fake GNSS signals to fool the GNSS receiver to compute wrong position and/or time.



Kartverket

What is GNSS meaconing?

Re-transmission of real GNSS signals with time delay.



What is Jammertest?

- Event arranged 19-23 September 2022 & 18-22 September 2023 in and around the village Bleik at the island of Andøya in the Vesterålen district, northern Norway (69.3°N, 16°E)
- Testing of PNT related equipment under transmission of disturbing or spoofing GNSS-like radio signals
  - Lots of technical equipment contain GNSS chipsets
- Organizers:

Statens vegvesen
Norwegian Public Roads Administration

NKOM Norwegian Communications Authority

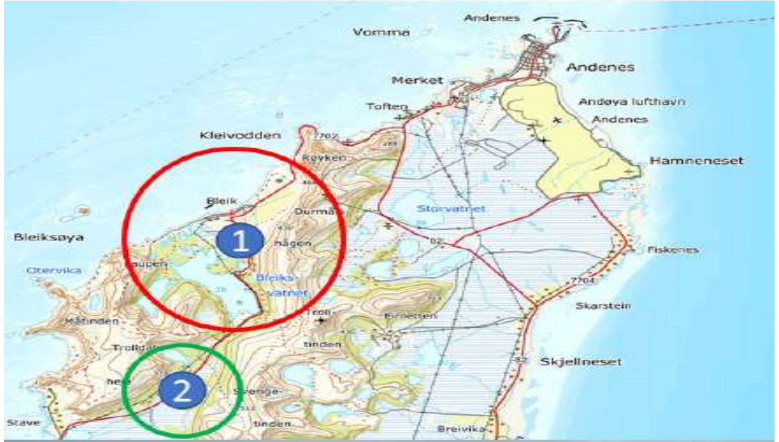
FFI Forsvarets forskningsinstitutt
Norwegian Defence Research Establishment

Justervesenet

Norsk Romsenter
Norwegian Space Agency

- Participants: Governmental, research institutions, industry
- 2022: ~100 participants from several countries
- 2023: ~200 participants from several countries
- Base camp at the Bleik community house.

Kartverket



Biler, droner, helikoptre og annet utstyr har blitt utsatt for ja
Foto: Duus media

NMA at Jammertest 2022

People:

Tor-Ole Dahlø and Anders M. Solberg

Equipment:

- Geodetic GNSS receivers: Trimble Alloy, Leica GR50
- Mass market GNSS receiver: u-blox ZED-F9P (in standalone SPP mode)
- GNSS antennas, tribrachs, 5/8'' adapters, tripods, antenna cables

  → Static data collection
- Indoors operation of the receivers (however, somewhat chilly because the antenna cables needed to go through a slightly open window)
- High-effect jammer located about 1.1 km away

Kartverket

NMA at Jammertest 2023

People:

Carl H. Ellingstad and Anders M. Solberg

Equipment:

- Geodetic GNSS receivers: Leica GR50
- Mass market GNSS receivers:
  - u-blox ZED-F9P standalone SPP
  - u-blox ZED-F9P connected to CPOS NRTK service
- GNSS antennas, tribrachs, 5/8'' adapters, tripods, antenna cables

  → Static data collection
- Indoors operation of the receivers
- High-effect jammer located about 1.1 km away

Kartverket

U-blox ZED-F9P

17.0 mm x 22.0 mm x 2.4 mm

Antenne:
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
    2. B2I (old signal type) is only transmitted by the quite few BDS-2 satellites
  - Somewhat restricted number of channels: Apparently too few channels to track 2 frequencies for all visible satellites at the same time
- 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

Broadcast of Galileo HAS

25.5 cm

24.8 cm

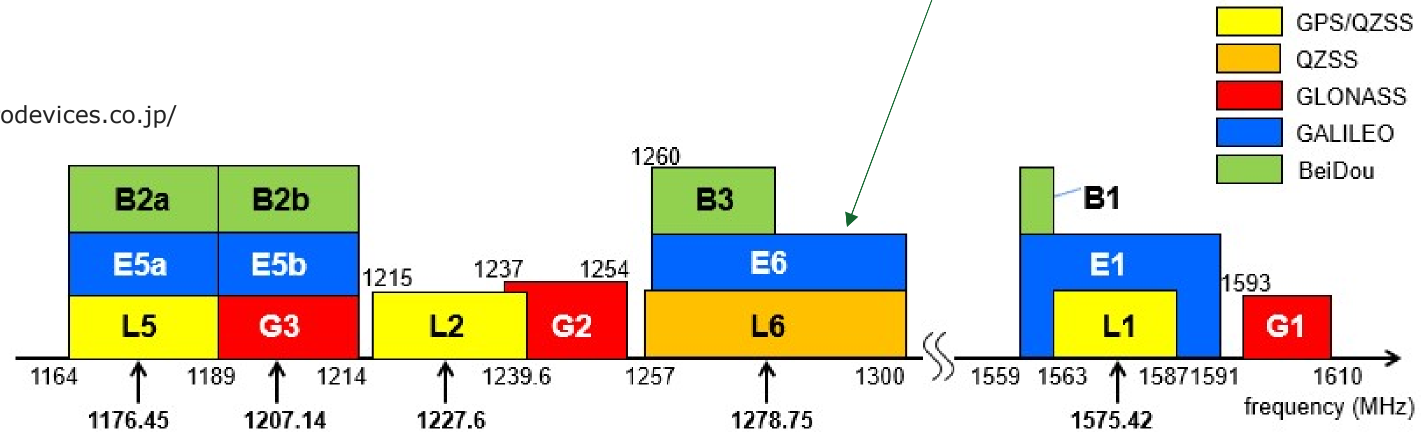
24.4 cm

~24.1 cm

19.0 cm

~18.7 cm

https://www.nisshinbo-microdevices.co.jp/



U-blox ANN-MB

U-blox ANN-MB

Lower L-band

Upper L-band

Effects on U-blox F9P positioning

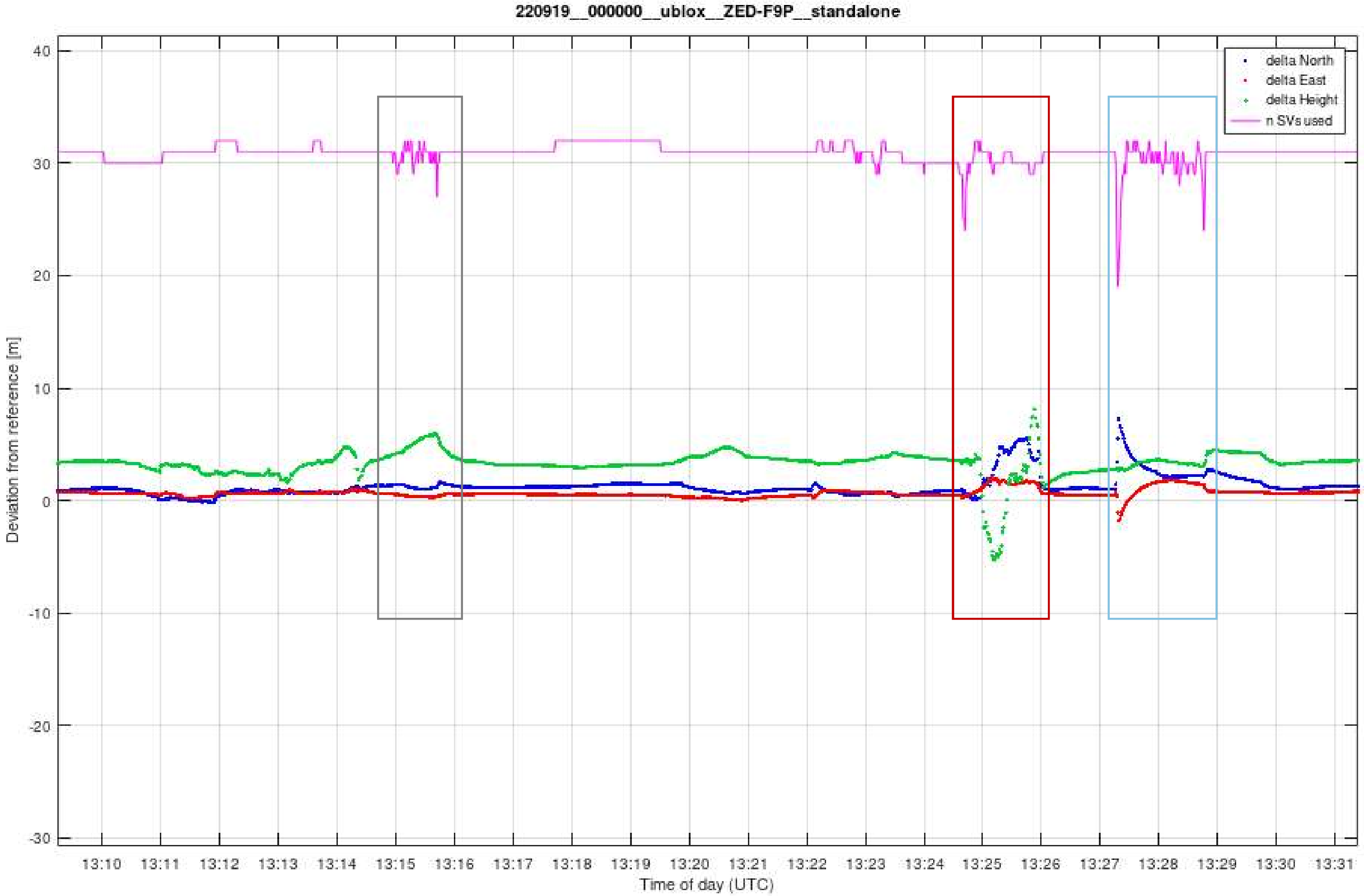
- On the following slides, example results from the U-blox ZED-F9P standalone receiver are shown.
- This receiver type is assumed to be relevant for automotive applications.
- U-blox outputs text (NMEA 0183) formatted positioning data and metadata in binary .ubx files (a bit messy in my opinion)

  → Using open-source Python library “pyubx2” (runs somewhat slowly) to be able to parse such files
- Very simple analysis:
  - Plotting time series: Position deviations, number of satellites used in positioning
  - Looking for abnormal behaviour
  - Inspecting metadata (residuals, estimated standard deviations etc.) if necessary
- All position deviation numbers in the following plots are in the unit meters

Handheld jammers, 2022

Distance to jammer: ~50 m

Often no or limited effect on positioning.



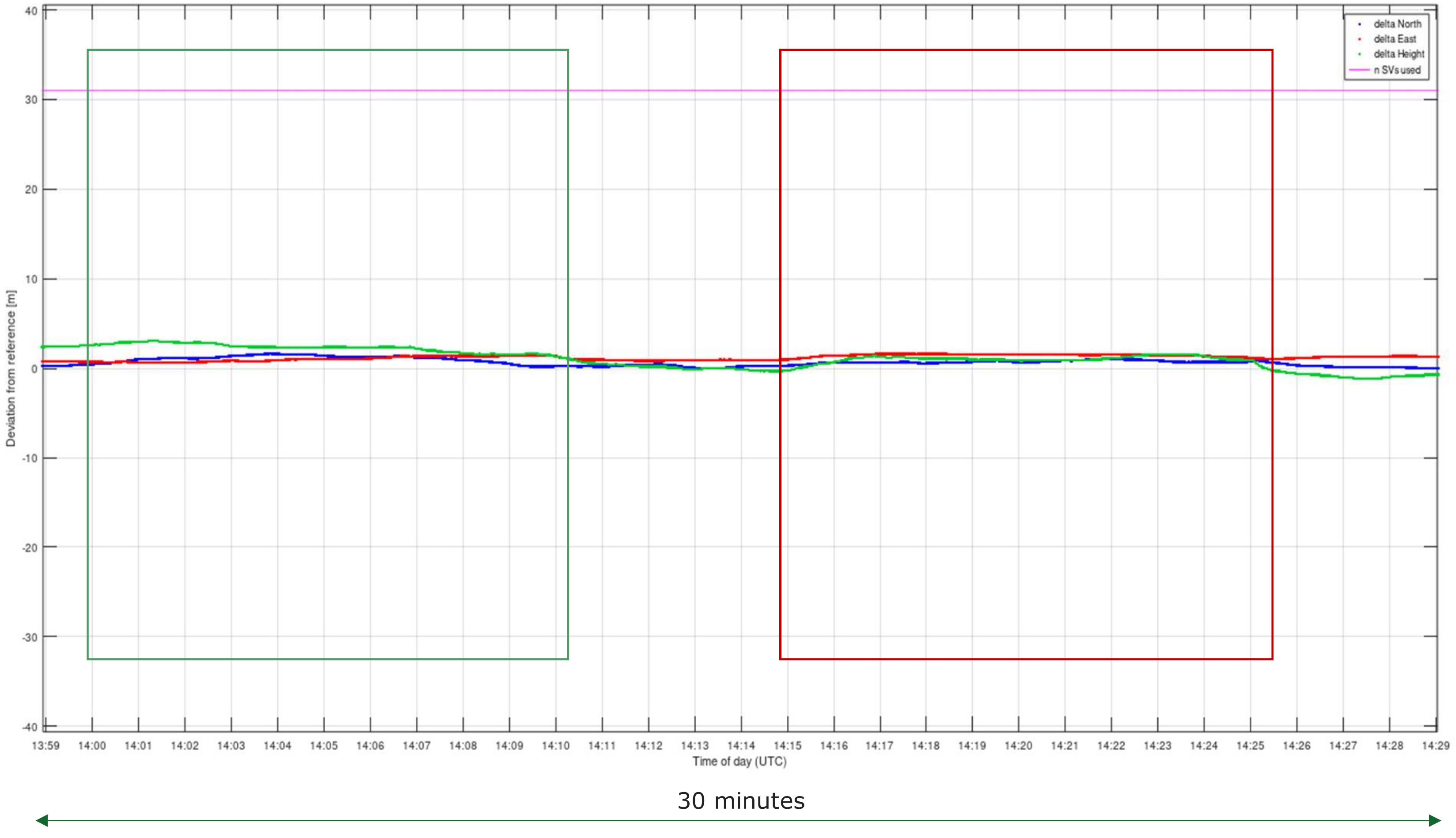
Kartverket

High-power jamming 20 W, 1.1 km away, 2022

Jamming of L1

Continuous Wave signal (CW) jamming:
→No visible effect.

PRN-code jamming:
→L1-band signals heavily disturbed, but no visible effect on positioning due to use of other frequencies.



Kartverket

High-power jamming 20 W, 1.1 km away, 2022

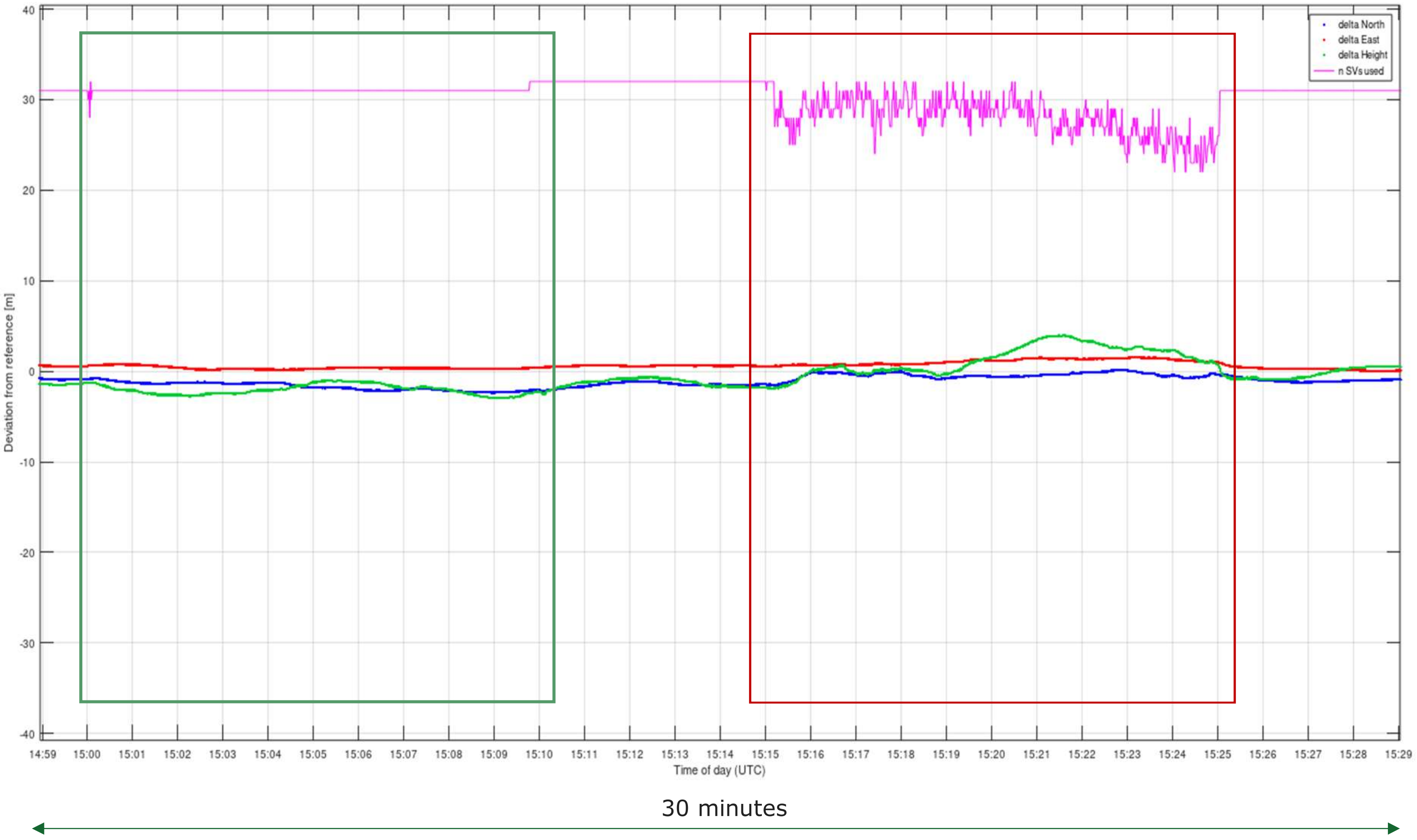
Jamming of L1, G1, L2

Continuous Wave signal (CW) jamming:

→Nearly no effect

PRN-code jamming:

→Fast oscillation and a certain reduction in the number of used satellites



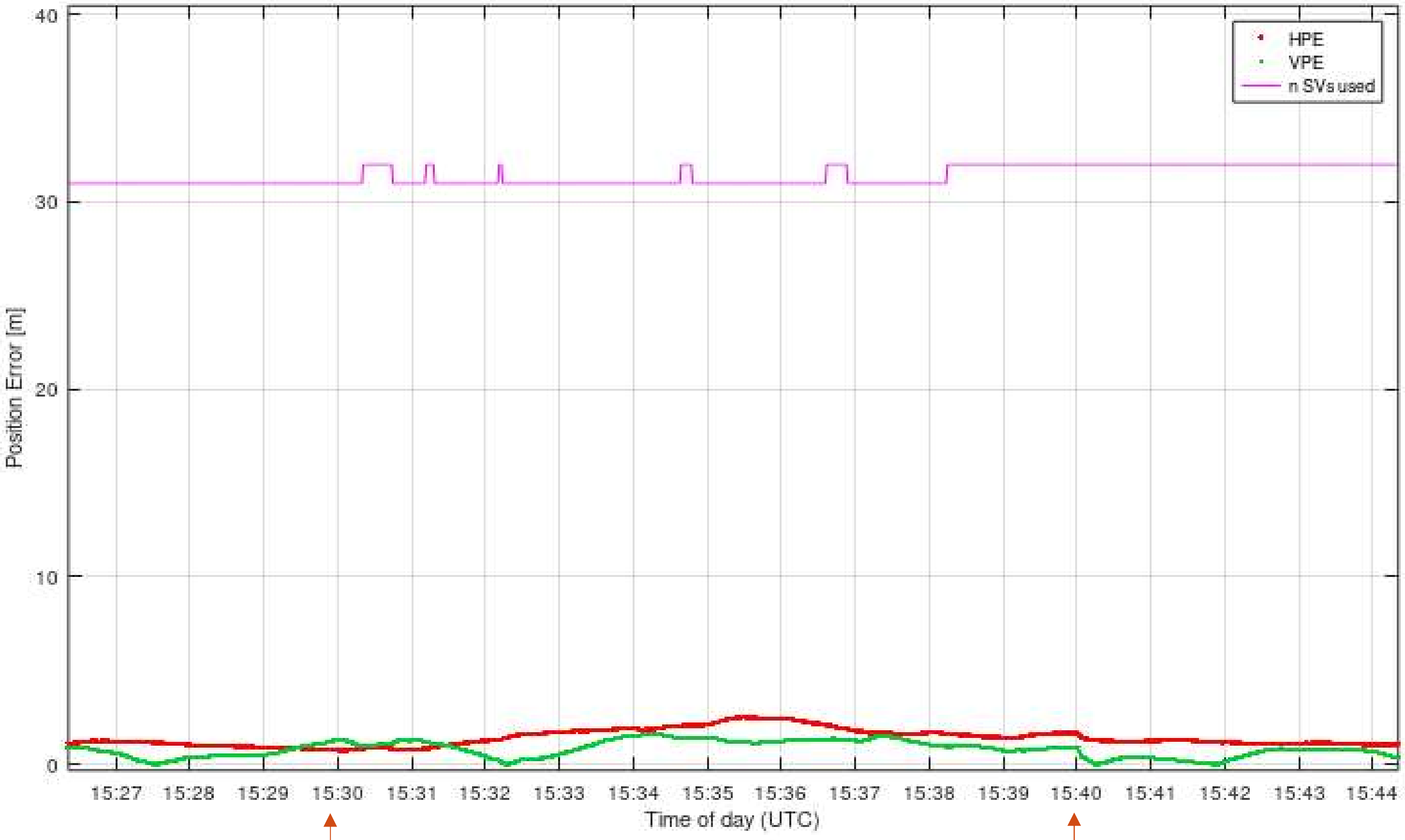
30 minutes

Kartverket

High-power jamming 20 W, 1.1 km away, 2022

CW jamming of L1, G1, L2 and L5

Almost no effect.



Jamming starts

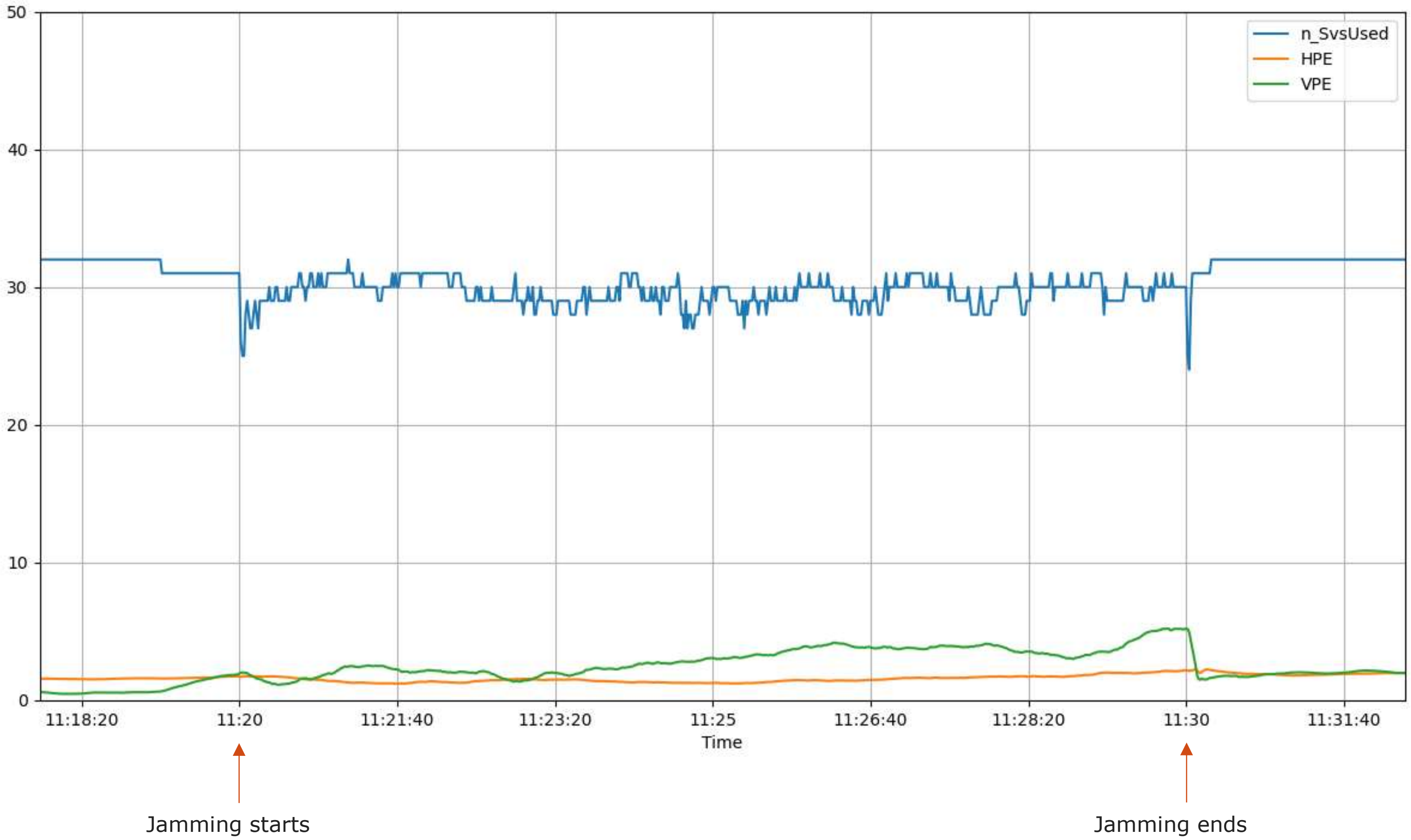
Jamming ends

Kartverket

High-power jamming 20 W, 1.1 km away, 2023 (page 1)

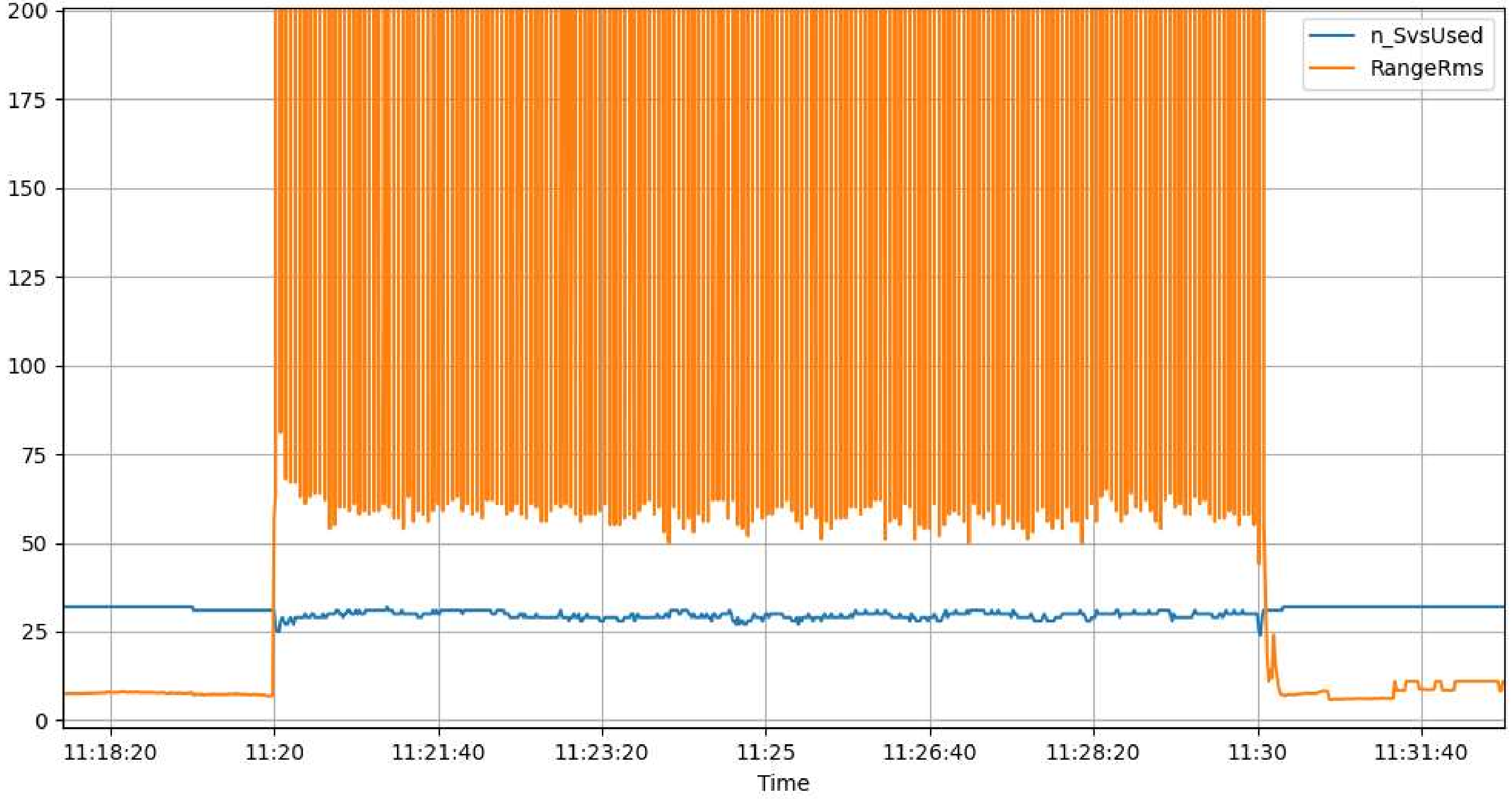
CW jamming of L1, G1, L2 and L5 led to more disturbance on the positioning in 2023 than in 2022.

- Surprising
- However: Different physical receiver in 2023 (perhaps different firmware installed)



High-power jamming 20 W, 1.1 km away, 2023 (page 2)

Range RMS (a-posteriori Sigma0) from position computation in the F9P seems very sensitive to interference. This is the case for many of the tests (not only this one).



Kartverket

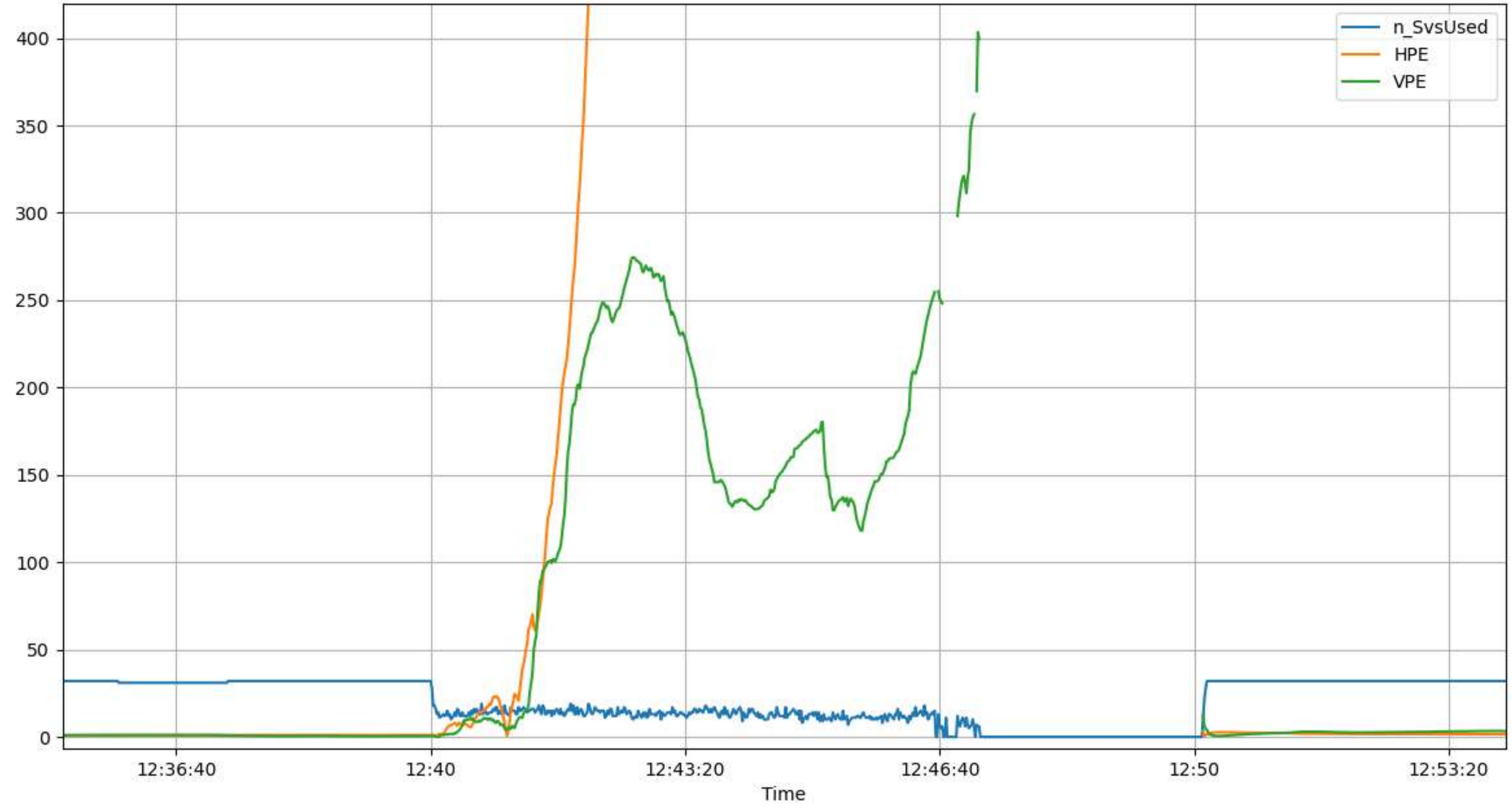
High-power jamming 20 W, 1.1 km away, 2023

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.



Kartverket

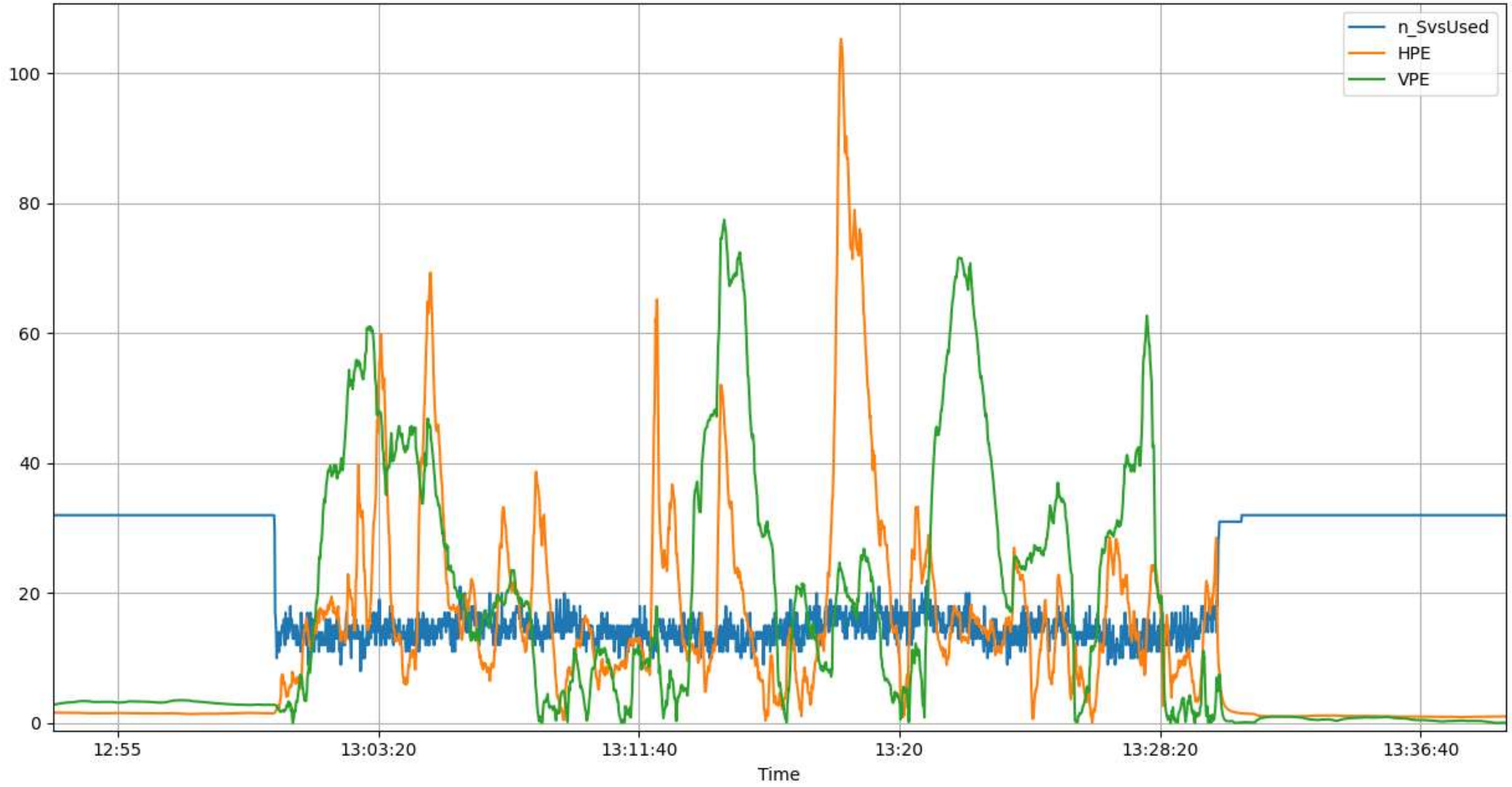
High-power jamming 20 W, 1.1 km away, 2023

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.



Kartverket

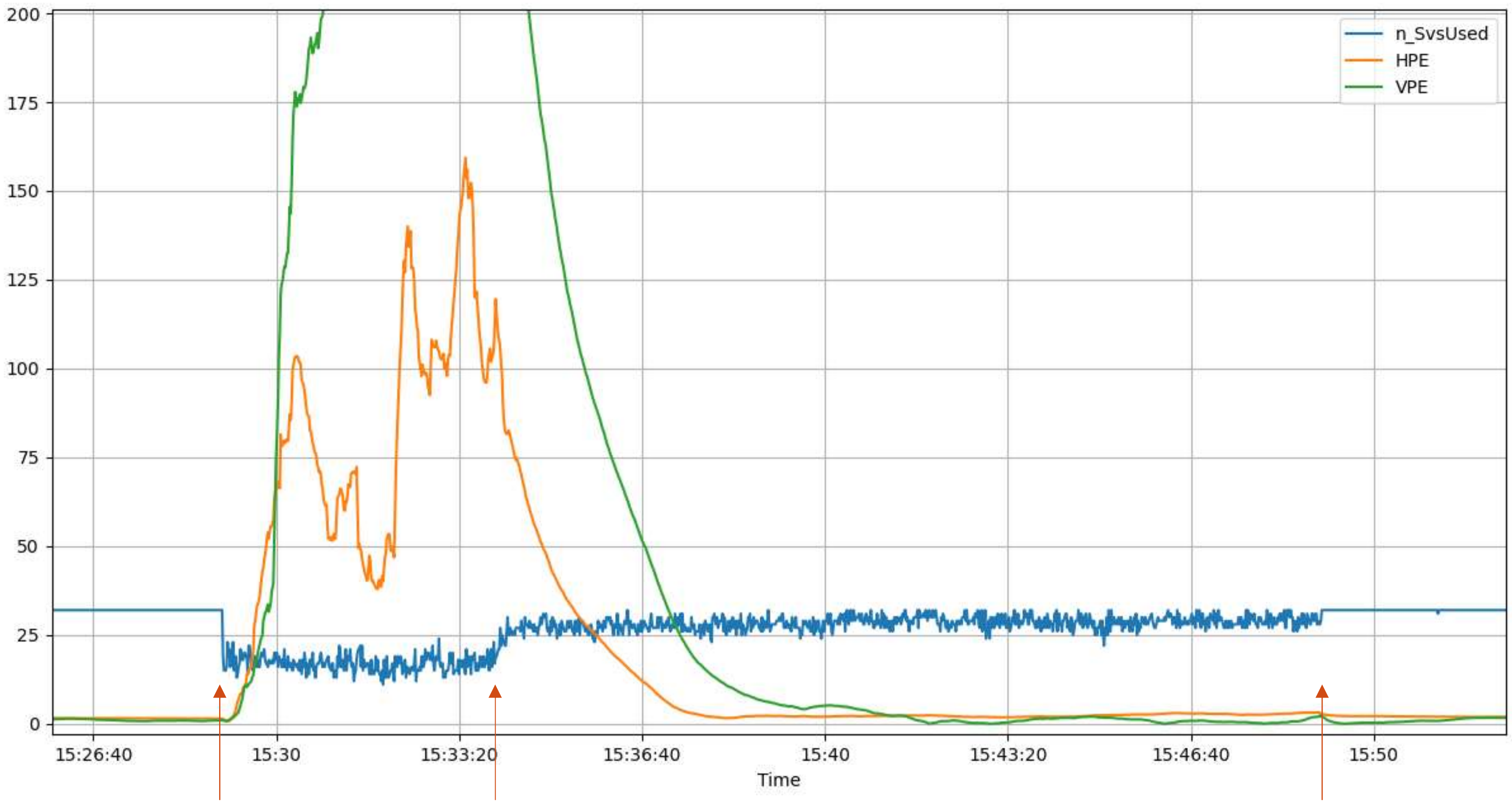
Meaconing 10 W, GPS L1 & L2, 1.6 km away, 2023

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.



Jamming starts

Jamming ends,
meaconing starts

Meaconing ends

Kartverket

Simple spoofing attack example 1, 2023

20 Sep, 07:03 – 07:23 UTC

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

Spoofed position 70°N, 10°E

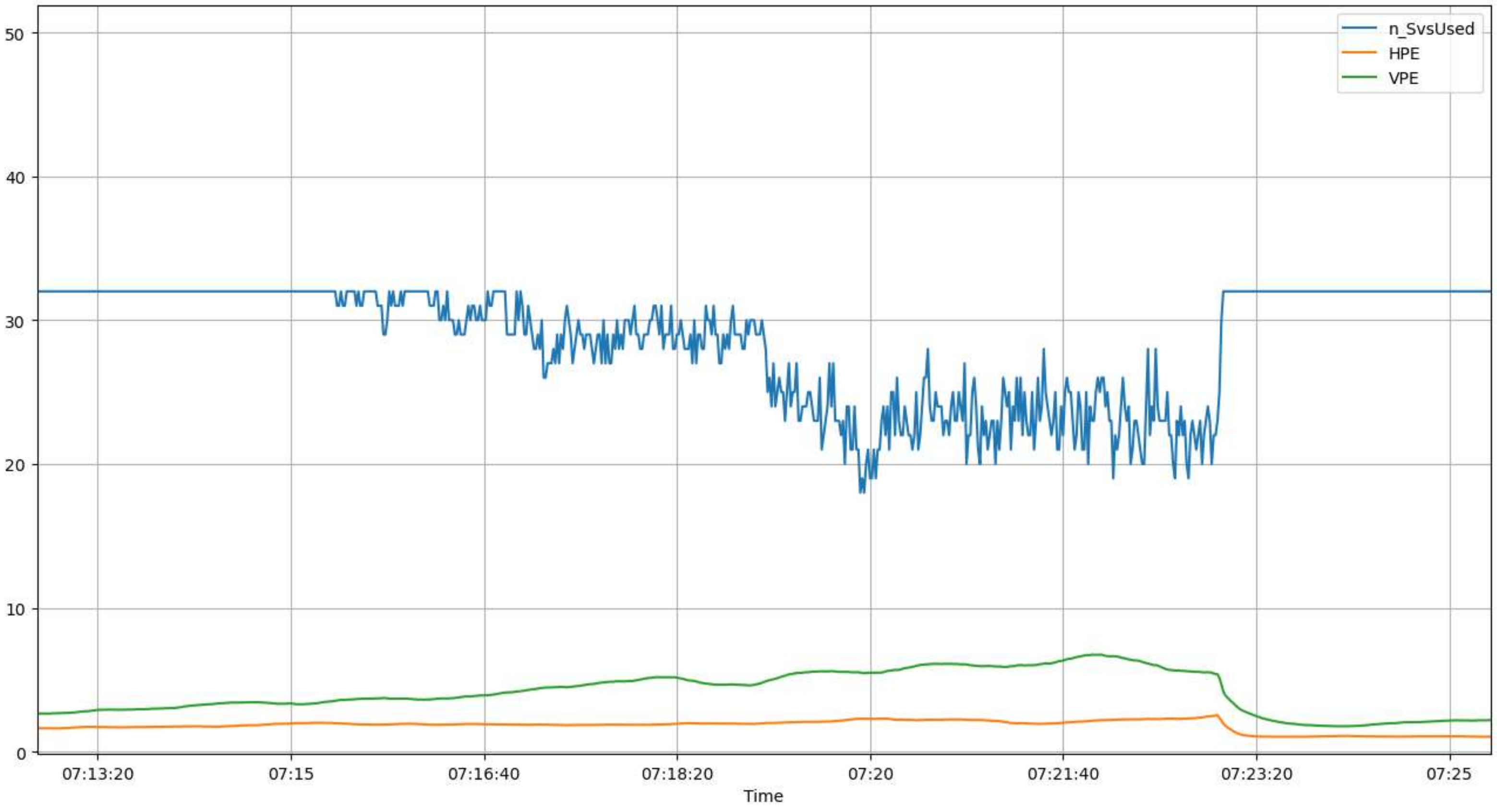
Spoofed start time 01.10.2023 12:00

No jamming.

Spoofed signals:

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

Attack resisted by the receiver but positioning accuracy somewhat degraded.



Kartverket

Simple spoofing attack example 2, 2023

Incoherent spoofing with jamming, using synthetic ephemerides.

Large position and time jump.

- Spoofed position 70°N, 10°E (far away)
- Spoofed start time 01.10.2023 12:00

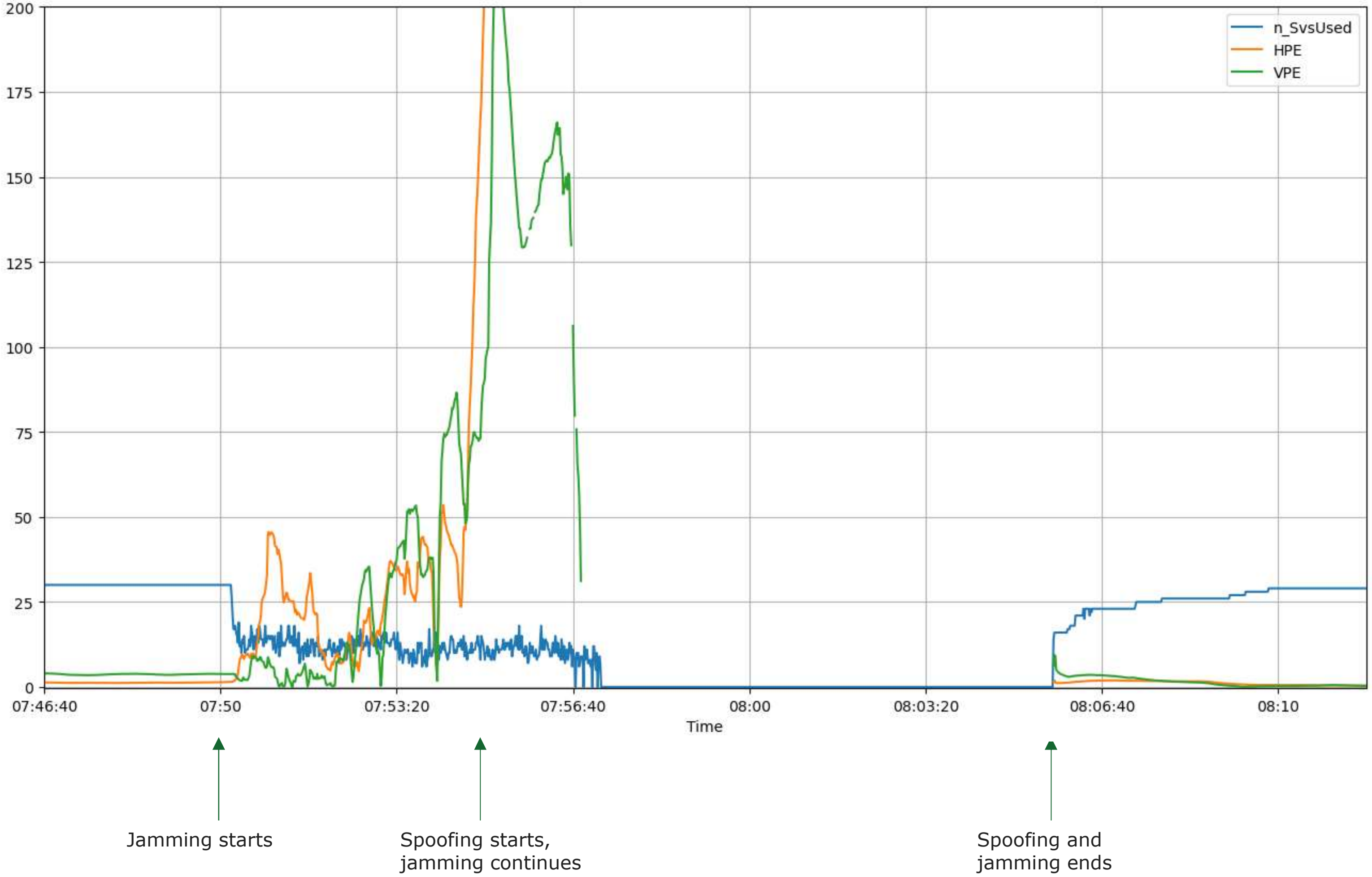
Jammed signals:

- L1, G1, B1l, E6, L2, E5b, L5

Spoofed signals:

- GPS L1C/A
- Galileo E1

Receiver never showed the spoofed position, but extreme position drift and eventually loss of positioning. Unclear if this was solely caused by the jamming or if the spoofing signal and/or spoofing data played a role as well.



Jamming starts

Spoofing starts, jamming continues

Spoofing and jamming ends

Kartverket

More advanced spoofing attack example (page 1)

Coherent spoofing using true ephemerides.

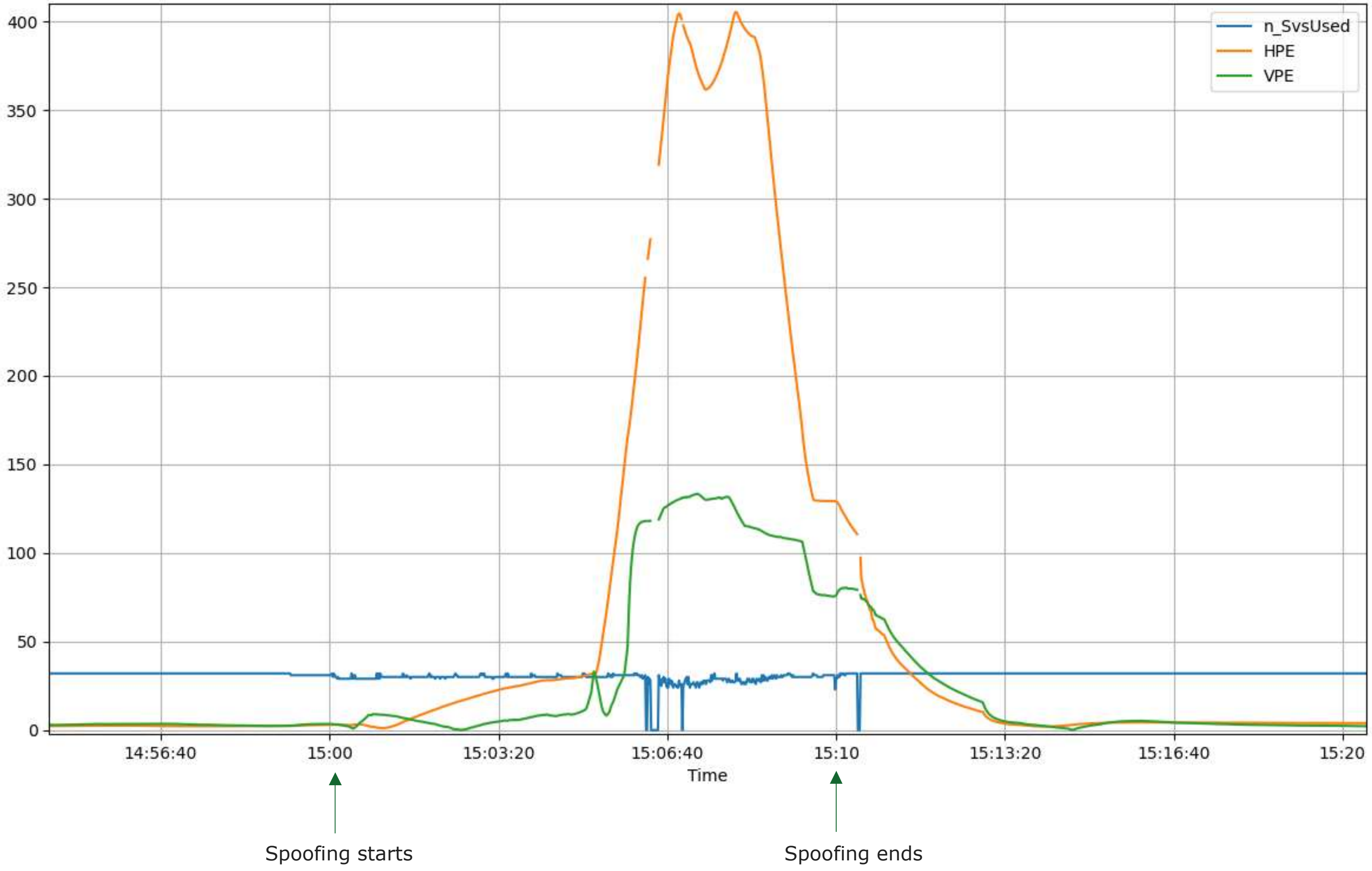
Spoofed route: Flying (“drone scenario”).

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.

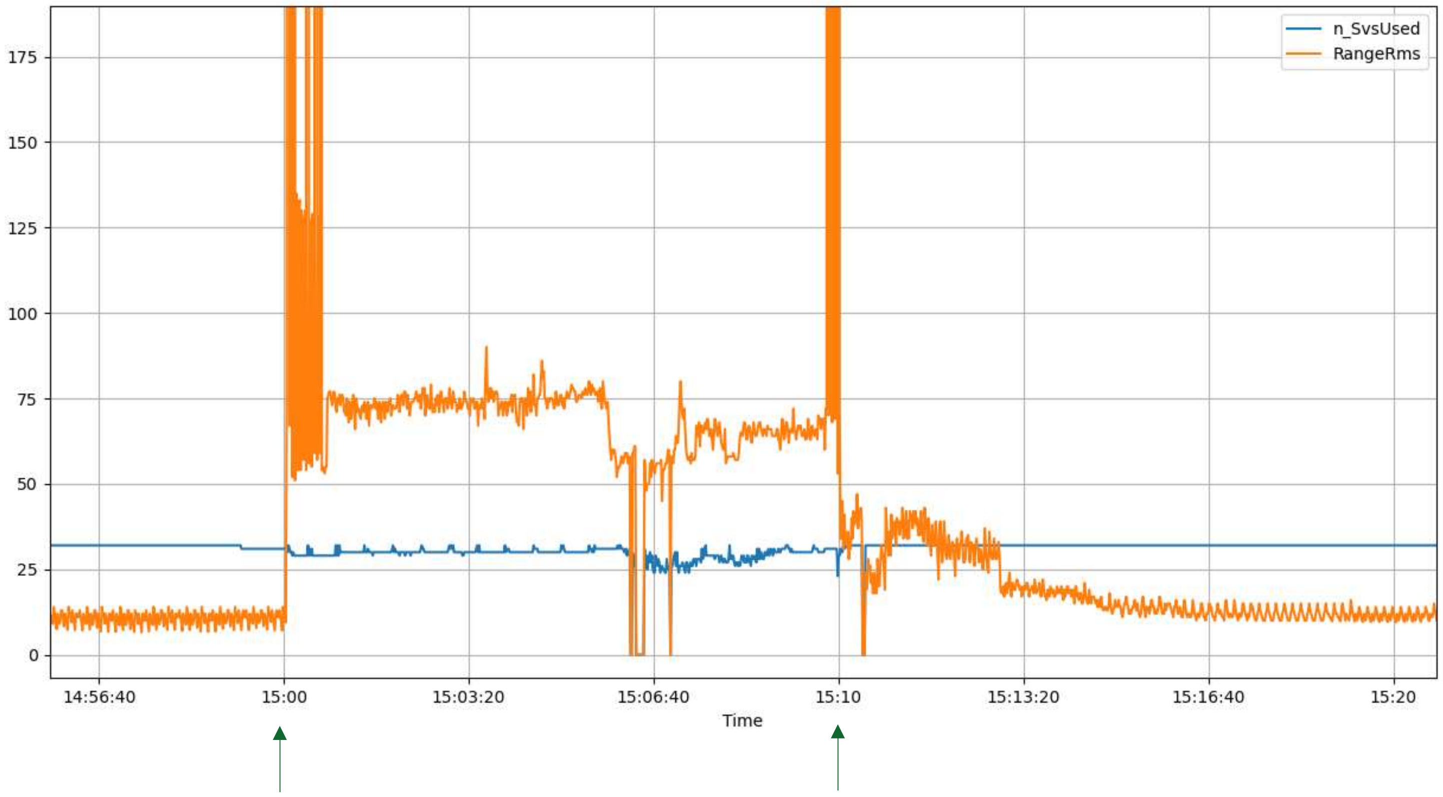


Kartverket

More advanced spoofing attack example (page 2)

Range RMS (a-posteriori sigma0) 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 sigma0 level (at least most of the time).



Spoofing starts

Spoofing ends

Conclusions, U-blox F9P positioning

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 tests done (the meaconing signals are experienced as jamming).

Spoofing:

+: The receiver resists the simplest spoofing attacks. Some attacks is 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.

Leica GR50

GR50 GNSS receiver.

AR20 GNSS antenna with choke ring

555 channels, multiple 1Hz native raw data logging and streaming including RTK corrections; Ethernet, Bluetooth, serial, slot-in module; USB host & client interfaces; PPS out, event input and external oscillator port.
Includes:

- Multi-constellation & multi-frequency package: GPS, GLONASS, Galileo, BeiDou, QZSS and SBAS.
- Server Package: RINEX, FTP push, Multi-client & Ntrip caster.
- Interference mitigation and event log.

Kartverket

Conclusions, Leica GR50

+ : Interference detection add-on seems to work very well.

- : Problems in 2023: Carl has the details ☺

Questions?

Contact information

→ Anders Solberg

→ anders.martin.solberg@kartverket.no

Kartverket

Kartverket