GNSS interference monitoring system

Kibrom Ebuy Abraha

NKG Science Week 2024, Reykjavik, ICELAND
12-14 March 2024

LANTMÄTERIET

GNSS Vulnerability

GNSS Cybersecurity

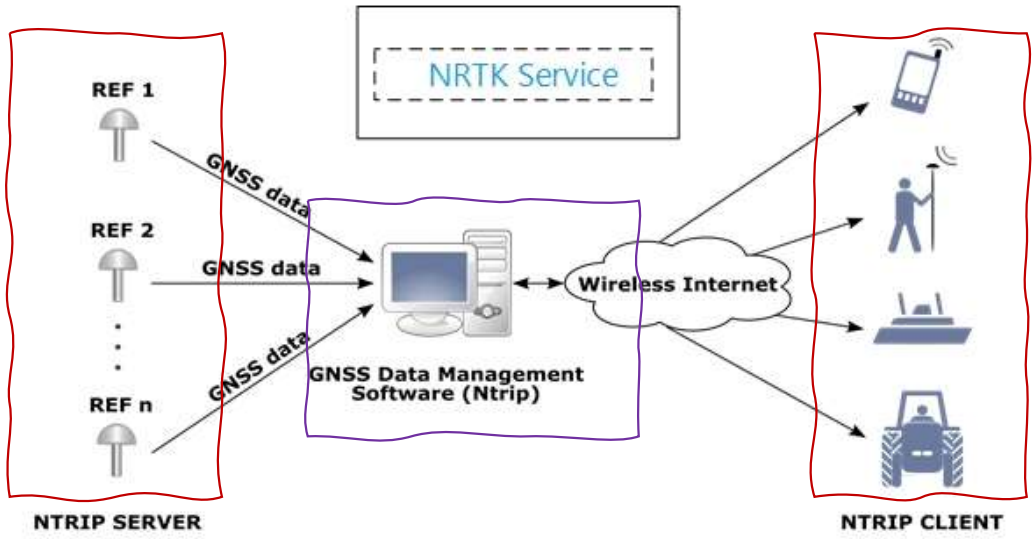
Space Segment

- Space weather
- Satellite attacks

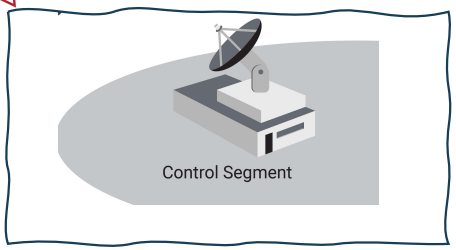
When will Russia attack GPS? Interview with former CIA analyst George Beebe

February 24, 2022 · By Dana Goward · Est. reading time: 3:30

User Segment



- System hack



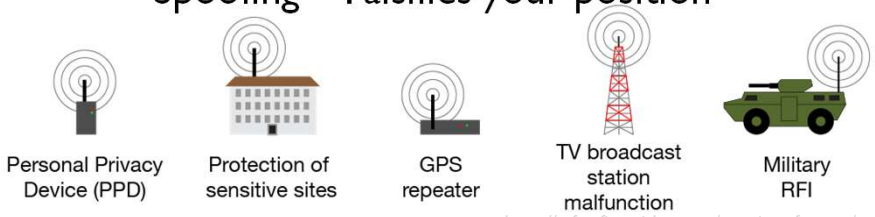
GNSS Interferences

- Jamming
- Spoofing
- Meaconing

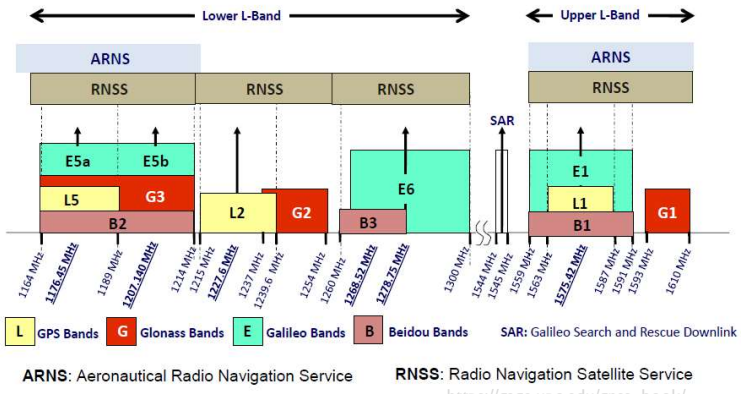
- System hack

GNSS interference threats

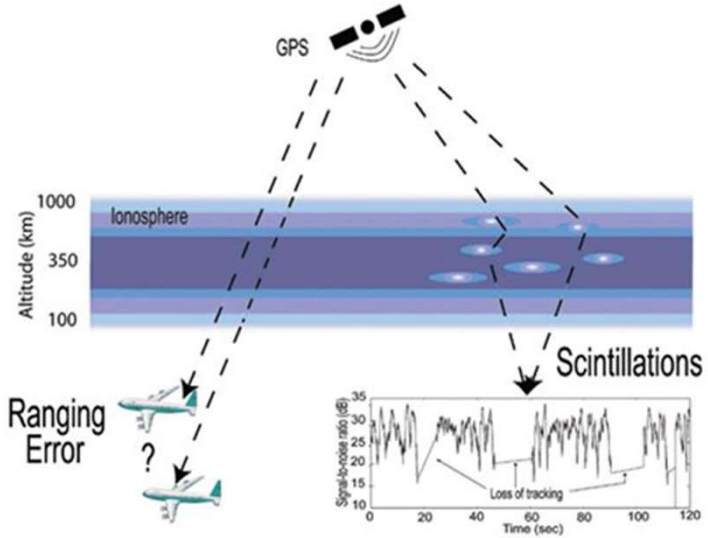
- GNSS signals have low power which can easily be disrupted
- Wider frequency bands
- Increased (un)intentional sources
  - Unintentional
    - Multipath, intersystem
    - Ionospheric scintillations
    - Radio Frequency Interference (RFI)
    - GNSS receiver, antenna
  - Intentional
    - Jamming – Disrupts your signal
    - Spoofing – Falsifies your position



https://safetyfirst.airbus.com/gnss-interference/



https://gage.upc.edu/gnss_book/



http://www.nap.edu/catalog/12507.html

More Russian GPS jamming than ever across border to Norway

Four passenger aircraft have over the last few days lost GPS signals when flying in Norway's northeastern region. Since Russia's invasion of Ukraine, jamming has been registered more than 20 days.

This article is more than **2 years old**

Finland reports GPS disturbances in aircraft flying over Russia's Kaliningrad

Australian aircraft's GPS receiver jammed by alleged Chinese warships

March 23, 2023 - By Maddie Saines

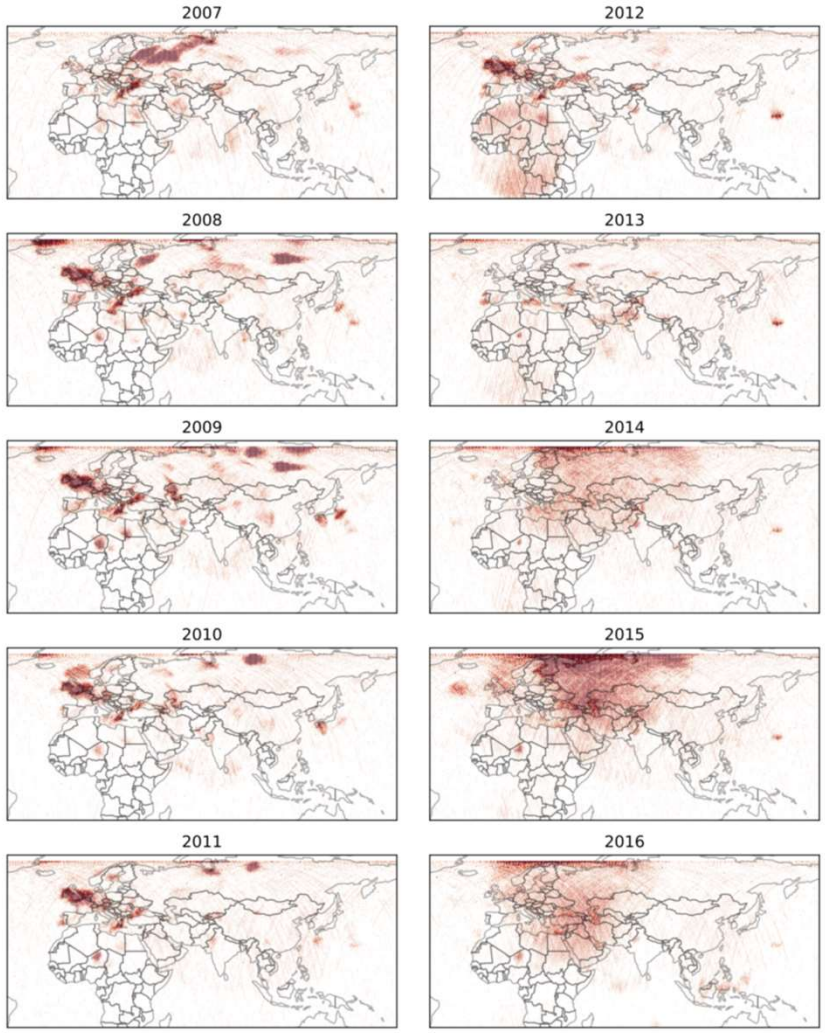
Transport

Agency confirms GPS jamming in Finland on NYE

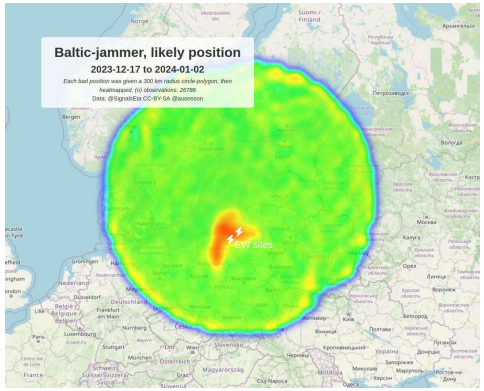
MILITARY & DEFENSE

Nordic countries are struggling to fly planes

- **Temporal variations of RFI over Europe, Asia, Africa**
- **Russia-Ukraine conflict effect visible in 2014-2016**
  - **Roberts M et al 2021**



Baltic Jammer



Forbes
https://www.forbes.com › ... › Aerospace & Defense

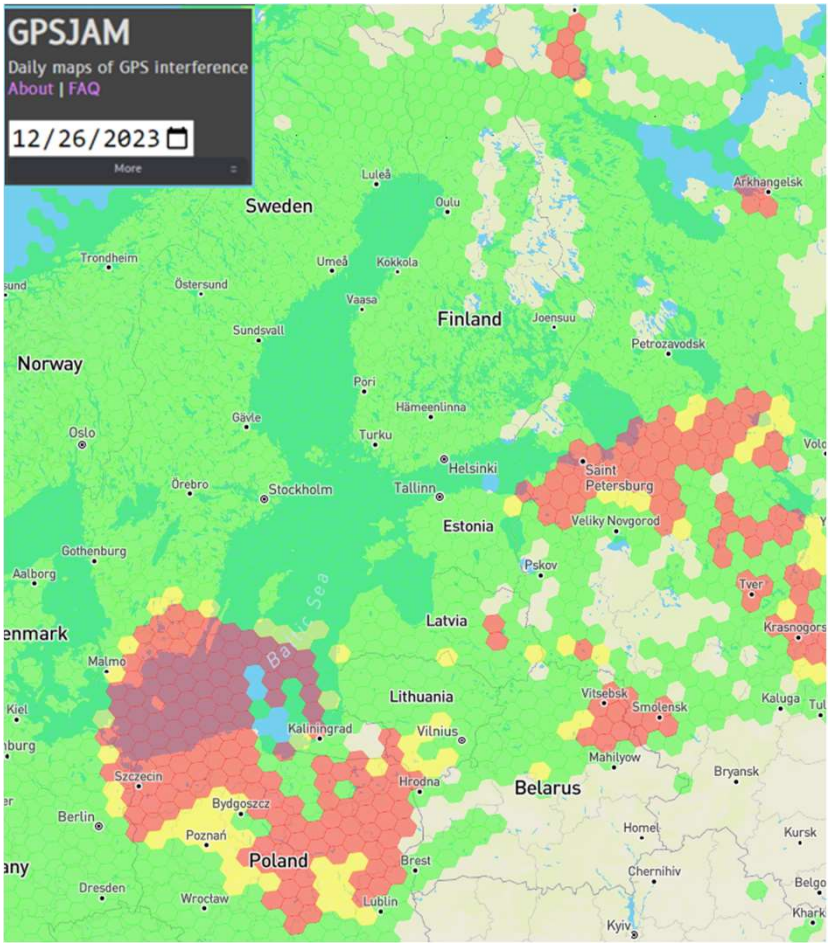
GPS Spoofing Is Now Affecting Airplanes In Parts Of Europe

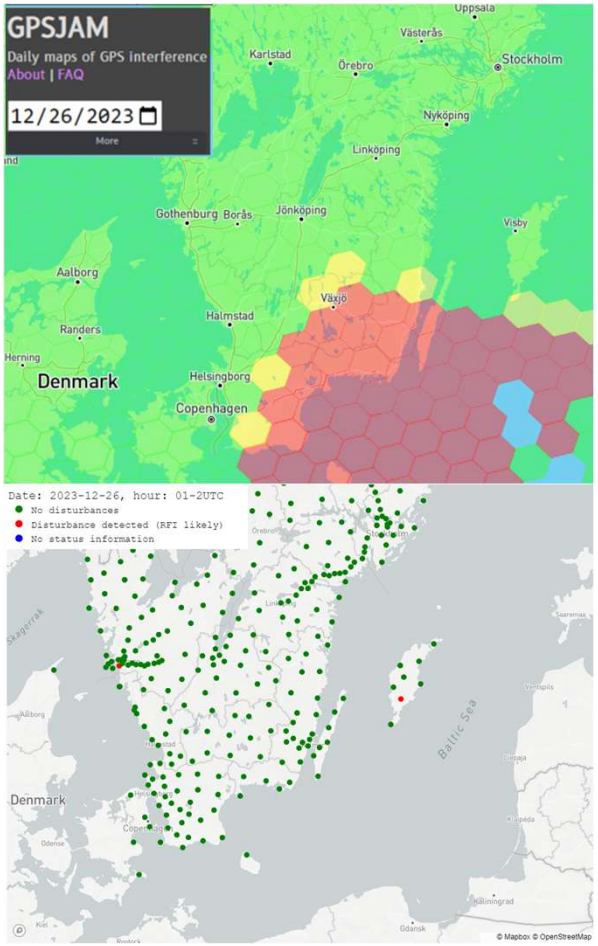
EU response to GPS jamming and spoofing

31 1 2024

GPS-Based Devices in Baltic States Disrupted

Russia has jammed signals to thwart Ukrainian drones





SWEPOS GNSS Signal disturbance monitoring and detection - Goals

Monitor

- Monitoring of anomalous events
- Using GNSS geodetic infrastructure – SWEPOS (not external monitoring system)
- Characterizing GNSS signals
- Monitoring signal strength
- Consistency check

Detect

- Detect anomalous events
- Classify anomalous events
- Multipath? Equipment failure? RFI?

Respond

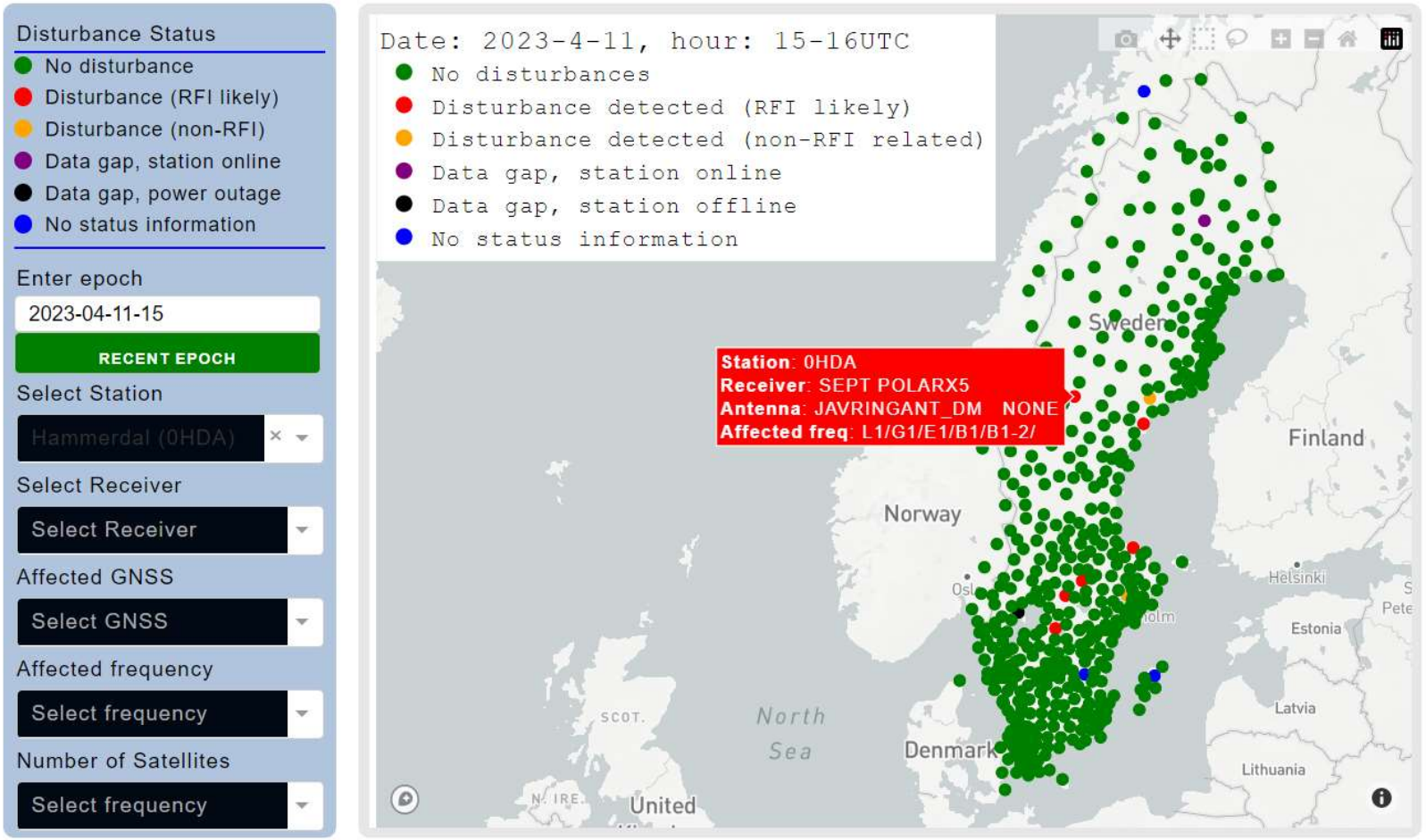
- Contain the event
- Geolocate the source
- Assess the impact and continuity of the event
- Mitigate it
  - Receivers, softwares
- Inform users

Unmitigated interference

- Flag off the station
- Move the station
- GNSS dependent Infrastructures should have a clear plan of recovering their system in the event of large scale attacks and have other alternatives.

SWEPOS® GNSS interference Monitoring

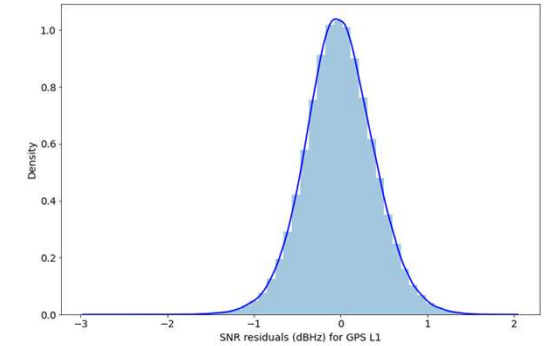
- Monitors all Swepos stations + third party stations = ~544 stations

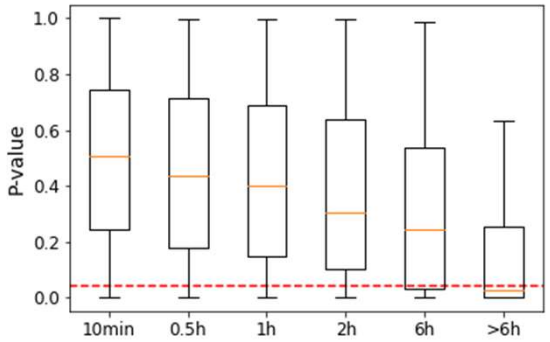


SNR residuals characteristics

- Model SNR for each satellite (it takes receiver, elevation, azimuth, power flex, and other dependent effects into account)
- Get SNR residuals (model – data) for each satellite

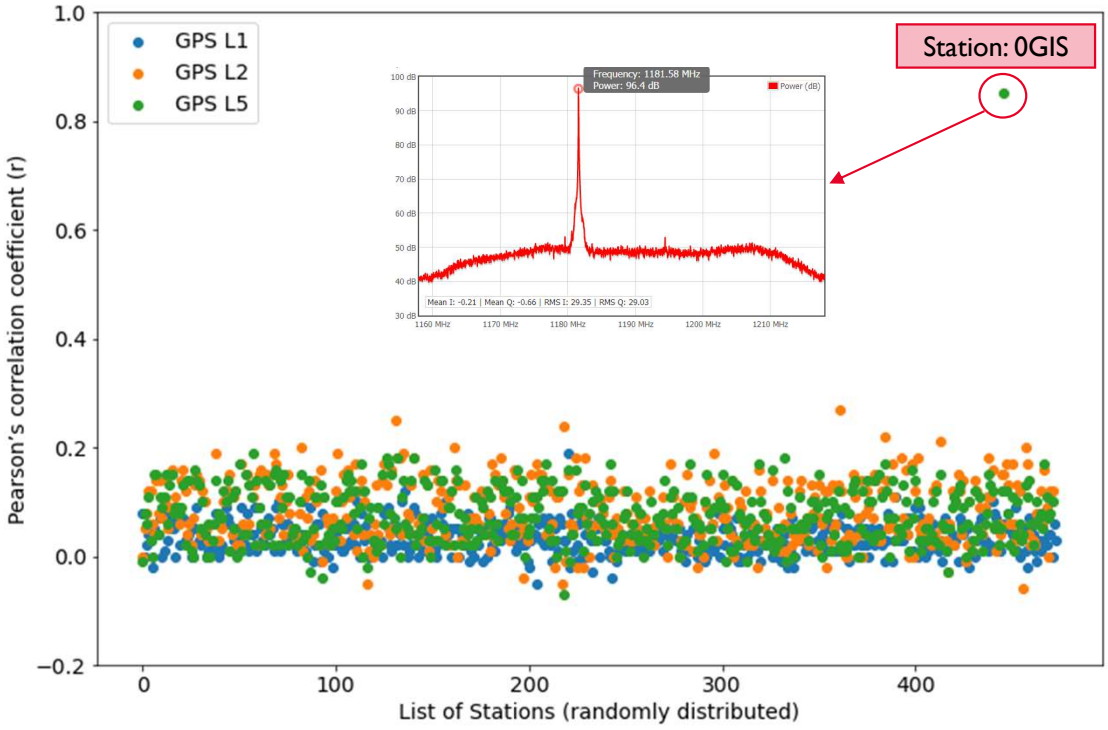
- SNR changes slowly unless interference is present
- Over a short period of time SNR can be treated as a stationary process
- Normally distributed
  - Shapiro-Wilk normality test of SNR residuals
  - Null hypothesis – residuals are normally distributed
  - Null-hypothesis is rejected for p-value < 0.05 (red-dotted line)
  - SNR residuals normally distributed over shorter periods
  - Over longer periods (longer than 6 hours), p-values fall below 0.05 for most of the stations





SNR residuals characteristics

- Cross correlation of SNR residuals among simultaneously tracked satellites.

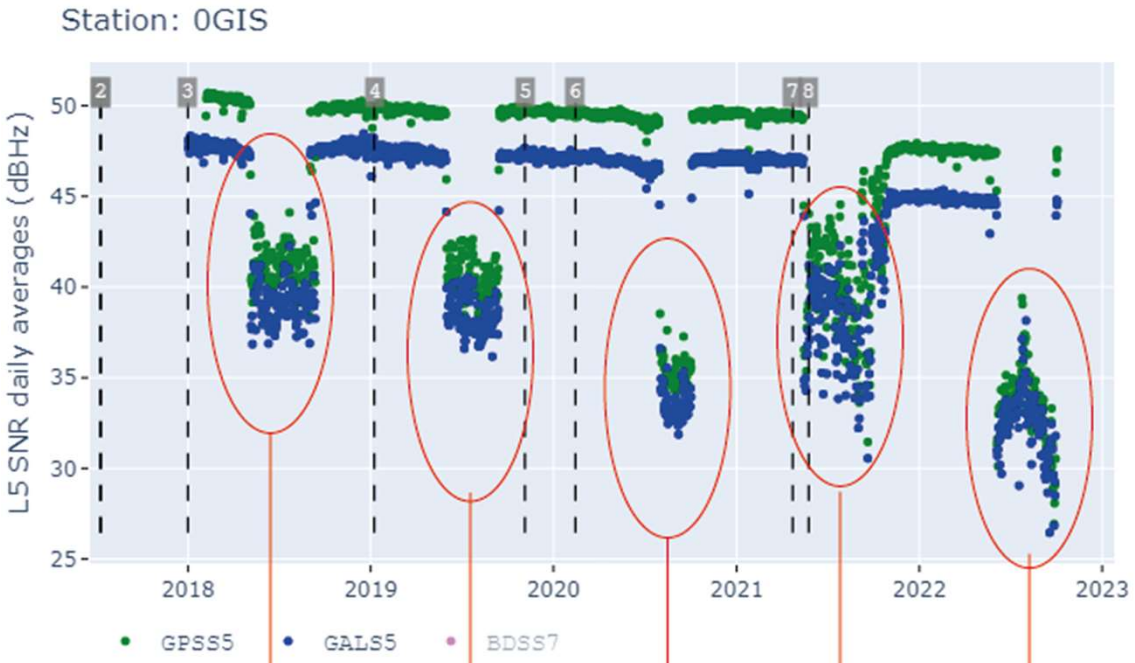


Key points of the detection system:

- In the presence of interference
  - Noise level increases, results in SNR drops
  - SNR residuals normally distributed over shorter periods
  - SNR are correlated among tracked satellites
    - SNR drops due to signal attenuation e.g., by trees and ionospheric scintillations won't be correlated among simultaneously tracked satellites

RFI-related actual interferences detected by the system

Real signal interference incidents at Grisselham (0GIS)



2018:
Started - May 6
Stopped - September 13

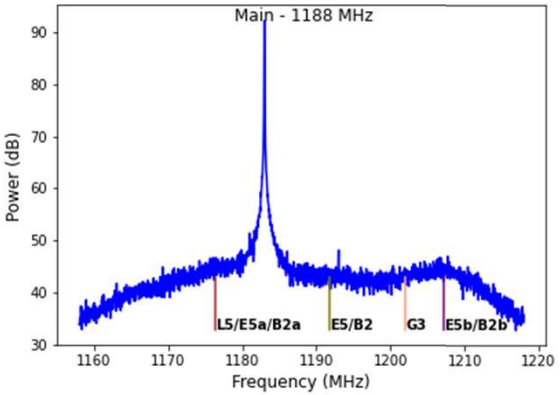
2019:
Started - June 1
Stopped - September 14

2020:
Started - July 31
Stopped - October 3

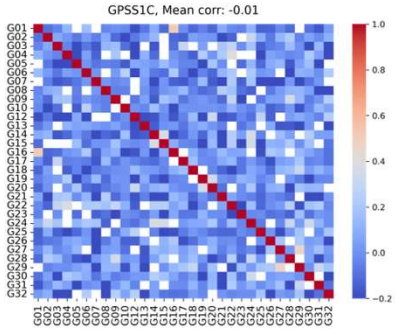
2021:
Started - May 15
Stopped - October 26

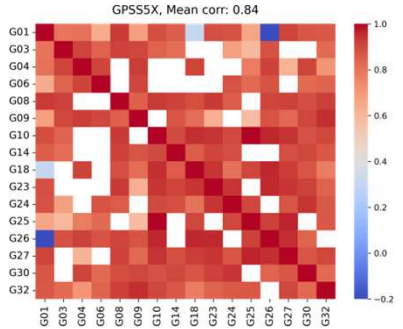
2022:
Started - June 4
Stopped - October 1

PTS located the source to be a boat.
The boat left the port on 1 October.
The disturbance has since ceased.
The source seems that same boat coming every year.
PTS will follow up for more information on the equipment



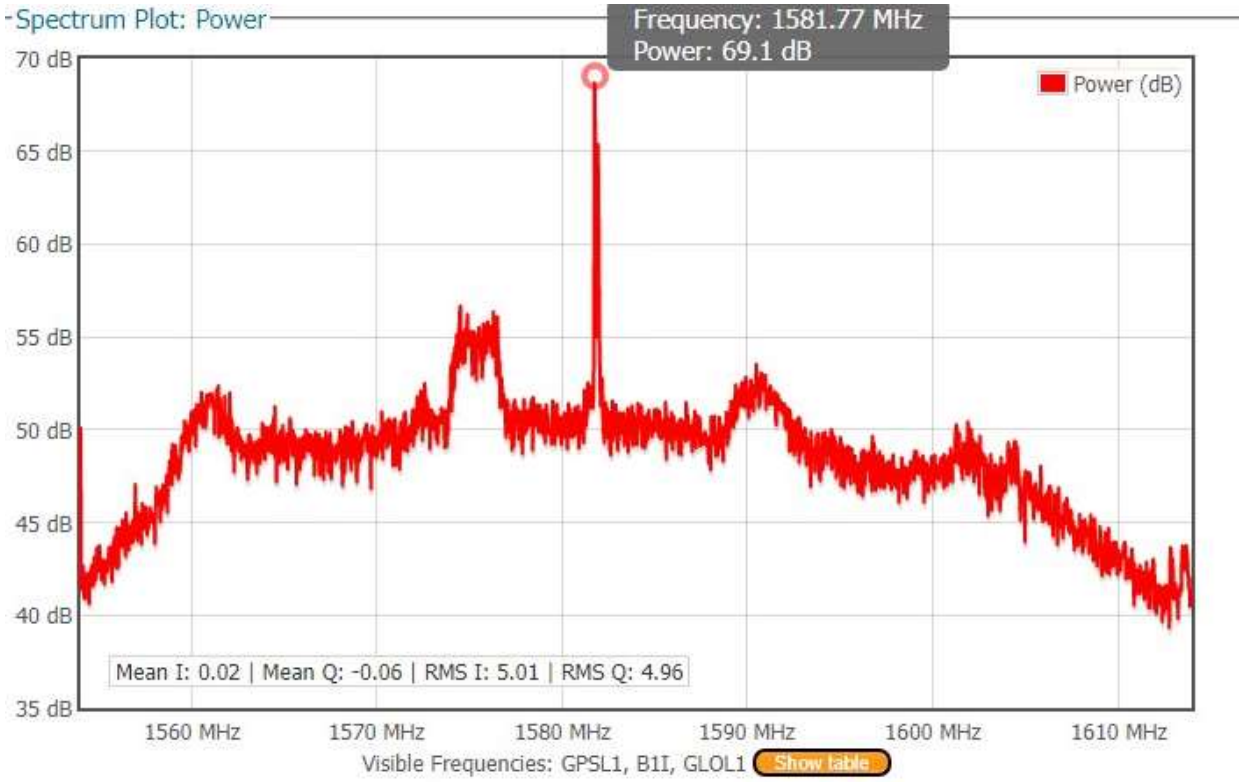
- RFI centered at 1181.0 MHz, but affected a wideband (-5 MHz to +26 MHz)





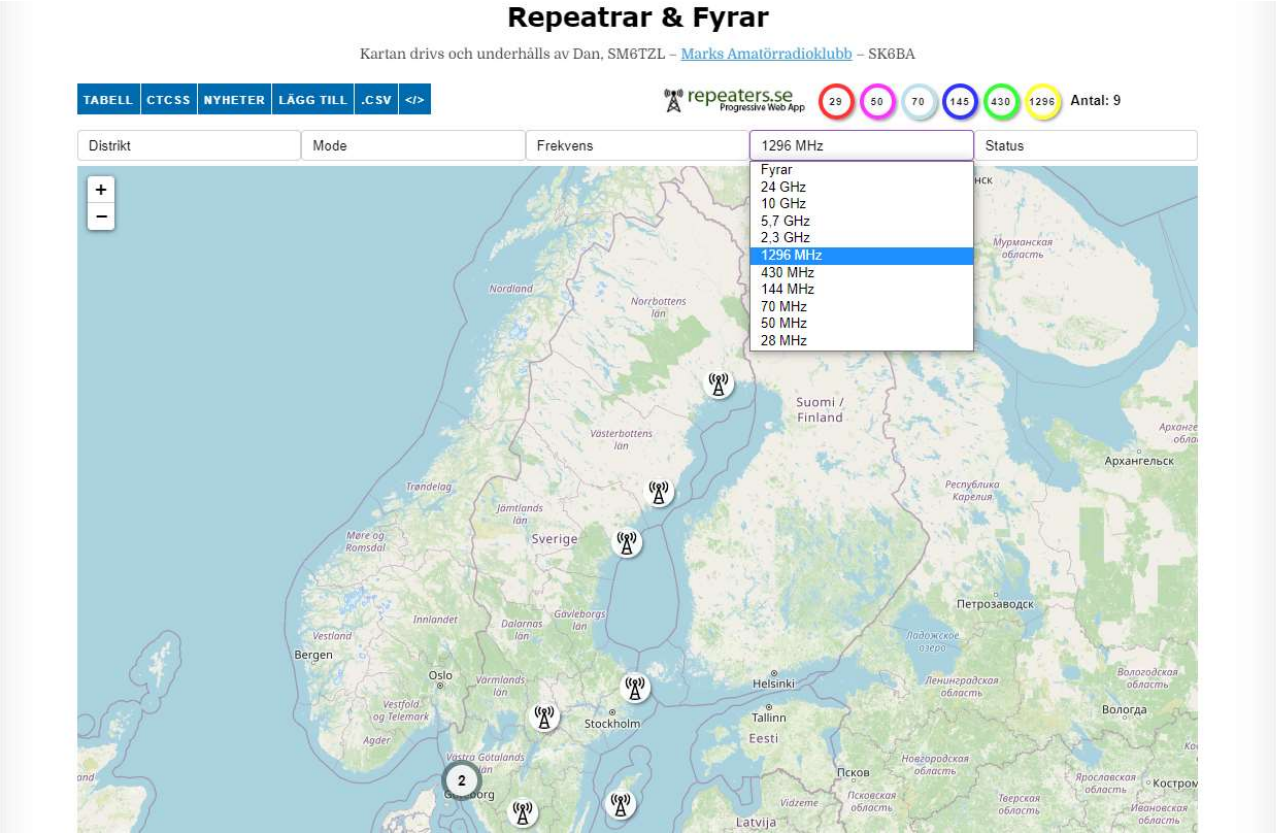
L1 disturbance – source located and contained

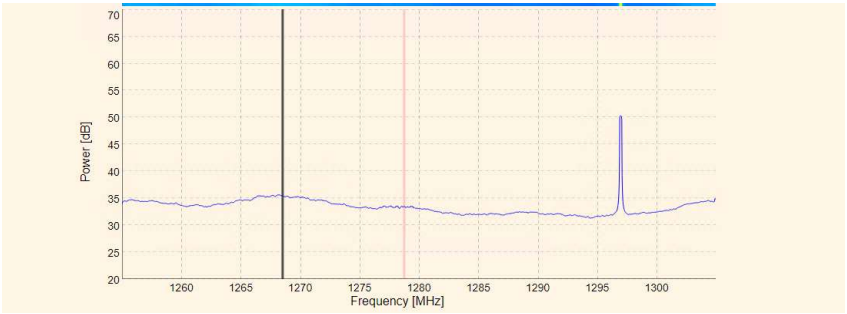
- RFI centered at 1581 MHz (~L1)
- 20-30 dBHz above the noise floor
- 5-6 MHz away from L1 center
- Affected GPS/GLO/GAL L1
- Detected at more than one station.
- Didn't have a major import on the performance of the station
- Source was located and contained, **GPS repeater in a lab**

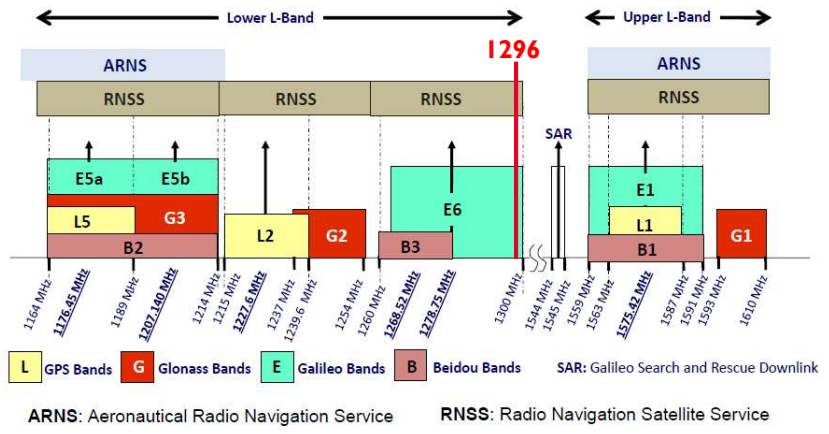


Radio Amateurs – Beacons at 1296, affecting Gal E6

- Six SWEPOS stations affected
- Why affecting Galileo E6?
  - E6 transmission can extend to 1296
- B3 is also slightly affected

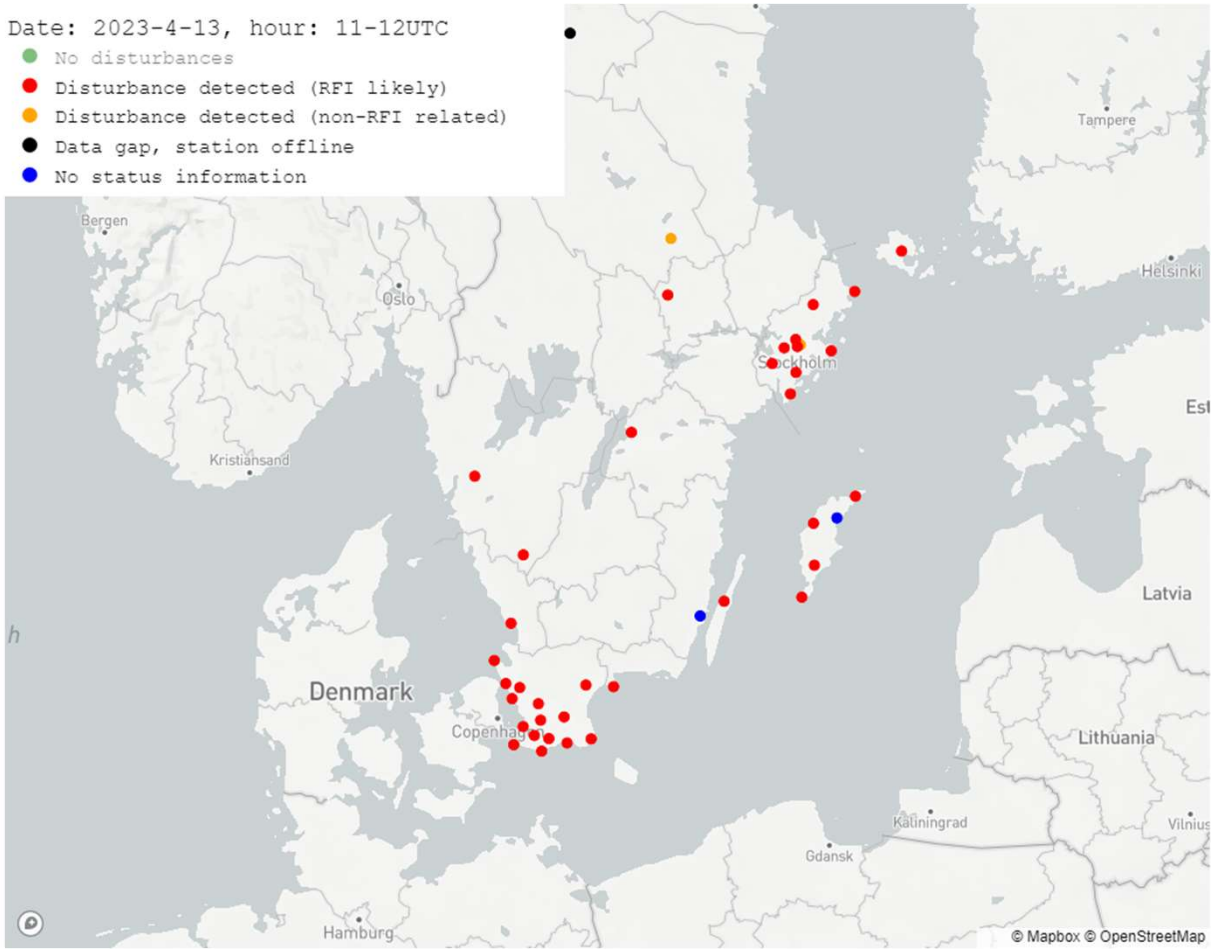






RFI Regional disturbance

- RFI centered at 1260, and1325 MHz
- Affected GPS/GLO L2, BDS B3, Galileo E6
- Detected by several stations simultaneously
- Negligible impact on users
- PTS confirmed/detected the interference



Future development plans

- MSB – The Swedish Civil and Contingencies Agency granted us with funding for further development

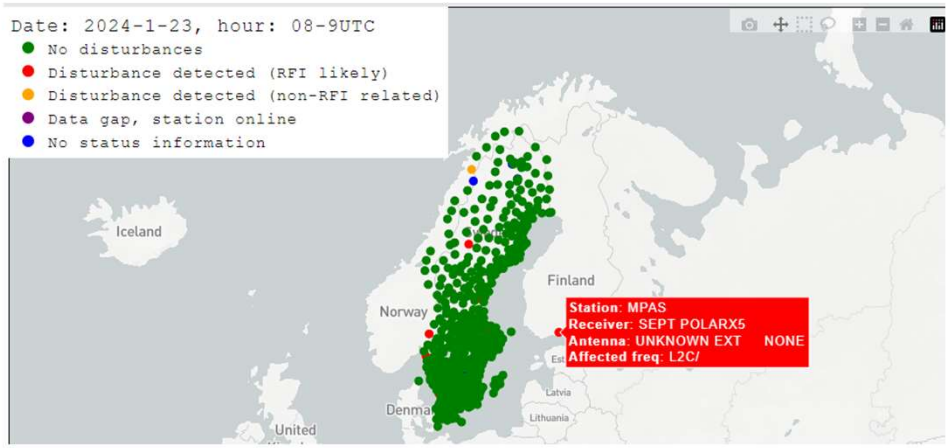
- Development includes
  - Monitoring web and API
  - Real-time monitoring service
  - Improvement of detection algorithm, support it with more parameters statistical characterization of AGC values
  - The plan is to deliver the new development at the end of the year
  - Initial planning starts in April

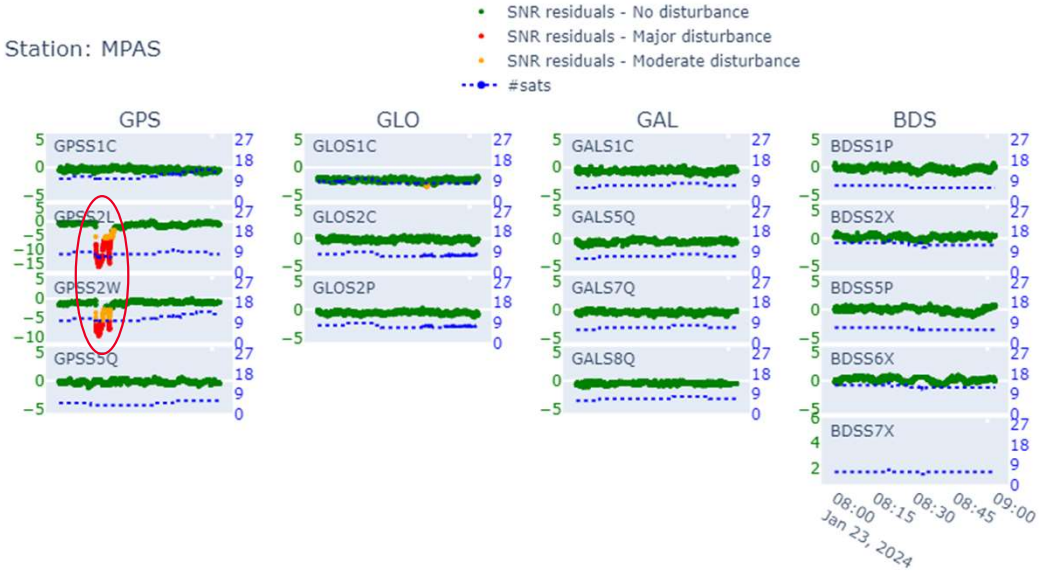
NKG collaboration

NKG meeting in Copenhagen, April 2023

- Session/ topic: Interference (jamming and spoofing)
  Peter and Kibrom will discuss the possibility to include other countries into their interference monitoring system.
  Task force is active

- A station MPAS from Finland has been added
- We have access to the streams of the SRX messages
- Added to our monitoring in January 2024
- We have not established an automated way of sharing disturbance status information
- L2C disturbance that lasted about 5 minutes detected by both Swedish and Finish monitoring systems





Nordic cooperation suggestions

- Joint Monitoring Stations
- Intererence information sharing and emergency response coordination
- Collaborative research and development within the GNSS cyber security
- Interference monitoring reporting standards and guidelines

Takeaway!

- The SWEPOS interference monitoring system has been effective in detecting signal disturbances of different sources
- No impactful interreferences for the NRTK service were detected, only on single stations
- No disruptions to the NRTK service due to the recent GNSS disruptions in the Baltic region

- **Nordic-scale interference monitoring system would provide more comprehensive coverage and better situational awareness of GNSS interference events in the region – demands Nordic cooperation**

- Monitor-Detect-Respond
  - The goal is to protect critical GNSS and GNSS-dependent infrastructures against emerging (un)intentional threats; we should also use the same infrastructure for autonomous signal-situation awareness of threats.
  - Receiver and antenna manufacturers should consider interference threats when developing high-end GNSS receivers.
    - Users should make this part of a procurement when making receiver/antenna purchases