Resilience and Security of Geospatial Data for Critical Infrastructures

Session 6: Resilient Position, Navigation and Timing (PNT)

United Nations/Finland Workshop on the Applications of GNSS

October 24, 2023

Helsinki, Finland

Prof. Zahidul Bhuiyan

Finnish Geospatial Research Institute

Agenda

1. Background

2. Actual impact

3. Resilient PNT Actions at FGI

4. Recommendations

Background

- GNSS, being the backbone of any global scale navigation system, offers accurate PNT in good signal conditions but is vulnerable to jamming/spoofing

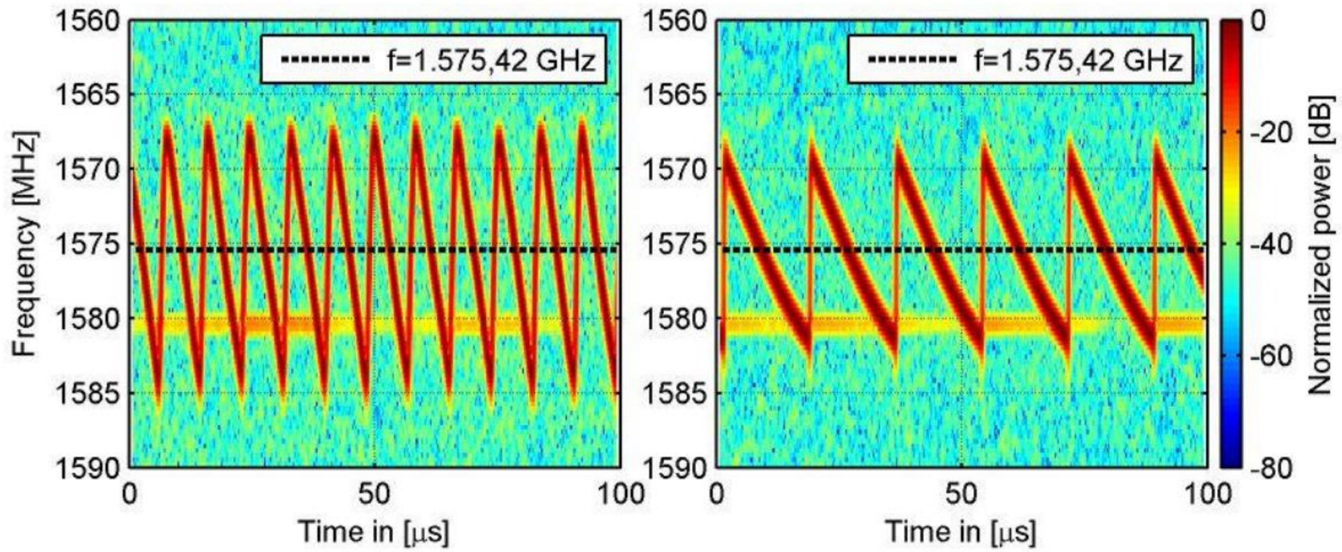
  => due to weak signal reception and open unprotected signal authentication provision

- Heavy dependence on GNSS-based PNT systems has made jamming/spoofing a growing threat
- There has been a considerable upsurge in GNSS vulnerability incidents due to the advancement of affordable software-defined radios, signal simulators, cheap availability of jammers, and a broader understanding of spoofing as an effective disruption strategy against GNSS-based applications.

Radio Frequency interference

In short: unwanted signal at GNSS frequencies

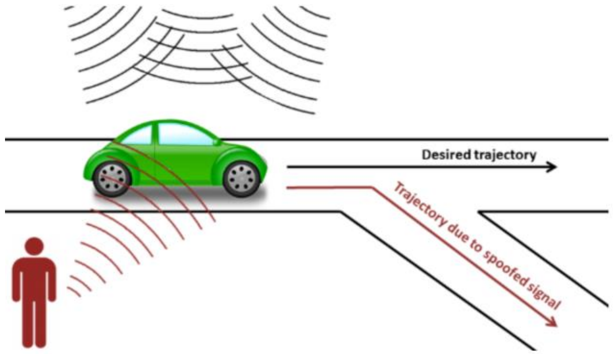
- Unintentional interference
  - Natural causes, e.g. ionospheric effects
  - Man made, e.g. faulty electronic equipment
- Intentional interference
  - Personal privacy devices
  - Criminal intent
  - State level electronic warfare
- Mitigation techniques
  - Receiver algorithms, Antenna design, Monitoring…

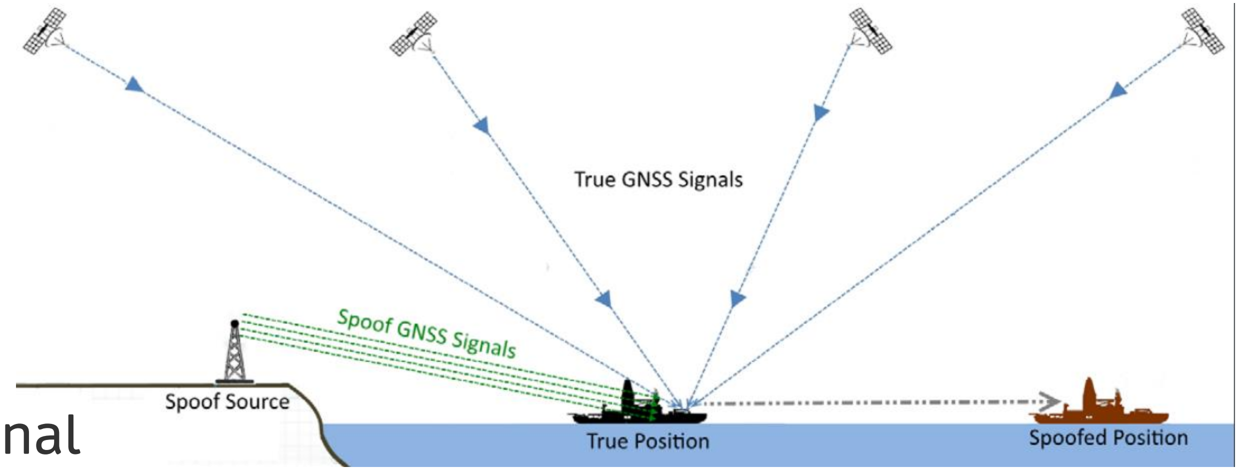


GNSS Spoofing

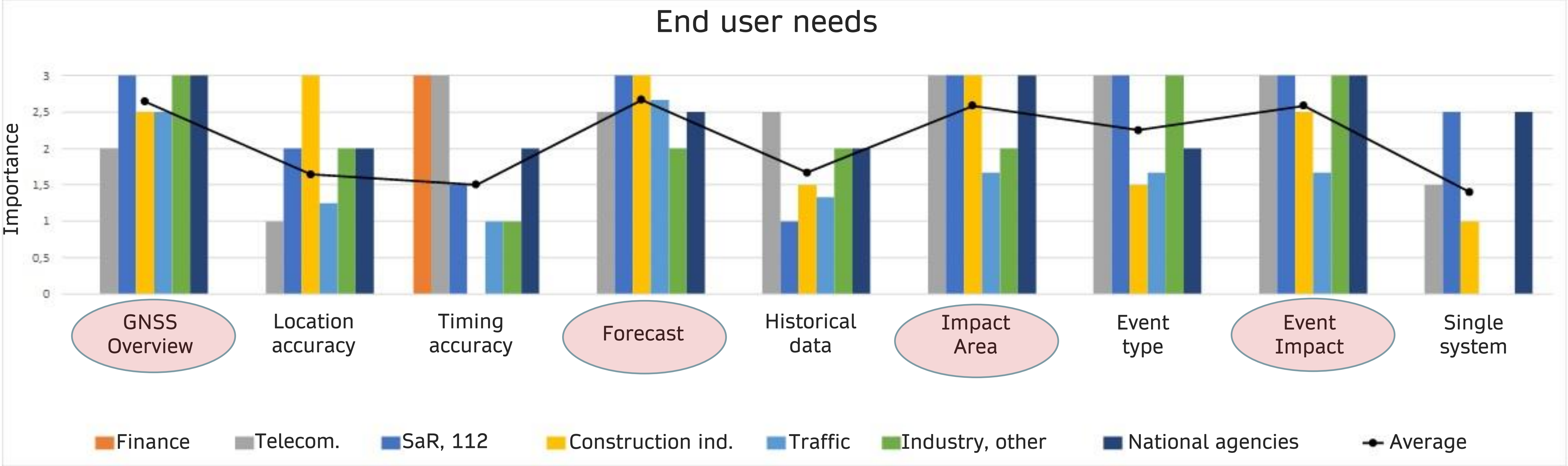
In short: Trick the receiver to use wrong position and/or time

- Can be either:
  - Targeted: time and/or location synchronised with target receiver
  - Untargeted, time and/or location are completely off
  - Meaconing, real GNSS signal repeated (with delay)
- Mitigation techniques
  - Navigation message authentication (Galileo OSNMA, ACAS and/or PRS), signal methods in the receiver





Importance of PNT as perceived by Finnish GNSS stakeholders



https://www.maanmittauslaitos.fi/sites/maanmittauslaitos.fi/files/GNSS_selvitys_loppuraportti.pdf

Agenda

1. Background

2. Actual impact

3. Resilient PNT Actions at FGI

4. Recommendations

Impact of spoofing on different COTS GNSS receivers

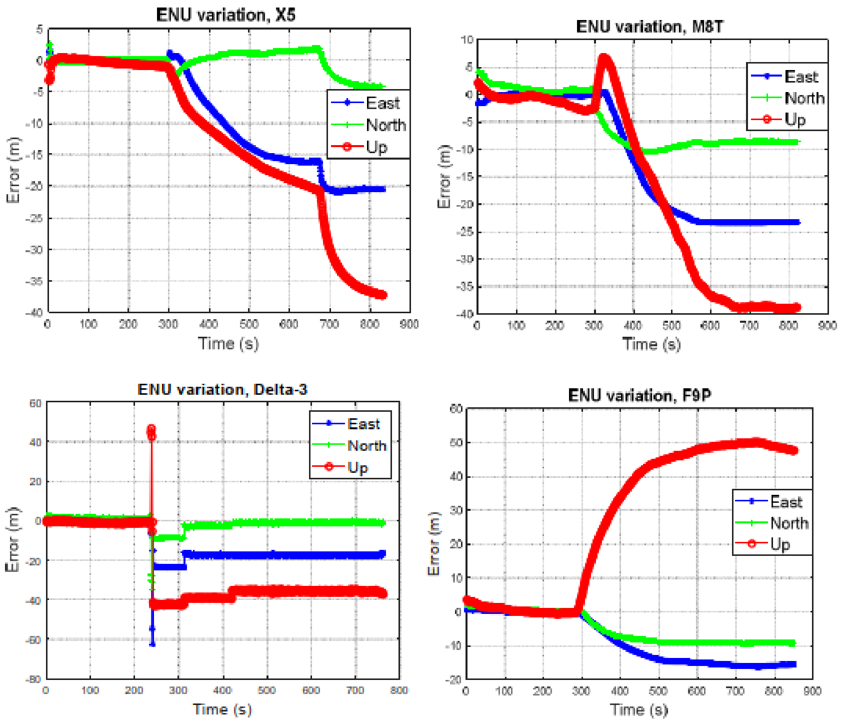
- 5 different receivers were tested under different types of spoofing attacks

TABLE VI. OVERVIEW OF SPOOFING IMPACTS ON DUTS

DUT	*Targeted spoofing*	*Untargeted spoofing*	*Meaconing*
	Spoofed?	Spoofed?	Spoofed?
M8T	YES	YES	NO
F9P	YES	YES	NO
X5	YES	NO	NO
Delta-3	YES	NO	NO
FGI-GSRx	YES	NO	NO

TABLE VII. SUMMARY OF SPOOFING IMPACT ON POSITIONING ACCURACY FOR LIVE-SKY SPOOFING ATTACK

DUT	ε_{3D}	ε_H	σ_H	ε_V	σ_V	*Availability (%)*	*Impact*
M8T	29.2	17.3	10.7	23.5	16.2	100	High
F9P	37.1	12.8	7.7	34.9	21.4	100	High
X5	21.6	12.1	8.2	17.8	12.3	100	High
Delta-3	34.8	15.9	8.7	31.0	17.0	89.6	High
FGI-GSRx	74.0	49.3	29.4	55.1	33.1	100	High

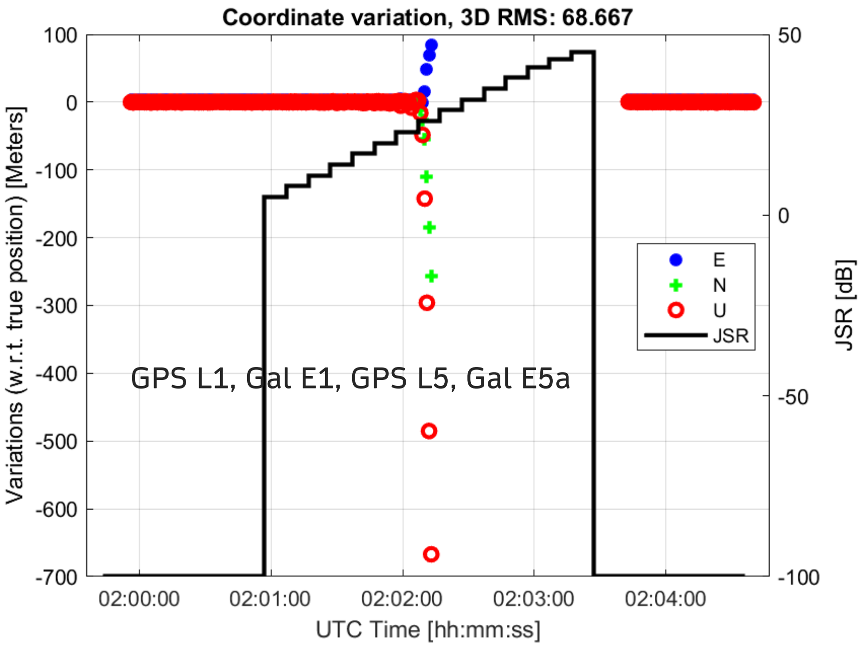


Varying spoofing impact on different GNSS receivers

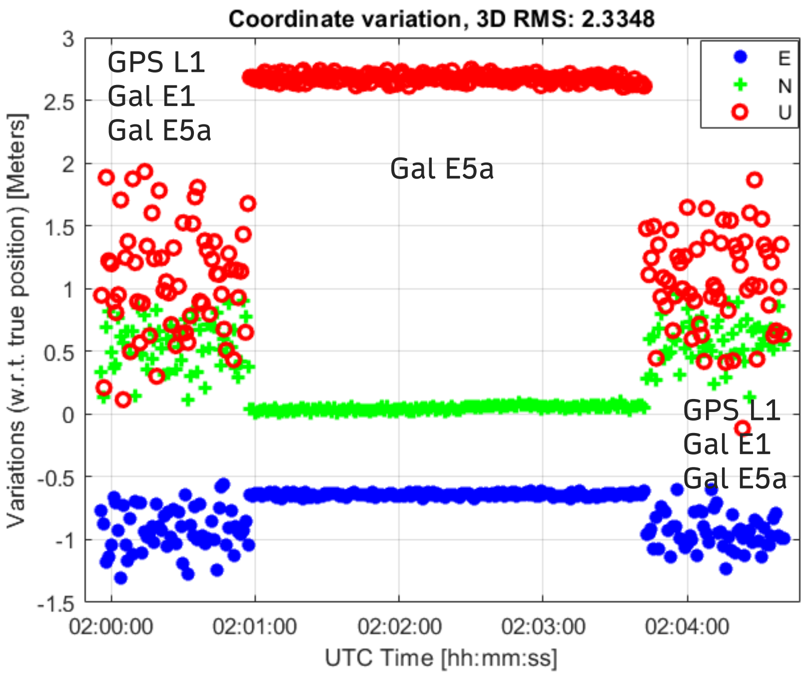
Islam, S., Bhuiyan, M. Z. H., Pääkkönen, I., Saajasto, M., Mäkelä, M., and Kaasalainen, S. (2023) "Impact analysis of spoofing on different-grade GNSS receivers," IEEE/ION PLANS 2023, April 24-27, 2023, California, USA.

Impact of high-power jamming on L1/E1 in terms of positioning accuracy

Scenario ID	GNSS Constellation	DUT scope	Comments
JAM-CH-S-02: - Static, Chirp wide (fast) in-band - L1/E1	- GPS L1 C/A - Galileo E1 - GPS L5 - Galileo E5a	<u>Mitigation</u>: - Interference detected on L1/E1 - MFMC based mitigation	- MFMC diversity is applied on-the-fly based on the detection of interference at signal level for each frequency



No Mitigation Applied



Mitigation Applied with AGC/IQ -based detection followed by MFMC mitigation

STRIKE3 International Monitoring Network

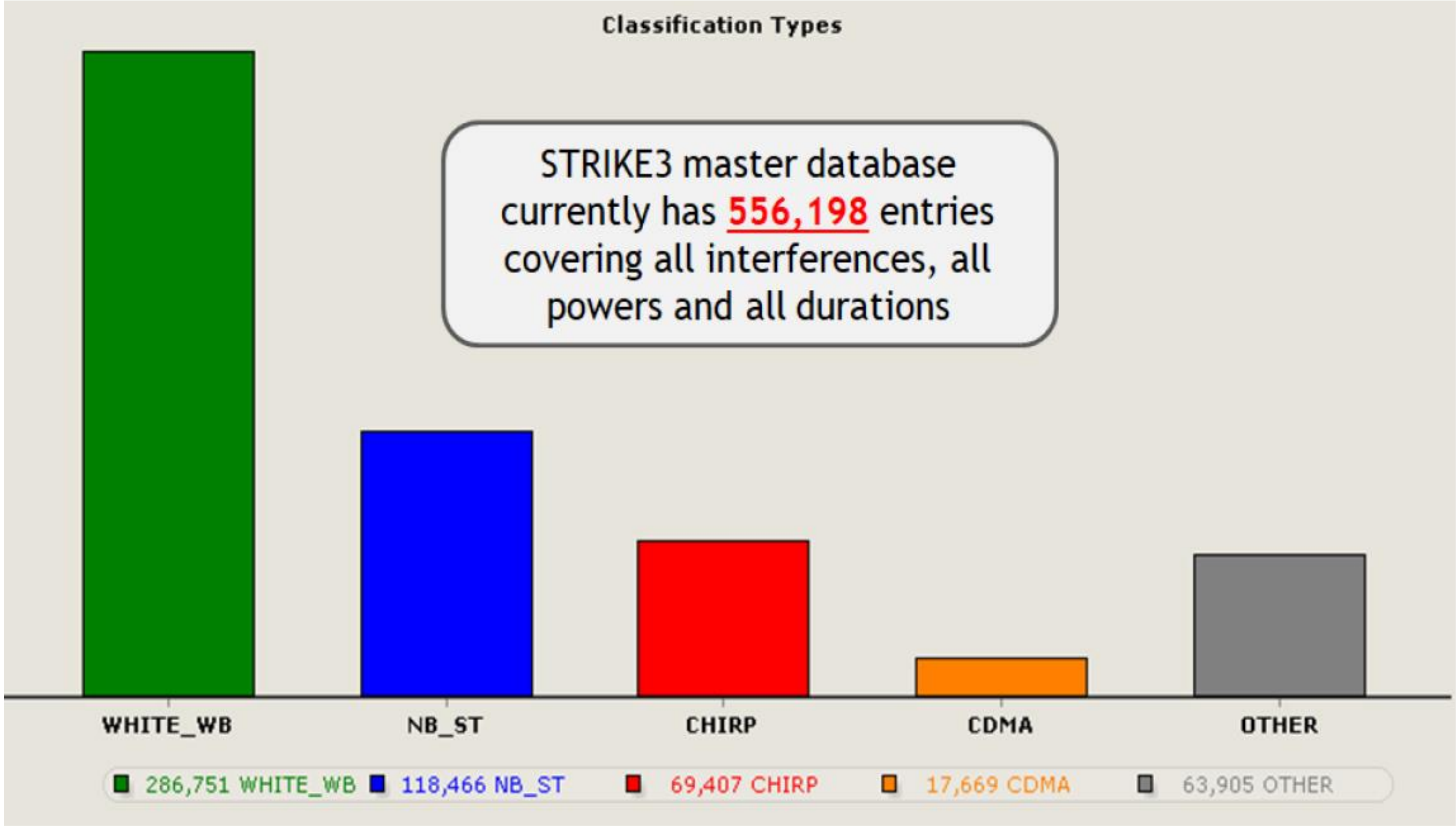
Across the globe

- United Kingdom
- Sweden
- Finland
- Germany
- France
- Poland
- Czech Republic
- Spain
- Slovakia
- Slovenia
- Netherlands
- Belgium
- Croatia
- Latvia
- New Zealand
- Canada
- India
- Vietnam
- Thailand
- Malaysia
- Japan

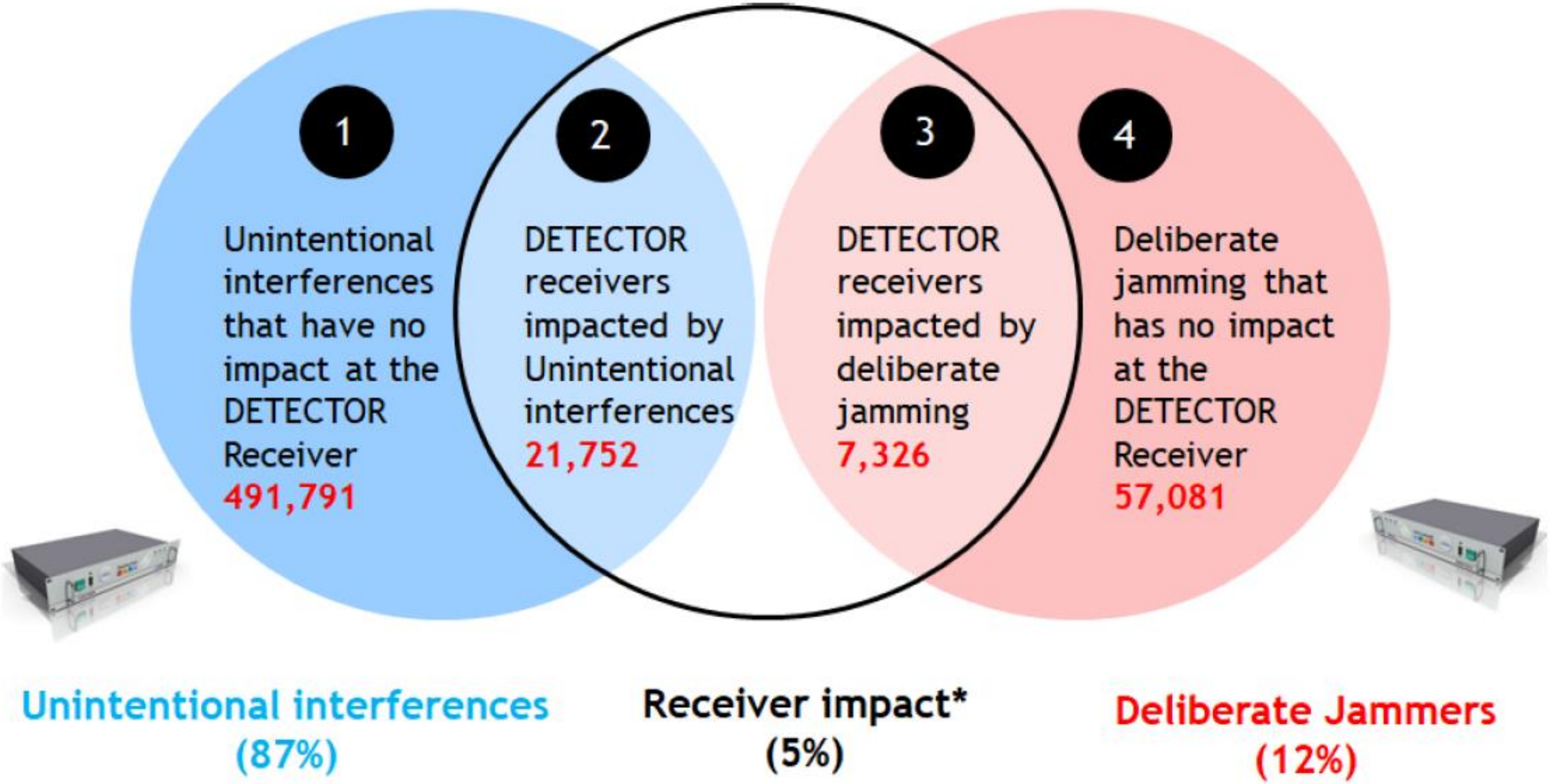
50 monitoring sites

STRIKE3 participant countries each have 3+ sites. **STRIKE3 Partnering countries** have had 1 or 2 sensors. Some countries have moved a sensor to multiple locations to try to build up a bigger picture. Typical duration of a monitoring campaign at a site has been between 3 – 24 months.

STRIKE3 Master Database (1/2/2016 – 31/01/2019)

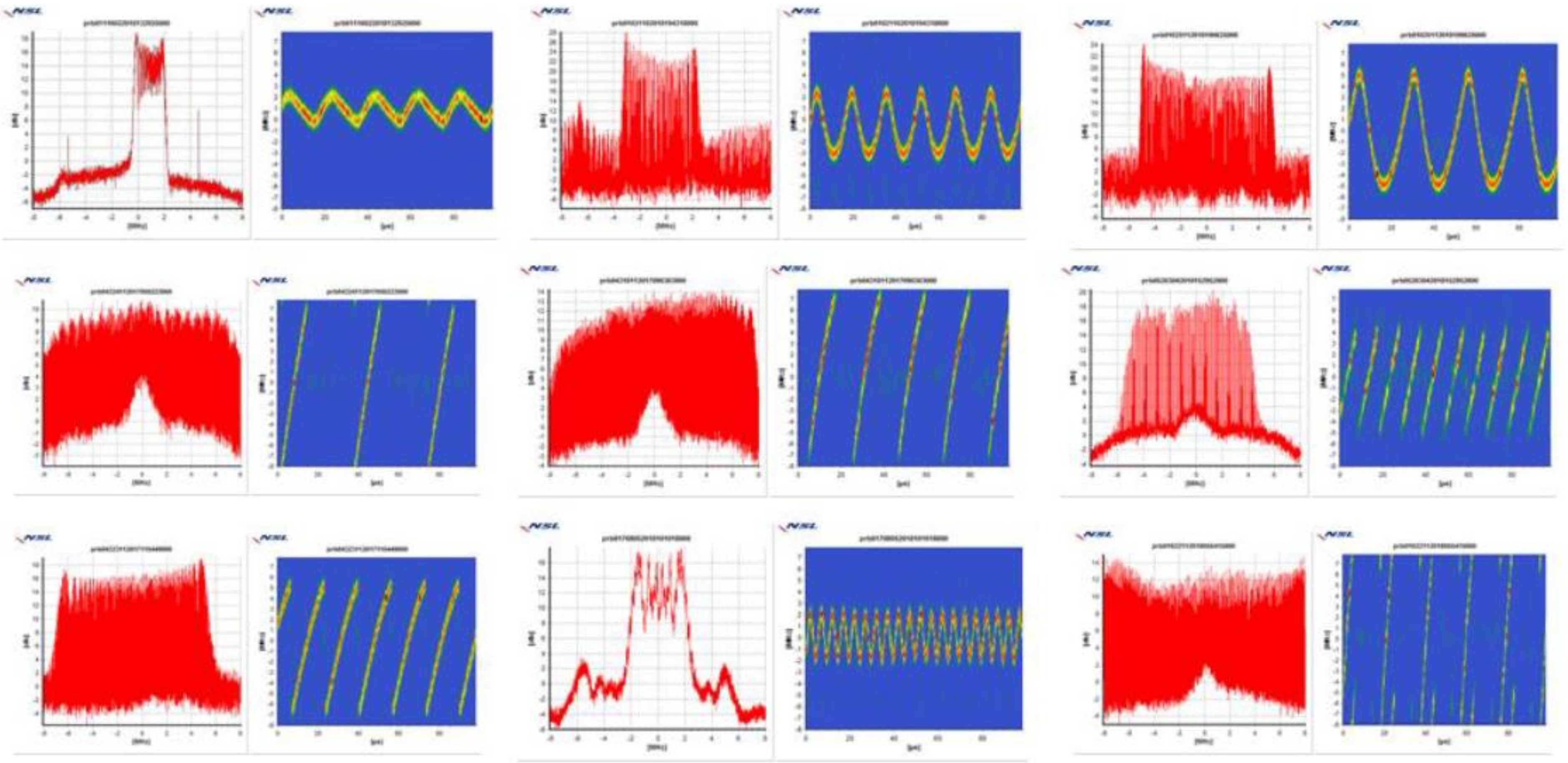


STRIKE3 Breakdown of **556,198** Events



2

7,326 *"jammers"* that **denied** GNSS



Distance and dynamics

Jammer power

Jammer effectiveness

Local factors

Agenda

1. Background

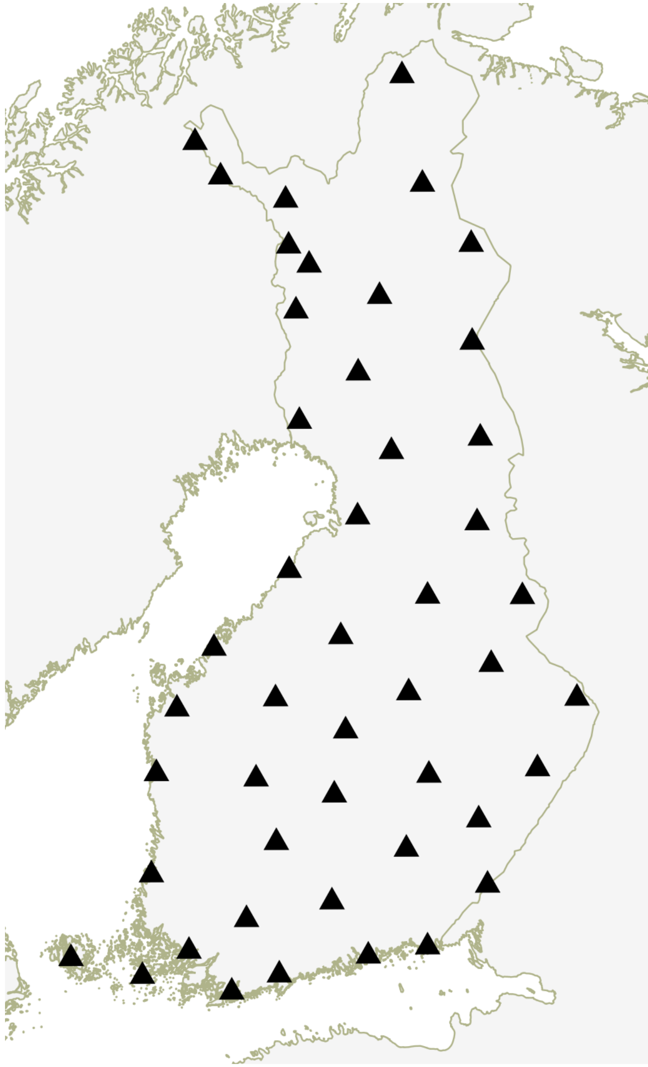
2. Actual impact

3. Resilient PNT Actions at FGI

4. Recommendations

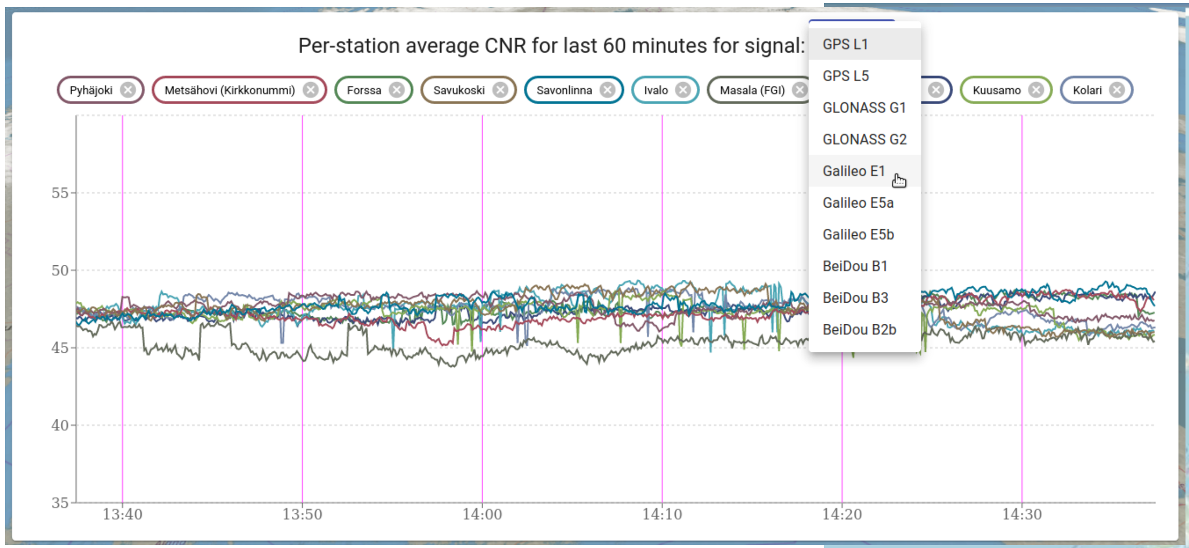
Finnish National Reference Network (FinnRef)

- **47 CORS** → Basis for the national reference frame, EUREF-FIN, few stations also serve as IGS stations, and also co-located with EGNOS RIMS
- All GNSS and multiple frequencies are observed
- Real-time positioning service 'FINPOS' uses FinnRef data to provide DGNSS, Network RTK measurement data
- Data format available in RINEX and real-time streams (RTCM MSM (GPS+GLO+GAL+BDS)

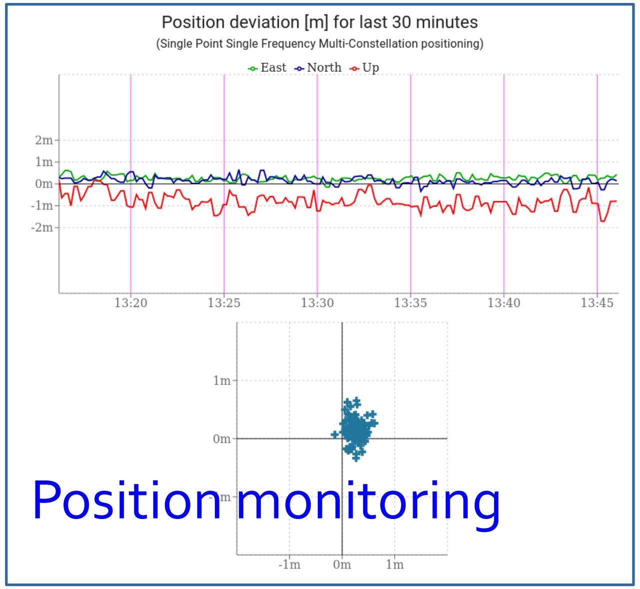


Typical FinnRef station

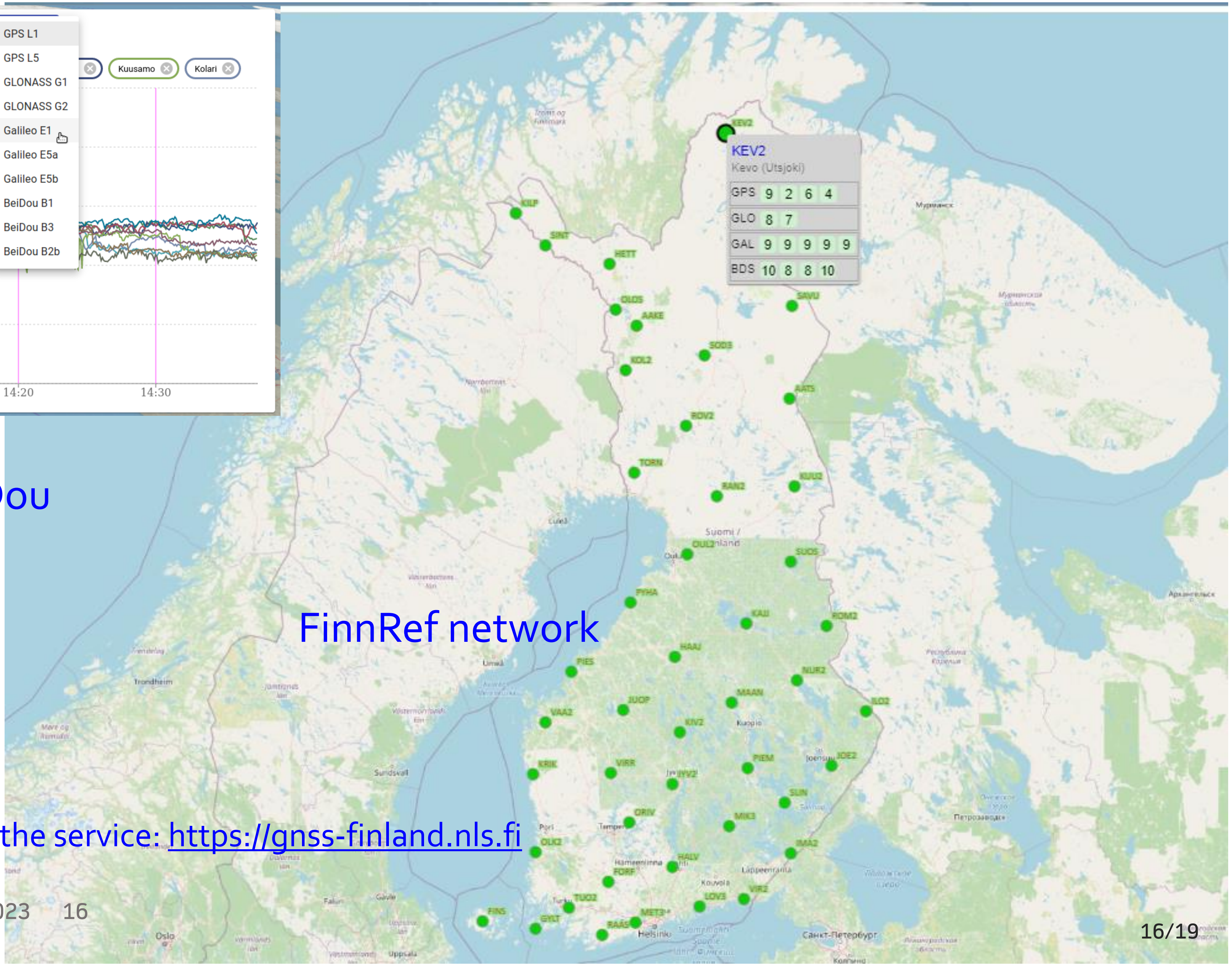
GNSS-Finland Service: Monitoring GNSS signal quality on all global constellations in multiple frequencies in 47 FinnRef stations



Signal strength of:
GPS, Galileo, GLONASS, BeiDou



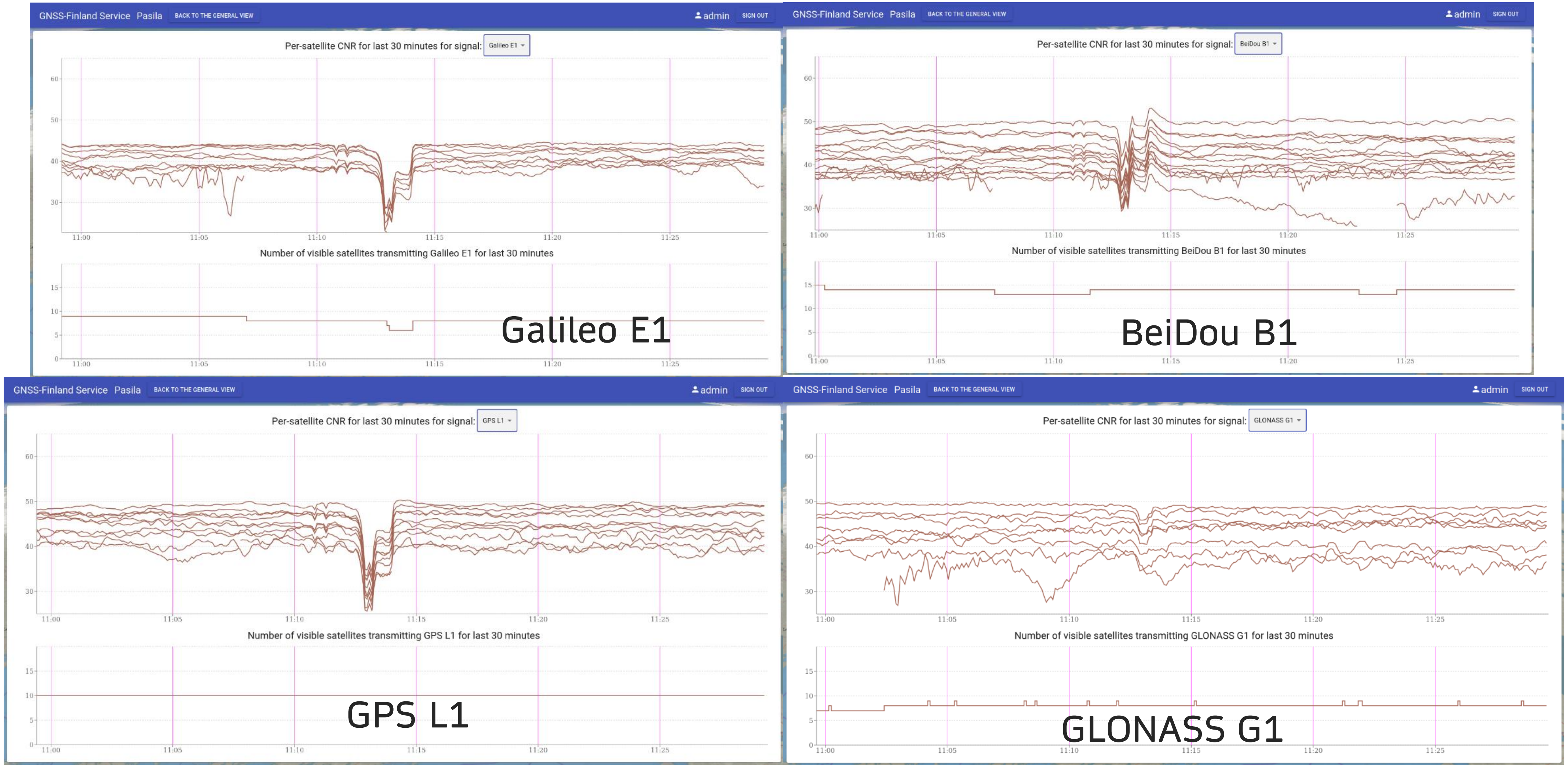
Position monitoring



FinnRef network

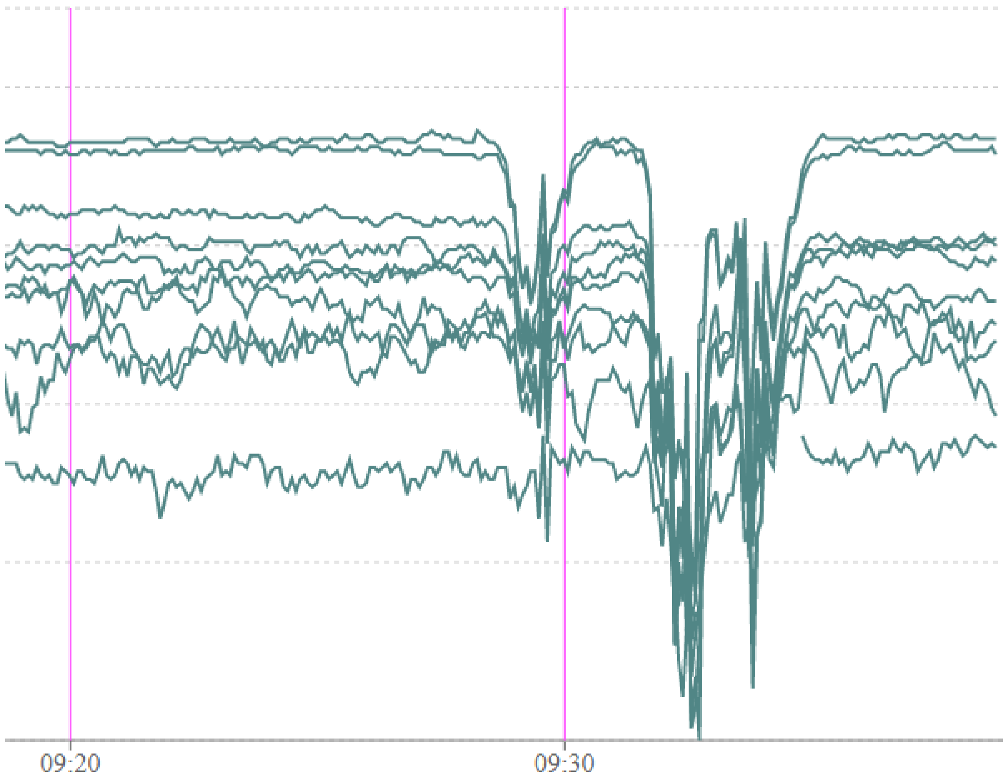
Link to the service: https://gnss-finland.nls.fi

Detected Jamming Incident in Pasila, Helsinki



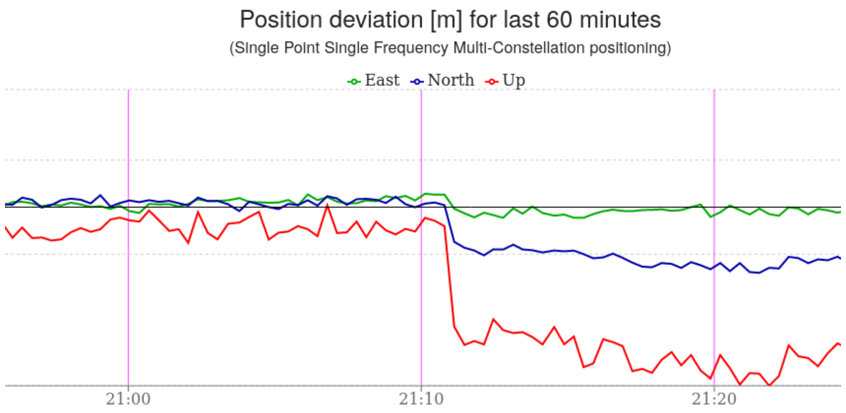
GNSS-Finland Service: Observed Event, Example 2

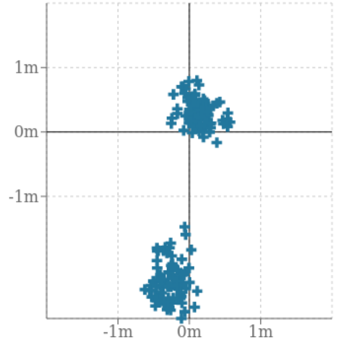
Metsähovi, GLONASS G1, C/N_0 drop



20. Jan 2021

Gyltö, position bias

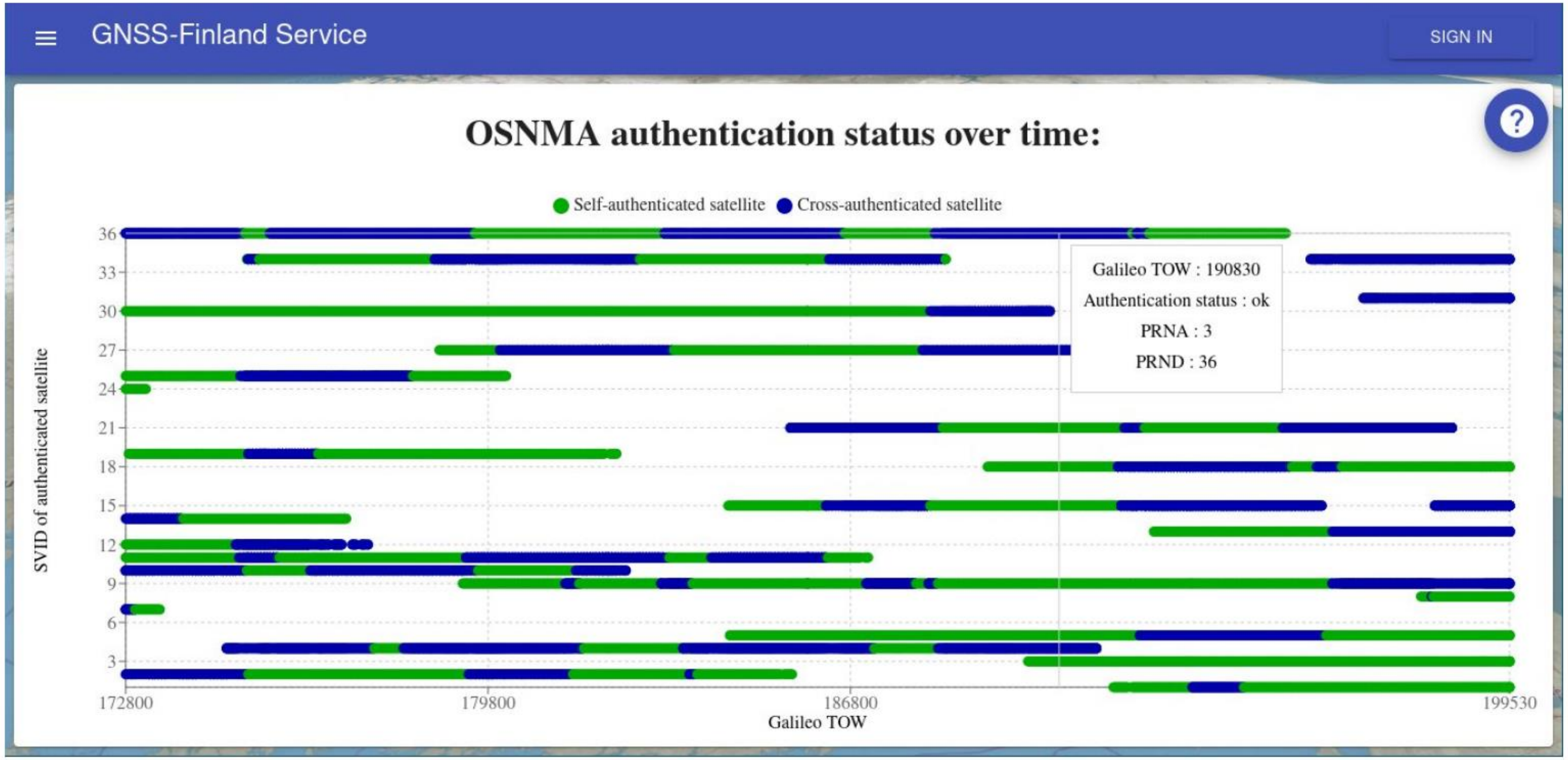




+ Kevo, Tornio, Romuvaara

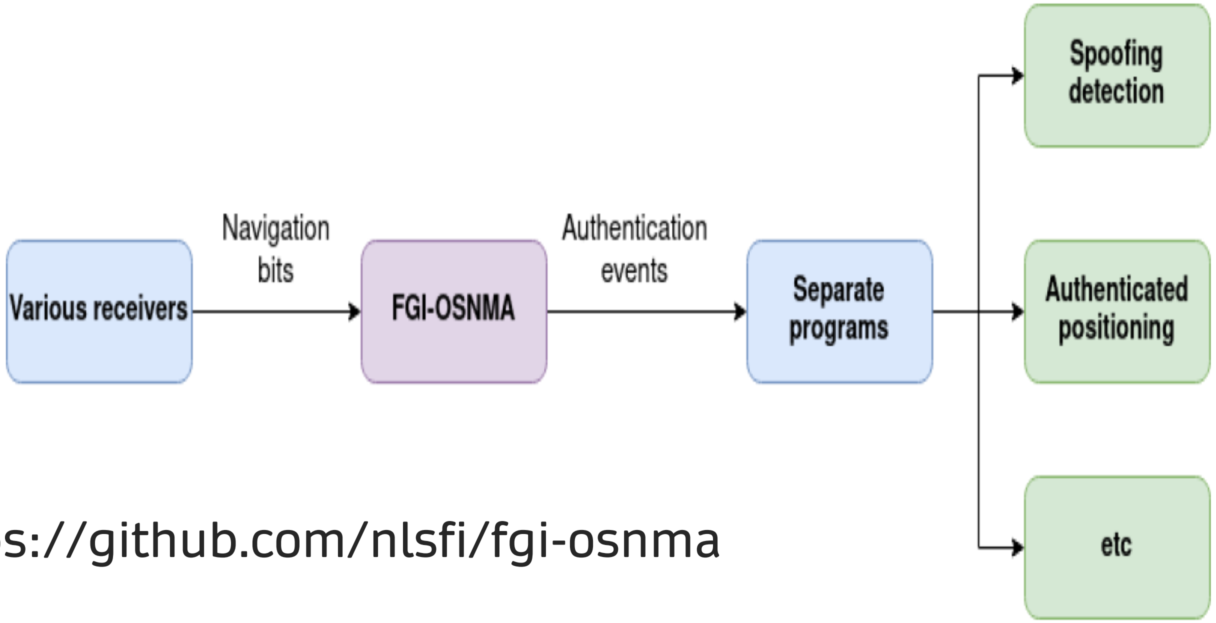
GNSS-Finland Service: Navigation Message Authentication status of monitored Galileo satellites

- Galileo satellites’ NMA monitoring status in GNSS-Finland Service
- Notification to subscribed users for a spoofing event detection

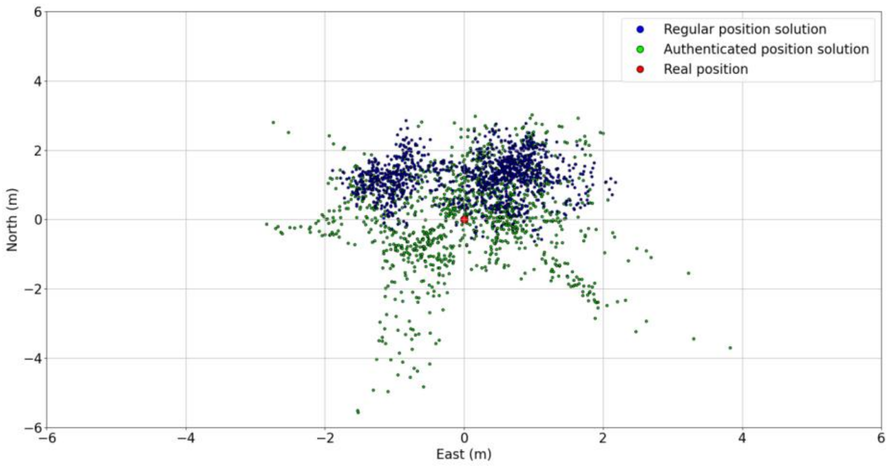


FGI-OSNMA: An Open-Source Implementation of Galileo's Open Service Navigation Message Authentication

- The purpose of FGI-OSNMA is OSNMA processing
  - Decode OSNMA related information from a data stream
  - Authenticate navigation messages based on this information
  - Report the results, or pass them forward
  - Notification to subscribed users for a spoofing event detection



https://github.com/nlsfi/fgi-osnma



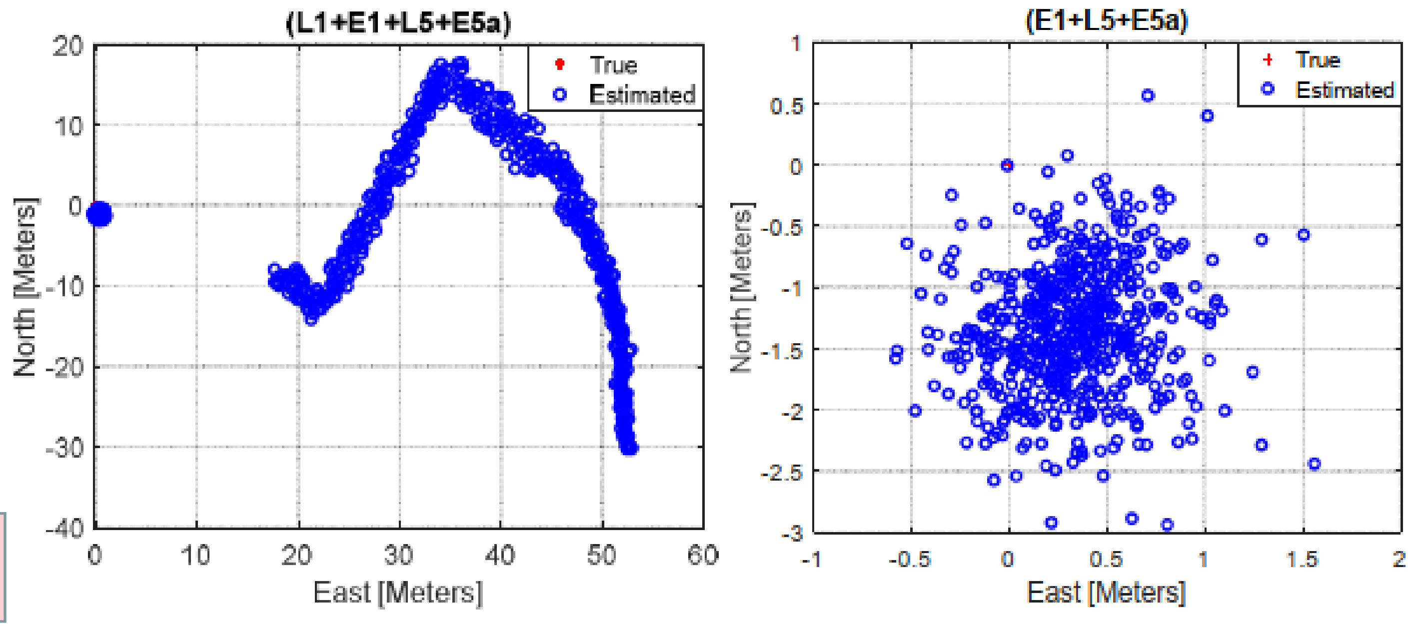
Regular vs authenticated position using FGI-OSNMA

Mitigation via exploiting multi-constellation and multi-frequency diversity

- **Resilient FGI-GSRx MFMC receiver**: Intelligent signal selection based on key vulnerability matrix.

TABLE VIII. SUMMARY OF SPOOFING IMPACT ON POSITIONING ACCURACY FOR SPECIAL SPOOFING ATTACK (GPS L1 ONLY)

DUT	ε_{3D}	ε_H	σ_H	ε_V	σ_V	*Availability (%)*	*Impact*
FGI-GSRx (L1 only)	194.8	190.6	98.7	40.2	18.0	100	High
FGI-GSRx (L1+E1)	80.2	74.9	37.7	28.6	14.8	100	High
FGI-GSRx (L1+E1+L5+E5a)	39.8	37.8	18.6	12.4	6.1	100	High
FGI-GSRx (E1+L5+E5a)	4.5	1.5	0.4	4.2	0.9	100	Low
M8T	158.4	100.5	62.0	122.4	77.2	98.1	High
F9P	117.5	117.1	68.4	9.6	6.1	100	High
X5	12.9	11.4	7.4	6.1	4.1	78.1	High
Delta-3	86.7	63.4	57.3	59.1	53.6	100	High



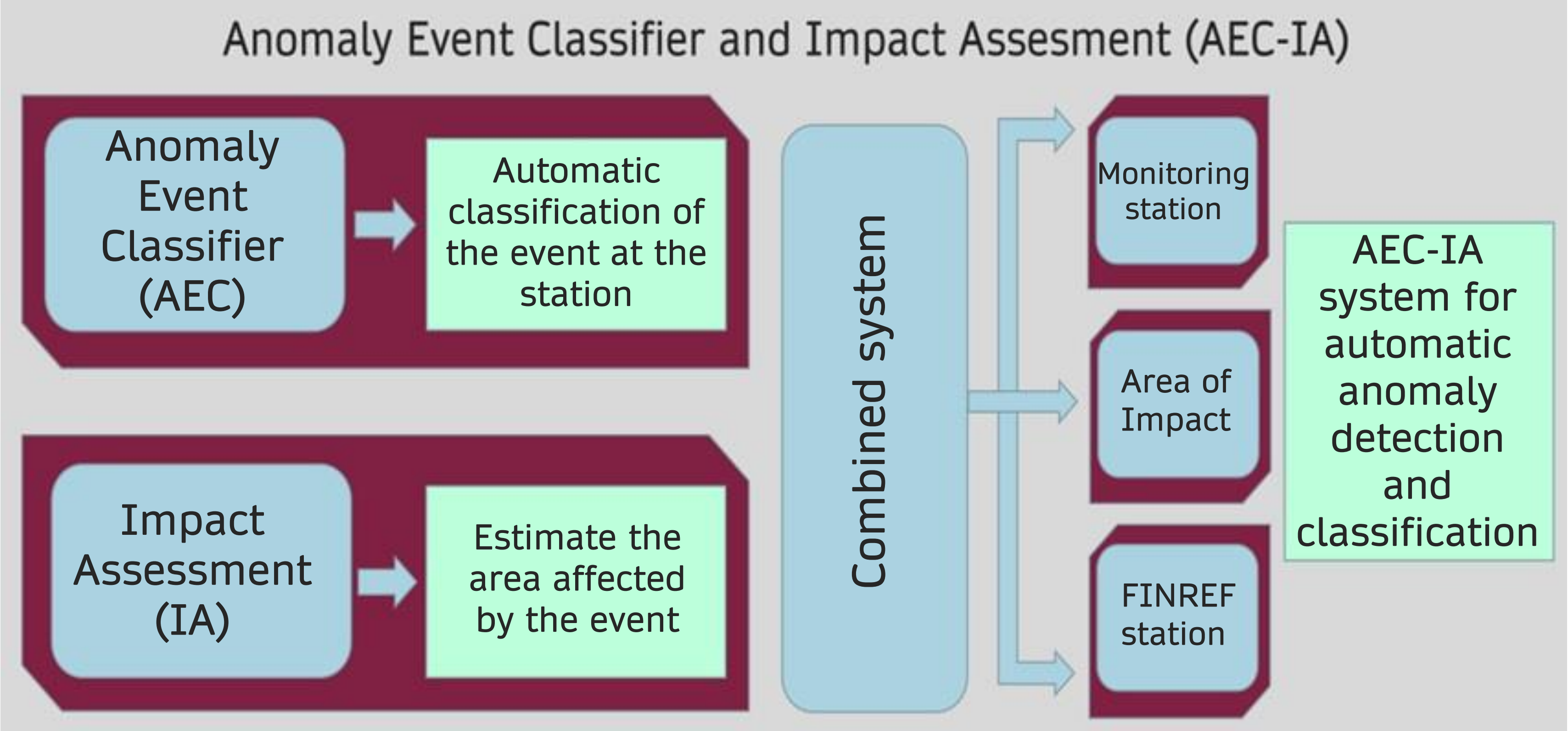
(Left): Position solution with all available constellations, (Right): Spoofing detection-based constellation selection for position solution with FGI-GSRx

https://github.com/nlsfi/FGI-GSRx
https://doi.org/10.1017/9781108934176

Islam, S., Bhuiyan, M. Z. H., Pääkkönen, I., Saajasto, M., Mäkelä, M., and Kaasalainen, S. (2023) "Impact analysis of spoofing on different-grade GNSS receivers," IEEE/ION PLANS 2023, April 24-27, 2023, California, USA.

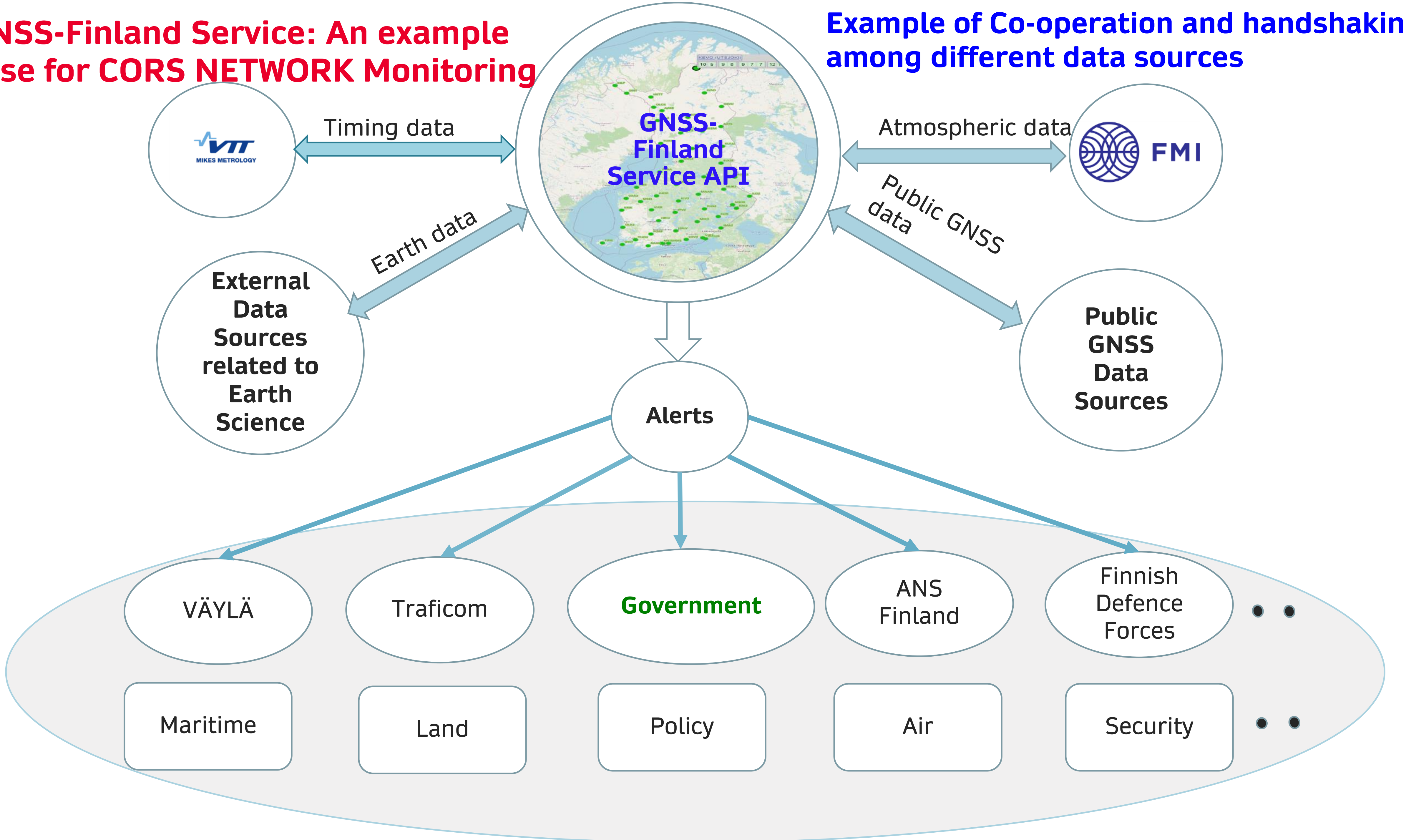
GNSS-Finland Service: Ongoing Activities

- Utilise machine learning methods for event identification
- Automatic classification of events
- Theoretical ’area-of-impact’ analysis on interference events
- Smart notification to end-users based on alert level



GNSS-Finland Service: An example case for CORS NETWORK Monitoring

Example of Co-operation and handshaking among different data sources



Agenda

1. Background

2. Actual impact

3. Resilient PNT Actions at FGI

4. Recommendations

Recommendations: Receiver/Antenna Technologies

- Multi-constellation Multi-frequency diversity
- Modernized GNSS signals and services such as Galileo E1 OSNMA (currently under live testing phase) and Galileo E6 CAS encryption (currently under development)
- Intelligent advance algorithms at tracking and measurement layers
- 'Resilient PNT Conformance framework'* will directly influence the future design, acquisition, and deployment of resilient PNT systems at a global scale.
- Low-cost antenna array solution may improve PNT resilience in the form of interference/spoofing source detection, localization, and mitigation

* https://www.dhs.gov/sites/default/files/2022-05/22_0531_st_resilient_pnt_conformance_framework_v2.0.pdf

Recommendations: Alternate PNT / Sensor Fusion

- LEO signals and satellite constellations specifically dedicated to PNT
- Receiver specific implementation that is yet to be emerged as a commercial solution to exploit GNSS+INS+LEO+SOOP (5G, etc.) with intelligent fallback mechanism.
- Space-borne interference monitoring at LEO
- Coupling of communication and localization capabilities could be used for positioning in drones, road, in and around airports and coastal areas.

Recommendations: GNSS Performance Monitoring and Alerting Network

- A wide area GNSS threat monitoring system can be developed utilizing existing national or international continuously operated reference stations, that can simultaneously monitor all GNSS frequency bands and report to a central database in case of a vulnerability incident.
- The establishment of an international or EU-level unified interference monitoring hub to identify, detect, locate, and auto-report GNSS disruptions.
- Crowdsourced interference detection could be better utilized for GNSS interference/signal quality heatmap generation.
- Privacy issue is a big concern from a regulatory perspective, and this needs to be tackled for crowdsourced data.
- Dissemination actions among the member states need to be undertaken to increase awareness and motivation among all authoritative bodies

Advancing together

NLS
FINNISH GEOSPATIAL
RESEARCH INSTITUTE
FGI